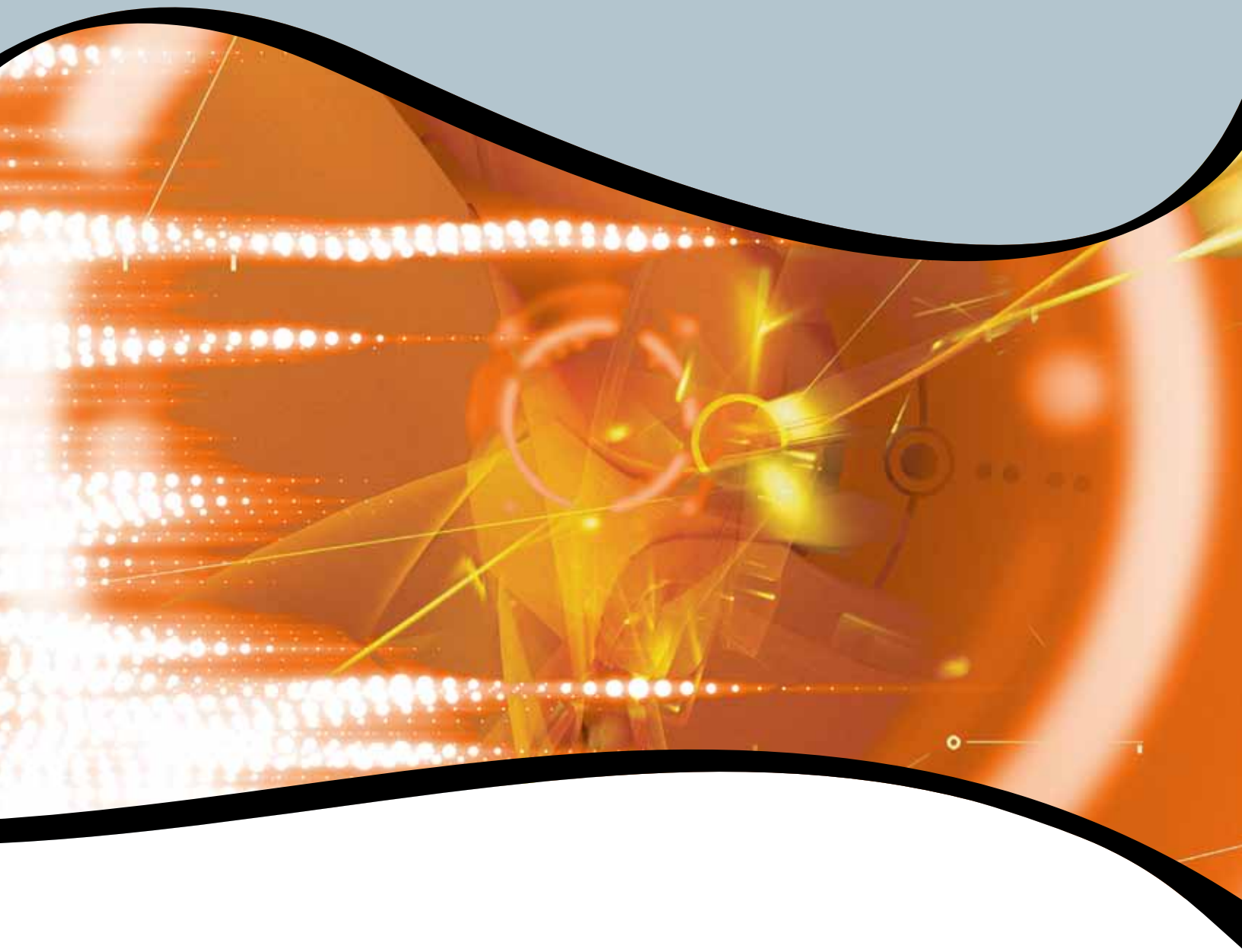
Tools

Information Assurance Tools Report

First Edition

September 17, 2009

Malware



IATAC

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
17-09-2009	Report	17-09-2009

4. TITLE AND SUBTITLE

Tools Report on Anti-Malware

5a. CONTRACT NUMBER
SPO700-98-D-4002

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Karen Mercedes Goertzel

5d. PROJECT NUMBER

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

IATAC
13200 Woodland Park Road
Herndon, VA 20171

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Defense Technical Information Center
8725 John J. Kingman Road, Suite 0944
Fort Belvoir, VA 22060-6218

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution Statement A. Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES
IATAC is operated by Booz Allen Hamilton, 8283 Greensboro Drive, McLean, VA 22102

14. ABSTRACT

This Information Assurance Technology Analysis Center (IATAC) tools report provides a brief background on what malware is, the types of malware and how they operate, recent trends in malware capabilities, behaviors, and incidents, and what makes systems vulnerable to malware infection. The report also discusses the types of countermeasures used to fight malware, and the technological capabilities employed by those countermeasures. The report goes on to provide a summary of the characteristics and capabilities of 150+ publicly-available anti-malware tools (commercial, open source, and free). Finally, the report identifies a number of suggested resources for learning more about malware and anti-malware technology and tools and for obtaining guidance on how to effectively mitigate malware risks throughout the information technology life cycle.

15. SUBJECT TERMS
IATAC Collection, malware, malicious code, virus, worm, Trojan horse, Trojan, botnet, spyware, adware, rootkit, scanner, quarantine, heuristic, signature-based

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
					Tyler, Gene
a. REPORT	b. ABSTRACT	c. THIS PAGE	None	230	19b. TELEPHONE NUMBER *(include area code)*
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED			703-984-0775

About the Authors

- **Karen Mercedes Goertzel,** CISSP, [1] leads Booz Allen Hamilton's Security Research Service. She is a subject matter expert in software assurance, cyber security, and information assurance. She was lead author of Software Security Assurance: A State-of-the-Art Report (July 2007) and The Insider Threat to Information Systems (October 2008), and contributing author to Measuring Cyber Security and Information Assurance: A State of the Art Report (May 2009), published by the Defense Technical Information Center (DTIC). Ms. Goertzel has advised the Naval Sea Systems Command (NAVSEA) and the Department of Homeland Security (DHS) Software Assurance Program; for the latter, she was lead author of Enhancing the Development Life Cycle to Produce Secure Software (October 2008). Ms. Goertzel was also a contributing author of National Security Agency's (NSA) Guidance for Addressing Malicious Code Risk, and chief technologist of the Defense Information Systems Agency (DISA) Application Security Program, for which she co-authored a number of secure application developer guides. She contributed to several National Institute of Standards and Technology (NIST) Special Publications (SP), including SP 800-95, Guide to Secure Web Services. She also tracks emerging technologies, trends, and research in information assurance, cyber security, software assurance, information quality, and privacy. Before joining Booz Allen (as an employee of what is now BAE Systems) Ms. Goertzel was a requirements analyst and architect of high-assurance trusted systems and cross-domain solutions for defense and civilian establishments in the United States (U.S.), the North Atlantic Treaty Organization (NATO), Canada, and Australia.
- **Theodore Winograd,** CISSP, has been involved in software security assurance and information assurance for over five years, particularly service-oriented architecture security and application security. He has supported the DHS Software Assurance Program, the DISA Application Security Program, and the DISA Net-Centric Enterprise Services project. Mr. Winograd has also supported security engineering efforts for multiple government organizations. Mr. Winograd has served as lead author for multiple NIST SPs, including SP 800-95, Guide to Secure Web Services, and has served as a contributing author for state of the art reports for the DTIC's Information Assurance Technology Analysis Center (IATAC).

References

1 Certified Information System Security Professional

Table of Contents

SECTION 1 ▸ **Introduction**

Note: All documents and online content cited in this report or used in its development are listed in Appendix A, Bibliography.

The Information Assurance Technology Analysis Center (IATAC) provides the Department of Defense (DoD) with emerging scientific and technical information to support Information Assurance (IA) and defensive information operations. IATAC is one of 10 Information Analysis Centers (IAC) sponsored by DoD and managed by the Defense Technical Information Center (DTIC). IACs are formal organizations chartered by DoD to facilitate the use of existing scientific and technical information. Scientists, engineers, and information specialists staff each IAC. IACs establish and maintain comprehensive knowledge bases that include historical, technical, scientific, and other data and information, which are collected worldwide. Information collections span a wide range of unclassified, limited-distribution, and classified information appropriate to the requirements of sponsoring technical communities. IACs also collect, maintain, and develop analytical tools and techniques, including databases, models, and simulations.

IATAC's mission is to provide DoD with a central point of access for information on emerging technologies in IA and cyber security. These include technologies, tools, and associated techniques for detection of, protection against, reaction to, and recovery from information warfare and cyber attacks that target information, information-based processes, information systems, and information technology. Specific areas of study include IA and cyber security threats and vulnerabilities, scientific and technological research and development, and technologies, standards, methods, and tools through which IA and cyber security objectives are being or may be accomplished.

As an IAC, IATAC's basic services include collecting, analyzing, and disseminating IA scientific and technical information; responding to user inquiries; database operations; current awareness activities (*e.g.,* the *IAnewsletter, IA Digest*, IA/Information Operations Events Scheduler, and *IA Research Update*); and publishing State-of-the-Art Reports, Critical Review and Technology Assessments reports, and Tools Reports.

The IA Tools Database is one of the knowledge bases maintained by IATAC. This knowledge base contains information on a wide range of intrusion detection, vulnerability analysis, firewall applications, and anti-malware tools. Information for the IA Tools Database is obtained *via* open-source methods, including direct interface with various agencies, organizations, and vendors. Periodically, IATAC publishes a Tools Report to summarize and elucidate a particular subset of the tools information in the IATAC IA Tools Database that addresses a specific IA or cyber security challenge. To ensure applicability to Warfighter and Research and Development Community (Program Executive Officer/Program Manager) needs, the topic areas for Tools Reports are solicited from the DoD IA community or based on IATAC's careful ongoing observation and analysis of the IA and cyber security tools and technologies about which that community expresses a high level of interest.

Inquiries about IATAC capabilities, products, and services may be addressed to:

Gene Tyler, Director
13200 Woodland Park Road, Suite 6031
Herndon, VA 20171
Phone: 703/984-0775
Fax: 703/984-0773

Email: *iatac@dtic.mil*
URL: *http://iac.dtic.mil/iatac*
SIPRNET: *https://iatac.dtic.mil*

1.1 Purpose

This report provides a brief background on what malware is, the types of malware and how they operate, recent trends in malware capabilities, behaviors, and incidents, and what makes systems vulnerable to malware infection. The report also discusses the types of countermeasures used to fight malware, and the technological capabilities employed by those countermeasures. The report goes on to provide a summary of the characteristics and capabilities of publicly available anti-malware tools (commercial, open source, and free). Finally, the report identifies a number of suggested resources for learning more about malware and anti-malware technology and tools and for obtaining guidance on how to effectively mitigate malware risks throughout the information technology life cycle.

IATAC does not endorse, recommend, or evaluate the effectiveness of any specific tools. The written descriptions are based solely on the suppliers' claims and are intended only to highlight the capabilities and features of each tool. These descriptions do not reflect the opinion of IATAC. It is up to the readers of this document to assess which product, if any, might best meet their needs. Technical questions concerning this report may be addressed to *iatac@dtic.mil*.

1.2 Scope

Currently, the IATAC database contains descriptions of numerous tools that can be used to reduce the risks posed by malware. Malware, or malicious code, is defined by the Committee for National Security Systems Instruction 4009 *National Information Assurance (IA) Glossary* as "software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an [Information System]."

According to the NSA's *Guidance for Addressing Malicious Code Risk,* "adverse impact" is not limited only to loss of confidentiality, integrity, availability: it includes loss of *any* required property of the targeted information system, including dependability, usability, performance, and privacy. Privacy is a particular concern when it comes to malware, as many forms of malware, especially spyware, are specifically intended to steal personal and personally identifying information from the computer systems they target.

Anti-malware tools are programs that perform one or more of the following activities to minimize the risk posed by malware—

- Detection of malware, malware indicators, or anomalous behavior that may indicate the presence of malware;
- Blocking malware from entering or installing on a system;
- Isolation and constraint (also known as *quarantine*) to prevent malware's execution from adversely impacting the system;
- Eradication to remove the malware and its associated traces, ideally with full recovery from its effects.

Different anti-malware tools may use different techniques and technologies to accomplish one or more of these risk-mitigating activities. To some extent, the approaches a tool uses will be governed by the type or types of malware the tool is intended to address. Viruses and worms have different

modi operandi and adverse impacts than spyware and rootkits, so the techniques and tools used to find, isolate, and eliminate them will differ.

Many vendors and developers of such tools (heretofore referred to collectively as "suppliers") advertise the uniqueness or advanced nature of their tools' technical approaches as key selling points. This marketing strategy is driven by the widespread recognition that the most well-established technology for fighting malware—detection based on the malware signature [2]—is increasingly ineffective in finding many emerging types of malware that have been expressly engineered to evade signature-based detection. An increasingly popular alternative detection approach is heuristic detection of anomalies in a program's or system's behavior that are known to be indicators of the presence of malware. A number of current anti-malware tool developers combine signature-based and heuristic detection techniques in hopes of improving their tools' "hit rate" by reducing the number of "false positives" (detections of malware that is not actually present) and "false negatives" (non-detections of malware that is, in fact, present).

Most tools that detect malware also provide some capability to isolate (quarantine) and eradicate (remove from the system) any malware the tool has detected. Again, a variety of techniques and technologies have emerged for implementing these actions in anti-malware tools. Some tools focus on keeping malware out of the system in the first place, either by blocking it at the entry point to the network to which the system is attached, or by preventing it from installing on the system. Non-installation is the goal of many anti-rootkit tools because, once installed, rootkits can be very difficult to locate and, if found, to remove without damaging the system.

All of the tools identified in this report are available on the Internet, either for direct download or for purchase. They range from elaborate commercial anti-malware tool suites to simple freeware tools produced by one or two developers. The sheer number of available tools required the authors to apply some criteria to decide which tools would be included, and which would not. The following criteria were used to exclude certain categories of tools from the descriptions in Section 4 of this report—

- **Tools that address only single malware instances.** There are a number of tools, such as AntiLove for removing the "I Love You" virus and the F-Secure® Anti-Virus "Klez" Removal Tool, that target only a single virus. Such tools are usually produced to fill a gap between the appearance of the virus and the addition of signatures for that virus to broader anti-virus tools. Such single-virus tools have been excluded from this report because by the time it is published, most, if not all of the viruses targeted by these tools will be addressed by most of the anti-virus and general anti-malware tools described here.
- **Anti-malware capabilities integrated into larger security tool suites or other software applications.** Numerous "enterprise security management" products, application firewalls, and even some virtual machine environments now incorporate anti-malware capabilities. The authors felt it would be inappropriate to describe all of these products, as their focus was not exclusively on malware. The authors have, however, identified instances in which a supplier has included the functionality of their anti-malware tool(s) in other of their security product offerings.
- **Tools that are not malware-specific, but are coincidentally useful as operational countermeasures or as malware analysis tools.** These include such tools as general security tools, spam filters, firewalls, virtual machine environments, and forensic analysis tools, binary code analysis, and reverse-engineering tools). Such tools are not included here because they are not malware-specific.
- **Tools reported to be or contain malicious code.** Even if such tools actually provide the anti-malware functionality they claim, their primary purpose has to be understood to be malicious, and therefore the authors deemed them not worthy of description. However, a discussion of such suspicious tools has been provided in Appendix D to raise the reader's awareness.

- **Tools that address only delivery vectors for malware rather than malware itself.** While vectors and exploits such as spam and cross-site scripting (XSS) are common delivery mechanisms for malware, they do not themselves constitute malware. For this reason, this report does not discuss tools for detecting or blocking spam, XSS, and other mechanisms or attacks used as malware delivery vectors.
- **Tools known (or strongly suspected) to be no longer supported by their suppliers or by any third party.** The authors have drawn the line at Microsoft® Windows® 2000 as the oldest platform of interest for the tools covered in this report. Tools that run *only* on operating system (OS) versions older than Windows 2000 (*i.e.,* Windows NT®, 98, and 95), UNIX versions prior to System V Release 3, or Macintosh® OS versions prior to OS X have not been discussed here. However, the report does cover tools that run on these earlier versions when they are supported in addition to later operating system versions. Regardless of platform, tools that have been reported by their suppliers to be no longer supported have also been excluded, even though they are still being made available without support. Ongoing support is particularly important for anti-malware tools that rely on signatures, as failure to issue signatures for new malware will rapidly render a tool obsolete.

The authors have used their best efforts to document all available anti-malware tools, but the sheer quantity of such tools virtually guarantees that some will have been inadvertently overlooked. In addition, anti-malware tools are constantly being added to the inventory to counter new threats. The tools listed in this Report are current as of 31 May 2009. Please be assured that any exclusions not related to the criteria above were not intentional. If you are aware of any tool(s) that you feel should have been included, please contact the IATAC at *iatac@dtic.mil* with information or pointers to information about the excluded tool(s).

1.3 Report Organization

This report is organized into five sections and four appendices, listed and described in Table 1-1.

Table 1-1 Report Organization and Content

Section	Title	Contents
1	Introduction	Provides introductory and background information on the IATAC and on the key concepts and remaining content of the report
2	Malware Overview	Categorizes and describes what constitutes the various types of malware for which countermeasures, in the form of tools, are available. This section also identifies the vulnerabilities in systems that make them subject to malware infection, and discusses some of the recent trends observed the nature of malware incidents, and the motivations of their perpetrators.
3	Anti-malware Countermeasures	Describes the variety of approaches used by anti-malware tools to detect, block, isolate and constrain, and eradicate malware. This section also discusses how anti-malware countermeasures can be included in IT security programs, and also how user, administrator, and developer awareness and knowledge of the malware threat can be increased.
4	Anti-malware Tools	Describes the approaches used to categorize the anti-malware tools in the IATAC IA database and the criteria for their inclusion in the database, and provides the descriptions of available anti-malware tools
5	Information Resources	Lists some key sources of information about malware, and some recommended guidance documents for addressing malware risk. This section also lists organizations and initiatives focused on addressing the problem of malware.
6	References and Bibliography	Lists print and online resources cited in or used in the development of this report
7	Acronyms and Abbreviations	List and amplifies all acronyms and non-common abbreviations used in this report
8	Definitions	Lists and defines key terms as they are used in this report
9	Additional Information	Provides additional information on the perpetrators of malware incidents, on how worms operate, and on the problem of anti-malware tools that are themselves malicious

References

2 A malware "signature" is a uniquely identifying portion of code extracted from a malware program that has been captured by a malware researcher. Because it is unique to a particular malware program, a signature can be used to perform pattern matching comparisons against the content of files and executables that are suspected to be "infected" in order to locate other instances of the same malware program. Signatures are referred to by some anti-malware developers and vendors as "fingerprints."

SECTION 2 ▸ Malware Overview

Because the first malware to gain public attention was the computer virus, the term "virus" has come to be used interchangeably with "malware" (other terms, such as "badware" and "harmware" are also used), although a virus is a specific category of malware; other categories include worms, Trojan horses (also referred to as Trojans), bots (also botnets and zombies), logic bombs and time bombs, spyware, and rootkits, with further subdivisions possible within all of these categories. The main categories of malware, and the types of malware within each of those categories, are discussed below.

2.1 Categorization of Malware

Table 2-1 lists all malware types known to be active from 2003 to present. How malware is categorized is obscured slightly by the fact that "virus" is often used to refer to any type of delivered (*vs.* embedded) malware, including worms and Trojan horse programs.

Table 2-1 Malware Types

Category	Types within Category	Subtypes within Types
Virus Replicates by attaching its program instructions to an ordinary "host" program or document, so that the virus instructions are executed when the host program is executed	*File virus* Uses the file system of a given OS (or more than one) to propagate. File viruses include viruses that infect executable files, companion viruses that create duplicates of files, viruses that copy themselves into various directories, and link viruses that exploit file system features.	*Script virus* A subset of file viruses, written in one of a variety of script languages (Visual Basic® Script, JavaScript®, Windows Batch, PHP, *etc.*). Either infects other scripts, *e.g.,* Windows or Linux® command and service files, or forms a part of a multi-component virus. Script viruses are able to infect other file formats, such as HyperText Markup Language (HTML), if that file format allows the execution of scripts.
	Boot sector virus Infects the boot sector or the master boot record, or displaces the active boot sector, of a hard drive. Once the hard drive is booted up, boot sector viruses load themselves into the computer's memory. Many boot sector viruses, once executed, prevent the OS from booting. Boot sector viruses were widespread in the 1990s, but have almost disappeared since the introduction of 32-bit processors and the near-disappearance of floppy disks as a storage medium for executables.	

Category	Types within Category	Subtypes within Types
Virus Replicates by attaching its program instructions to an ordinary "host" program or document, so that the virus instructions are executed when the host program is executed	*Macro virus* Written in the macro scripting languages of word processing, accounting, editing, or project applications, it propagates by exploiting the macro language's properties in order to transfer itself from the infected file containing the macro script to another file. The most widespread macro viruses are for Microsoft® Office® applications (Word®, Excel®, PowerPoint®, Access®). Because they are written in the code of application software, macro viruses are platform independent and can spread between Mac, Windows, Linux, and any other system running the targeted application.	
	Electronic mail (email) virus Refers to the delivery mechanism rather than the infection target or behavior. Email can be used to transmit any of the above types of virus by copying and emailing itself to every address in the victim's email address book, usually within an email attachment. Each time a recipient opens the infected attachment, the virus harvests that victim's email address book and repeats its propagation process.	
	Multi-variant virus The same core virus but implemented with slight variations, so that an anti-virus scanner that can detect one variant will not be able to detect the other variants.	
	Radio Frequency Identification (RFID) virus A type of theoretical [3] virus that is expected to target RFID devices. So far, such viruses have only been demonstrated by researchers (as described at *http://www.rfidvirus.org/).*	

Category	Types within Category	Subtypes within Types
Network worm Self-propagating program that spreads over a network, usually the Internet. Unlike viruses, may not depend on other programs or victim actions (such as opening an infected email attachment or clicking on the Web link for a malware Web site) for replication, dissemination, or execution. Worms spread by locating other vulnerable potential hosts on the network (*e.g., via* scanning or topological analysis—see discussion of worm propagation strategies below), then copying their program instructions to those hosts. Worms have traditionally been categorized according to their dissemination medium. More recently, however, they have begun to be categorized according to their propagation speed. Appendix D:D.2 explains how worms are constructed and how they propagate.	*Email worm* Spread *via* infected email attachments.	*Mass-mailing worm* Embedded in an email attachment, which must be opened by the intended victim to enable the worm to install itself on the victim's host, from which it can copy and disseminate itself to other hosts.
	Instant messaging® (IM) worm Spread *via* infected attachments to IM messages or reader access to Uniform Resource Locators (URL) in IM messages that point to malicious Web sites from which the worm is downloaded.	
	Internet Relay Chat (IRC) worm Comparable to IM worms, but exploit IRC rather than IM channels.	
	Web or Internet worm Spread *via* user access to a Web page, File Transfer Protocol *(FTP)* site, or other Internet resource.	
	File-sharing or peer-to-peer (P2P) worm Copies itself into a shared folder, then uses P2P mechanisms to announce its existence in hopes that other P2P users will download and execute it.	
	Warhol worm Theoretical* worm conceived by a researcher at University of California at Berkeley: a worm that can spread across the Internet to infect all vulnerable servers within 15 minutes of activation. ("Warhol" refers to Andy Warhol's claim that every person has 15 minutes of fame.)	
	Flash worm Theoretical worm that spreads within seconds of activation to all of the vulnerable hosts on the Internet. The discussion of worm propagation techniques in Appendix D explains the types of scanning that could make a flash worm possible.	

Category	Types within Category	Subtypes within Types
Network worm Self-propagating program that spreads over a network, usually the Internet. Unlike viruses, may not depend on other programs or victim actions (such as opening an infected email attachment or clicking on the Web link for a malware Web site) for replication, dissemination, or execution. Worms spread by locating other vulnerable potential hosts on the network (*e.g., via* scanning or topological analysis—see discussion of worm propagation strategies below), then copying their program instructions to those hosts. Worms have traditionally been categorized according to their dissemination medium. More recently, however, they have begun to be categorized according to their propagation speed. Appendix D:D.2 explains how worms are constructed and how they propagate.	*Swarm worm* An intelligent theoretical worm able to cooperate with large numbers of other worms to exhibit emergent swarm behavior "wherein simple interactions of autonomous agents, with simple primitives, give rise to a complex behavior that has not been specified explicitly." At least one proof-of-concept swarm worm, "ZachiK," has been modeled and prototyped by researchers in the Worcester Polytechnic Institute Systems Security Research Laboratory in 2005-2006.	
Trojan Horse (or, simply, Trojan) A destructive program that masquerades as a benign program. Stealthware—such as spyware, rootkits, keyloggers, trapdoors, and certain adware—represents a subset of Trojans that is intentionally designed to be hard-to-detect or undetectable Trojan horse software installs itself on the victim's computer when the victim opens an email attachment or computer file containing the Trojan, or clicks on a Web link that directs the victim's browser to a Web site from which the Trojan is automatically downloaded. Once installed, the software can be controlled remotely by hackers for criminal or other malicious purposes, such as extracting money, passwords, or other sensitive information, or to create a zombie from which to disseminate spam, phishing emails, the same Trojan, or other malware to other computers on the network/Internet. Recently, Trojans have begun using process injection to a greater extent. Several factors make this technique dangerous—(1) the Trojan is not visible in traditional process viewers, including Windows Task Manager; (2) most Trojan and virus scanners have a very hard time detecting the running Trojan code; (3) the Trojan code is very difficult to unload.	*Backdoor Trojan* *(also known as Trapdoor Trojan or Remote-Access Trojan)* Acts as a remote administration utility that enables control of the infected machine by a remote host. Examples: Back Orifice, SubSeven	*Denial of service (DoS) Trojan* If the Trojan infection spreads widely enough, the remote attacker gains the ability to create a distributed denial of service (DDoS) attack.
		FTP Trojan Opens port 21, enabling the remote attacker to connect to the victim's machine *via FTP*.

Category	Types within Category	Subtypes within Types
Trojan Horse (or, simply, Trojan) A destructive program that masquerades as a benign program. Stealthware—such as spyware, rootkits, keyloggers, trapdoors, and certain adware—represents a subset of Trojans that is intentionally designed to be hard-to-detect or undetectable Trojan horse software installs itself on the victim's computer when the victim opens an email attachment or computer file containing the Trojan, or clicks on a Web link that directs the victim's browser to a Web site from which the Trojan is automatically downloaded. Once installed, the software can be controlled remotely by hackers for criminal or other malicious purposes, such as extracting money, passwords, or other sensitive information, or to create a zombie from which to disseminate spam, phishing emails, the same Trojan, or other malware to other computers on the network/Internet. Recently, Trojans have begun using process injection to a greater extent. Several factors make this technique dangerous—(1) the Trojan is not visible in traditional process viewers, including Windows Task Manager; (2) most Trojan and virus scanners have a very hard time detecting the running Trojan code; (3) the Trojan code is very difficult to unload.	*Data-collecting Trojan* Surreptitiously collects and sends back information from the victim's machine. The surreptitious nature of such software has led to it being referred to as "stealthware."	*Spyware Trojan (also known as a spybot or system monitor Trojan)* Trojan installed surreptitiously on a personal computer (PC) or laptop/notebook to collect information about its user, the user's computer, and/or his/her browsing habits without the user's informed consent. The functions of spyware extend beyond passive monitoring to active collection of various types of personal information (*e.g.,* Web surfing habits, sites visited); interference with user control of the computer through installation of additional software and/or redirection of browser activity; reconfiguration of computer settings, resulting in slow connection speeds, changing of home pages, and/or loss of Internet connectivity or functionality of other programs. Not all spyware programs are Trojans. According to Computer Associates' 2008 "Internet Security Outlook," Trojans accounted for 18 percent of all spyware in 2007—up from 11 percent in 2006.
		Keylogger Installs itself either into a Web browser or as a device driver, from where it monitors the data input by the user *via* the keyboard, and forwards that data to a control center, such as a phishing site.
		Screenlogger Captures snapshots of the victim's computer screen, which it forwards to a control center.
		Password SpyWare Trojan Sniffs and steals passwords from the infected machine.

Category	Types within Category	Subtypes within Types
Trojan Horse (or, simply, Trojan) A destructive program that masquerades as a benign program. Stealthware—such as spyware, rootkits, keyloggers, trapdoors, and certain adware—represents a subset of Trojans that is intentionally designed to be hard-to-detect or undetectable Trojan horse software installs itself on the victim's computer when the victim opens an email attachment or computer file containing the Trojan, or clicks on a Web link that directs the victim's browser to a Web site from which the Trojan is automatically downloaded. Once installed, the software can be controlled remotely by hackers for criminal or other malicious purposes, such as extracting money, passwords, or other sensitive information, or to create a zombie from which to disseminate spam, phishing emails, the same Trojan, or other malware to other computers on the network/Internet. Recently, Trojans have begun using process injection to a greater extent. Several factors make this technique dangerous—(1) the Trojan is not visible in traditional process viewers, including Windows Task Manager; (2) most Trojan and virus scanners have a very hard time detecting the running Trojan code; (3) the Trojan code is very difficult to unload.		*Notifier* Confirms that a machine has been successfully infected, and sends information about the Internet protocol (IP) address, open port numbers, email address, *etc.*, of the victim's machine.
	Downloader, or Dropper Downloads, installs, and in the case of the Downloader, launches additional malware on the victim's machine.	*Security software disabler* Terminates/kills the execution of security programs, such as anti-virus software, firewalls, and intrusion detection agents in order to render the victim's machine vulnerable to further attacks.
		Rogue security software Represents itself as as anti-malware or anti-spyware software but, in fact, either does nothing, leaving the system vulnerable (and the user with a false sense of security) or installs malware. Appendix D: D.3 discusses some of the ways in which such tools reveal themselves to be malicious.
		ArcBomb An archived file that sabotages the archive decompressor used to open archive files. When the infected archived file is opened, the bomb is executed, causing the victim's hard disk to be flooded with nonsensical data, its resources to be "hogged," or simply causing it to crash.
	Proxy Trojan Turns the victim's computer into a proxy server (*i.e.,* a zombie) that operates on behalf of the remote attacker. If the attacker's activities are detected and tracked, the trail leads back to the victim rather than to the attacker.	

Category	Types within Category	Subtypes within Types
Trojan Horse (or, simply, Trojan) A destructive program that masquerades as a benign program. Stealthware—such as spyware, rootkits, keyloggers, trapdoors, and certain adware—represents a subset of Trojans that is intentionally designed to be hard-to-detect or undetectable Trojan horse software installs itself on the victim's computer when the victim opens an email attachment or computer file containing the Trojan, or clicks on a Web link that directs the victim's browser to a Web site from which the Trojan is automatically downloaded. Once installed, the software can be controlled remotely by hackers for criminal or other malicious purposes, such as extracting money, passwords, or other sensitive information, or to create a zombie from which to disseminate spam, phishing emails, the same Trojan, or other malware to other computers on the network/Internet. Recently, Trojans have begun using process injection to a greater extent. Several factors make this technique dangerous—(1) the Trojan is not visible in traditional process viewers, including Windows Task Manager; (2) most Trojan and virus scanners have a very hard time detecting the running Trojan code; (3) the Trojan code is very difficult to unload.	*Rootkit* A collection of programs used by a hacker to evade detection while trying to gain unauthorized access to the victim's computer. Rootkits are designed to hide processes, files, or Windows Registry entries. Rootkits are used by hackers to hide their tracks or to insert threats surreptitiously on compromised computers. Various types of malware use rootkits to hide themselves on a computer. A rootkit is installed by replacing system files or libraries, or by installing a specially crafted kernel module. Kernel-mode rootkits are much more common than user-mode rootkits, because they more powerful and easier to hide. To install a rootkit, the attacker must first obtain user-level access to the victim's computer by cracking a password or by exploiting a vulnerability; once this access is gained, the attacker gathers other user identifiers (ID) on the system until he/she is able to obtain root or administrator privileges. Once hackers get "root access" to a computer, they can manipulate it to do anything they want. Used in combination with Trojan software, hackers use rootkits to change system settings and make use of the victim computer without the user—and usually without monitoring software such as firewalls or anti-virus programs—being able to detect it. In its 2006 annual malware report, Microsoft estimated that rootkits were present in 14 percent of computers—or 9 percent when copies of the Sony Bertelsmann Music Group rootkit are subtracted. In 20 percent of cases, rootkits were installed with Trojans.	

Category	Types within Category	Subtypes within Types
Trojan Horse (or, simply, Trojan) A destructive program that masquerades as a benign program. Stealthware—such as spyware, rootkits, keyloggers, trapdoors, and certain adware—represents a subset of Trojans that is intentionally designed to be hard-to-detect or undetectable Trojan horse software installs itself on the victim's computer when the victim opens an email attachment or computer file containing the Trojan, or clicks on a Web link that directs the victim's browser to a Web site from which the Trojan is automatically downloaded. Once installed, the software can be controlled remotely by hackers for criminal or other malicious purposes, such as extracting money, passwords, or other sensitive information, or to create a zombie from which to disseminate spam, phishing emails, the same Trojan, or other malware to other computers on the network/Internet. Recently, Trojans have begun using process injection to a greater extent. Several factors make this technique dangerous—(1) the Trojan is not visible in traditional process viewers, including Windows Task Manager; (2) most Trojan and virus scanners have a very hard time detecting the running Trojan code; (3) the Trojan code is very difficult to unload.	*Bot* Any type of malware (*e.g.,* Trojan, worm, spyware bots or spybots) that enables the attacker to surreptitiously gain complete control of the infected machine. Virtually always surreptitious. A computer that has been infected by a bot is referred to as a zombie or, sometimes, a drone. Bots may be further subcategorized according to their delivery mechanism. For example, a Spam bot is similar to an email virus or mass-mailing worm in that it relies on the intended victim's action to activate it, either by opening an attachment affixed to a spam email, or by clicking on a Web link within a spam email which points to a Web site from which the bot is downloaded to the victim's computer. If the bot clones or otherwise replicates itself and exports those clones to other machines, all of the bot instances can communicate and interact with each other, thereby creating a cooperative network of bots, referred to as a botnet. A computer that has been taken over by a bot to become part of a botnet is referred to as a zombie.	*Botnet* A networked group of zombies controlled by hackers known as Bot herders, usually through Trojan software that users have downloaded (either unknowingly, or believing it to be something other than malware). Using various Internet-based communications methods (*e.g.,* Internet Relay Chat, Instant Messaging) the hacker can "wake up" tens of thousands of zombies and direct them to perform actions on the hacker's behalf, such as delivering spam, phishing, or serving crimeware. It is believed by several malware experts that Conficker's actual purpose was to install bots on infected systems in order to establish a worldwide botnet.
Spyware (non-Trojan) Non-Trojan stealthware that has the same objectives and performs the same types of actions as spyware Trojans. A number of bots have spyware capabilities, and are referred to as spybots.	*Adware* Software that automatically displays advertising material to the user, resulting in an unpleasant user experience. If malicious, adware usually exhibits the behaviors and/or infection techniques used by viruses, worms, and/or spyware.	
	Tracking cookie A cookie is a data structure that stores information about a user's browser session state. While cookies are a necessary component of how many Web sites operate, tracking cookies are specifically designed to track a user's behavior across multiple sites. Spyware sites routinely use tracking cookies to monitor a user's browsing behavior and associate it with the user's personal data such as name, credit card number, and other private information, which can then be harvested and sold to illicit marketers or cybercriminals.	
Blended attacks Combines the properties of more than one type of malware—most often viruses, worms, and/or Trojans but also, more recently, bots and adware. For example, the recent trend (2006 onwards) of using worms as a delivery mechanism for other types of malware.		

Category	Types within Category	Subtypes within Types
Embedded Malicious Code Any type of malicious logic embedded in a valid executable program by its developer, integrator, distributor, or installer. Most frequently a logic bomb, time bomb, or Trojan.		
Crimeware Any malware used in aid of criminal activities. This said, there are specific types of malware used predominantly or exclusively as crimeware.	*Email redirector* Used to intercept and relay outgoing emails to the attacker's system.	
	IM redirector Used to intercept and relay outgoing instant messages to the attacker's system.	
	Clicker Redirects the victim to a Web site or Internet resource by sending the necessary commands to the victim's browser or replacing the system file(s) in which standard Internet URLs are stored (*e.g.,* the Microsoft® Windows® hosts file).	
	Transaction generator Targets not the end-user computer but the computer of a corporate or financial institution's computer center. The software generates fraudulent transactions on behalf of the attacker within the victim organization's payment processing or other financial systems. In some instances, transaction generators are used to intercept credit card data for abuse by the attacker.	
	Session hijacker Usually a malicious browser component that, after the victim logs in or begins a browser session, takes over that session to enable a hacker to exploit it, usually to perform criminal actions, such as transferring money from the victim's bank account.	
DoS and distributed denial of service DDoS tools Software tools expressly intended to automate denial of service attacks locally (DoS) or over the network (DDoS).	*Flooder* Floods data channels with useless packets and/or messages.	
	Nuker Utility that causes fatal errors in the victim machine's application or OS by sending it specially coded or phrased requests that exploit known vulnerabilities in the application or OS.	
Malware Constructors Software tools for developing/generating new malware.	*VirTool* Utility specifically geared towards simplifying virus-writing. May also provide analysis capabilities to reveal how the virus under construction might best be used in hacking attacks.	

Category	Types within Category	Subtypes within Types
Malware Constructors Software tools for developing/generating new malware.	*Cryptographic obfuscators (e.g., FileCryptor, PolyCryptor, PolyEngine)* Cryptographic tools used to encrypt malicious programs so that they cannot be detected by anti-malware software. Some of these tools use polymorphic algorithms to generate differently encrypted versions of the same virus, so that even if one is detected, the others will not be.	
Other hacker tools and programmed exploits Software tools used by attackers to penetrate remote computers, usually *via* backdoors, and use them as zombies, or to download other malicious programs to the victim machines. Dialers are another form of malware that uses modem connections to either dial back to the attacker, or causes the victim to use primary-rate billing numbers when making connections.		

2.2 Vulnerabilities Commonly Exploited by Malware

Based on an analysis of malware-related vulnerabilities in the National Vulnerability Database, [4] the following types of vulnerabilities are typically exploited by malware to disseminate, propagate, and install themselves. Most worms exploit vulnerabilities in the victim computer's software or network to effect their own propagation. When a software vendor issues a patch, or a "researcher" announces a vulnerability, the worm author can use the information in the announcement to understand and craft a worm to exploit the vulnerability.

- Buffer overflows (the real vulnerability is a design flaw, *i.e.,* the lack or failure of input validation to prevent the submission of overlong data strings);
- Weak access control (due to poorly designed or configured access controls);
- Poor or incorrect handling of malformed data (due to lack or failure of input validation to filter out malformed data);
- Decoding errors (*e.g.,* browser or Web server Uniform Resource Locator [URL] decoding errors);
- Sabotaged configurations (*e.g.,* through tampering with the configuration script);
- Vulnerabilities in anti-virus software (exploited to disable the software or evade its detection).

2.3 Trends in Malware Incidents

From 2005 to 2006 the total number of new malicious programs increased 41 percent, according to Kaspersky Lab's "Security Bulletin 2006: Malware Evolution," and a staggering 172 percent, according to L. Corrons in "PandaLabs' Annual Report 2007." Corrons also predicted a 60 percent increase in unique novel malware starting in 2007.

Malware appears in any given environment in which the following criteria are satisfied—

- The targeted platform runs an OS that is widely used.
- Reasonably high-quality documentation is available to the malware writer.
- The targeted system is not securely configured, or has a number of documented vulnerabilities.

Potentially vulnerable OSs and applications include—

- All popular desktop OSs (*e.g.,* Windows, Macintosh OS X, Linux);

- Most general purpose Web, office, graphics, and project management applications;
- Most graphical editors;
- Applications with built-in scripting languages.

It is common for hundreds or even thousands of types of malware to exploit the same handful of vulnerabilities. This happens because the vulnerabilities are not addressed by virus definitions produced by anti-virus software vendors, and patches are not always issued in timely manner (if at all) by the supplier of the target machine's OS or application; if they are issued, they may not be installed in a timely manner, if at all, by the target machine's administrator or operator.

The following are the most prevalent vectors for malware propagation—

- E–mail (includes spam and other phishing emails),
- Web sites,
- Instant messages,
- Removable media (*e.g.,* "thumb" drives, compact discs [CD]),
- IRC, [5]
- Bluetooth® (emerging),
- Wireless local area network (theoretical).

See Appendix D for more extensive descriptions of worm behaviors and propagation vectors.

Virus-writers are using increasingly complex techniques to prevent their virus code from being detected by signature-matching anti-virus scanners. The techniques they use include—

- **Polymorphic encryption**—The virus is encrypted to escape detection.
- **Metamorphic obfuscation**—The virus code is "morphed" by adding non-virus-related logic to obscure the presence of virus logic. As the code changes, so does the virus signature generated from that code, thereby rendering the virus undetectable by matching the signature of the pre-morphed virus.
- **Code integration**—Virus code is mixed into valid program code using a tool such as the Mistfall Virus Engine.

2.4 Malware Perpetrators and Their Motivations

The following diagram characterizes who the most prevalent perpetrators of malware are, and their motivations—

The Innovators

Who?	Focused individuals who devote their time to finding security holes in systems or exploring new environments to see if they are suitable for malicious code
Why?	Challenge
How?	Embrace the challenge of overcoming existing protection measures

The Amateur Fame Seekers

Who?	Novices of the game with limited computing and programming skills
Why?	Desire for media attention
How?	Use ready-made tools and tricks

The Copy - Catters

Who?	Would be hackers and malware authors
Why?	Desire for celebrity status in the cybercrime community
How?	Interested in recreating simple attacks

The Insider

Who?	Disgruntled or ex-employees, contractors and consultants
Why?	Revenge or theft
How?	Take advantage of inadequate security aided by privileges given to their position within the workplace

Organized Crime

Who?	Highly motivated highly organized, real-world cyber-crooks; Limited in number but limitless in power
Why?	Profit
How?	A tight core of masterminds concentrated on profiteering by whichever means possible—surrounding themselves with the human and computer resources to make that happen

Source: Organization for Economic Cooperation and Development (OECD)

One other group of malware authors not included in this diagram are malware researchers who model, simulate, and prototype various types of malware as proofs-of-concept to better understand how the malware operates, propagates, and the recognizable patterns that may be used in its detection.

According to Kaspersky Lab, in 2007 the motivation behind all major malware epidemics and widespread malicious programs was financial. This is a change from 2006, in which non-commercial "vandalware" still appeared (*e.g.,* Nyxem.E, a 2006 worm that did nothing but spread itself and delete files).

References

3 Theoretical malware is malware that has been observed in laboratory environments, but has not yet been detected "in the wild."

4 NIST National Vulnerability Database. Accessed 26 June 2008 at: *http://web.nvd.nist.gov*

5 This is the vector of choice for establishing botnet control.

SECTION 3 ▶ Anti-Malware Countermeasures

3.1 Technology-Based Countermeasures

Countermeasures to malware fall into three general categories—

- **Detection**—The ability to recognize and locate malware on a system, in a file on that system, and/or in software, hardware, or media not yet installed on the system;
- **Prevention**—Keeping malware from entering, installing, and/or executing on a system. Also, keeping malware from propagating itself to other areas of a system or to other systems. Also, deterring malicious actors from embedding or implanting malware in software before it is installed on the system.
- **Eradication**—Removing malware and all of its associated traces (files, processes, system changes), and restoring the system to its pre-infected state.

Each of these categories of countermeasures is discussed below.

3.1.1 Detection

The ability to detect the presence of malware is the first step toward its isolation and eradication. Traditionally, virus detection has been performed by matching "signatures" generated from virus code captured by researchers in a laboratory environment (*e.g.,* an anti-virus tool vendor's lab) against virus code captured in the wild. However, signature-matching has inherent inaccuracies, and is not effective for detecting more sophisticated, complex malware such as rootkits and logic bombs. More advanced behavior-based detection techniques are emerging to address the need to find such malware in both systems under development and systems in operation.

3.1.1.1 Signature-Matching

The majority of virus scanners rely on signature-matching, wherein a sequence of instructions unique to a virus is used to generate a "virus signature." The virus's signature is captured in a file that is provided to the virus scanning tool. The tool compares this signature against the contents of all binary files it scans; if the signature is present, the virus from which it was generated is determined to be present. Aside from being time-consuming, the results of such scans can be inaccurate, as a pattern match of a virus signature does not always indicate the presence of an actual virus; it may simply be a coincidence (*i.e.,* the seeming virus pattern may, in fact, be part of a larger benign string of binary code). Moreover, if the virus-writer has obfuscated the virus, the virus will be undetectable by signature-matching. What the virus scanner writer must then do is discover what obfuscating technique and transformations were used by the virus-writer, and determine whether those transformations can be reversed to enable scanning for the original virus signature.

Signature-matching scanners can run either on a network entry point (*e.g.,* firewall or intrusion prevention system) to scan email and other traffic before it enters the internal network, or on user clients (PCs, laptops, notebooks, *etc.*). Operationally, they are most effective when deployed on both. Because of competition, different vendors may be the first to issue different signature files; for this reason, it makes sense for server/network based virus scanning to be performed by a different vendor's scanner(s) than that used for client-based scanning.

Because signature-based scanning relies on "signatures" of pieces of actual malicious code, which must be generated by human experts, there is an unavoidable time lag between the first observation of a virus "in the wild" and the generation of that virus' signature. This time lag means that signature-based scanning is not effective against zero-day attacks. Current research to improve signature-based scanning focuses on automating the signature generation process to significantly reduce this time lag (*e.g.,* Autograph, developed by H. Ah-Kim at Carnegie Melon University).

Not all tool suppliers implement signatures for all of the same malware instances. For this reason, certain tools may detect malware instances that other tools do not. Operationally, this has led some organizations and individual users to install multiple anti-virus scanners from different suppliers on their systems, in hopes of increasing the number of different malware instances that get detected. For others, the management challenge of ensuring that all installed anti-malware tools are kept up to date outweighs the small advantage gained by deploying multiple scanners in this way. Recently, some anti-malware tools vendors have begun offering free online scanning services; such services enable users to gain access to the scanning tools of those suppliers without having to purchase and install them. Such services are limited in that they only detect malware, and cannot eradicate any that they find. The suppliers generally offer the services as "hooks" to encourage the customers to purchase their tools. But the services can also be used as an ongoing quality assurance measure—by checking periodically to see whether the online tools of another supplier detect more or different malware instances than the tools installed on one's own system, the user can decide whether it makes sense to augment or replace the tool currently in place.

3.1.1.1.1 Data Mining to Improve Signature Generation and Accuracy

Using data mining techniques/algorithms, malware executables or bytecode and/or malicious code episode data sets (*e.g.,* fixed-length or variable-length *n*-grams) are collected as "training samples" to be analyzed using a technique, such as feature extraction (described below), to determine detectable features common to malware. The objective is to use machine learning to develop a Classifier and model that can automate and refine analysis of the content of the collected malware samples/data sets. The size and number of samples to be analyzed is determined through techniques such as *n*-gram analysis developed by Maloof, M.A. *et al.* An *n*-gram at the binary level is a sequence of *n* consecutive bytes of binary executable; at the assembler level, it is a sequence of *n* consecutive assembly instructions. This approach is still only in the research and development phase.

3.1.1.1.2 Operational Threat Discovery to Augment Signature-Based Detection

Operational threat discovery is not so much a technical approach as a strategic methodology for combining multiple general security and malware-specific detection and analysis techniques to compensate for the deficiencies in signature-based detection. Intended for use by red teams and other expert security analysts, operational threat discovery augments traditional signature-based detection. Techniques combined may include—

- **Network traffic analysis**, using devices positioned strategically on the network to collect and analyze traffic flows for malware indicators such as beaconing, data exfiltration, communication, and command and control;
- **Device analysis**, to discover unique attributes of data collected from servers and clients that may indicate malware, spyware, or other suspicious activity;
- **Log analysis**, to detect suspicious activities associated with malware delivery or execution, such as large file transfers and beaconing activities;
- **Digital forensic analysis**, to locate malicious code indicators (file names, dates, account names, *etc.*) on hard drive images.

3.1.1.1.3 Emerging improvements to behavior-based detection

In hopes of improving early detection of viruses that propagate at hyper-fast speeds (not possible with current signature-based techniques), researchers at Sichuan University in China are applying finite state machine theory to the detection of a virus's self-relocation "gene," both in known virus executables and in unknown but suspicious executables.

3.1.1.2 Behavior-Based Detection

Behavior-based detection techniques focus on analyzing the behavior of known and suspected malicious code. Such behaviors include factors such as the source and destination addresses of the malware, the attachment types in which they are embedded, and statistical anomalies in malware

infected systems. One example of a behavior-based detection approach is the histogram-based malicious code detection technology patented by Symantec.

3.1.1.2.1 Feature Extraction in Support of Behavior-Based Malware Detection

Feature extraction, also known as function extraction, requires reverse engineering of the malware binary and the subsequent review of the resulting assembler or source code. The review focuses on extracting information about important malware features/functions, and analyzing machine code features and system application programming interface (API) call features (Dynamic Linked Library [DLL] function call information), in order to develop a robust characterization of how the malware operates so that such features can be recognized as hallmarks of future malware. Extensive research into feature extraction for malware is underway at University of Texas at Dallas. The software security analysis firm VeraCode also claims to perform feature extraction for malware as part of their commercial Security Review service.

For the past several years, researchers at Carnegie Mellon University's Software Engineering Institute have been working to implement Function Extraction (FX) technology for automating the derivation and calculation of the functional behavior of software. The objective of this behavior calculation is to reveal the net functional effect of software. Primarily intended to augment human analysis and design activities during the software life cycle, FX is also being investigated for its usefulness in detection and analysis of malicious code embedded within software by revealing its functional intentions and effects (as captured in behavior databases produced by function extractors), and then developing countermeasures to those malicious functional intentions.

3.1.1.2.2 Malicious Property Detection

Researchers in the University of Wisconsin's Wisconsin Safety Analyzer project have developed an approach for analyzing the semantic structures (*e.g.,* control flows and data flows) of software programs for presence of malicious *properties* such as "the program writes to an executable file," "the program monitors and changes executables as they are loaded into memory," and "the program behaves exactly like known virus *n*." Based on this analysis, the analyst can develop a "blueprint" of malicious virus behavior from a model of the program to be analyzed. Model checking is then used to determine whether the virus blueprint and the program model "match." Because it is based on behavioral analysis rather than pattern (signature or string) matching, this approach can be used to detect obfuscated/morphed viruses, and can be extended to model and analyze other types of malware (*e.g.,* Trojan horses, backdoors, spyware, worms, *etc.*).

3.1.1.3 Anomaly-Based Detection

Anomaly-based detection looks for indicators of unexpected and abnormal behavior indicative of the presence of malicious code. Specifically, anomaly-based detection establishes a baseline of expected operation within a computer system. Once a baseline has been established, any variations from the baseline are attributed to malicious code, allowing malicious code detection and removal tools to isolate the offending code and prevent it from performing its intended functions. Similar techniques are being used to detect other types of security intrusions and compromises, not just those associated with malware.

3.1.1.3.1 Heuristic scanning for code abnormalities indicating malware

Heuristic scanning looks for abnormal structures at certain locations in the code of the program suspected of harboring malicious logic; an example of an abnormal structure would be a *jump* at the beginning of a program. If the scanner finds an abnormal structure, it infers that the abnormality is caused by the presence of malicious logic. Unfortunately, the inferences and assumptions made by heuristic scanners are often incorrect, which renders them inaccurate tools that are only useful when run in conjunction with other behavior-based and anomaly-based tools.

3.1.1.4 Detection of Indirect Malware Indicators

Several approaches infer from indications of modifications to valid system contents or software code that the code must have been altered through the pre-installation embedding or post-installation insertion of malicious logic or the corruption of the operational software by interaction with running malware. Indirect malware indicators include—

- **Unauthorized software changes**—System integrity assurance techniques, such as peer reviews, software audits, and automated scans, focus on determining, at various stages in the system's life cycle whether unexpected or unintended changes have been made to the system's software. For example, a series of "manufacturing scans" during the acquisition, integration, and testing phases of system development involve running of virus detection, spyware detection, and other malware detection tools to determine whether malware has been introduced into the system by any of its commercial or open source components.
- **Checksum mismatches**—Calculation and comparison of checksums on pre-delivery and post-delivery binary executables may reveal tampering or corruption of the post-delivery binary. If the checksum was digitally signed, verification and validation of the signatures on the pre- and post-delivery versions' checksums before the checksums themselves are recalculated and compared can provide further indication that the checksum itself was tampered with/corrupted, and thus the code is likely to have been as well.
- **System profile anomalies**—System profiling can augment checksum calculation by verifying that the system's directory structures have not been corrupted or tampered with. Such profiling includes analysis and verification of valid file attributes, presence of unexpected files or absence of expected files, and review of other characteristics of the entire collection of files for indications of anomalies. System profiling usually relies on digitally signed databases, and includes file system checking that bypasses normal OS facilities that can detect checksum-aware malicious logic.
- **Steganographic obfuscation and/or encryption of inbound files**—More commonly used for detecting unauthorized exfiltration ("leakage") of data in outbound traffic, steganography detection can also be applied to inbound data/traffic, including streaming media, with presence of steganography interpreted as a potential indicator of the embedding of malicious code in the steganographically-obfuscated inbound data file or stream. Similarly, unexpected encryption of inbound data (*i.e.,* data not expected to be encrypted, or encrypted using an unfamiliar or unauthorized algorithm or protocol) may also indicate encryption used to avoid detection of malware. Detection (either at the network boundary or at the endpoint) of either steganography or encryption on inbound files, messages, *etc.*, can be used to justify blocking the data at the network boundary, or to trigger an alert when the file is forwarded on to the intended recipient that the file is suspicious and should either be checked directly for presence of malware before opening/accepting (higher risk) or simply deleted (lower risk).

3.1.2 Prevention

Approaches throughout the system life cycle are needed to prevent malware from (1) being embedded or implanted in systems under development, (2) being delivered to and installed on an operational systems, and (3) being executed on operational systems and then propagating to other systems on the same network. These approaches include—

- Software assurance during development, including "defensive" design and coding techniques, use of "safe" software tools and programming languages, and other software life cycle practices, such as secure configuration control, static analysis and other security testing techniques, and trusted distribution, to—
  - Minimize the presence of vulnerabilities in software that can be exploited by malware;

- Increase the likelihood of detection and removal of malicious logic "planted" by the system's developers, testers, or distributors before the software is fielded.

- Use of "demilitarized zones" and other approaches to create "closed" environments with access to the Internet or email, in which servers are hosted that run software (*e.g.,* servers, Web services, other "software as a service") or from which internal users can download software applications, patches, virus signature updates, *etc.*
- Survivability engineering uses techniques, such as system diversity and software evolution to minimize the susceptibility of the organization's entire computing infrastructure to the same malware. Survivability engineering also uses redundancy techniques to enable more rapid recovery from malware incidents by allowing for swapping in of clean backup systems, together with network topologies that allow for continued operation of unaffected portions of the infrastructure while infection portions are isolated/disconnected and sanitized/restored.

3.1.2.1 Quarantine

The objective of quarantine is to prevent detected malicious code execution from affecting the system without risking damage that might arise from simply deleting the infected file to which the malicious code has attached or inserted itself; for example, simply deleting the system's *explorer.exe* file because it is suspected of being infected would corrupt/destroy the system's ability to operate. The anti-malware tool that detects the infected file moves it to an isolated location that is controlled by the tool itself, where that file's execution (if/when it executes) will not affect other files on the system. This enables the system's user to send a copy of the quarantined file to the tool's research team, which should be able to determine whether that file is in fact infected, and if so, whether it can be safely "sanitized" and moved out of quarantine back to its original location in the file system, or whether it needs to be deleted and its pre-infection version restored from backup (or, better yet, from its original medium, *e.g.,* CD).

3.1.2.2 Constrained Execution Environments

Constrained execution provides a controlled, (fairly) closed environment in which suspicious or untrusted code can execute with minimum access to other parts of the system, thereby minimizing the impact (and extent of reach) of the executing code if it turns out to be malicious. Use of virtual machines and "sandboxes" and file system access controls can ensure that "untrusted" files entering a server or client can only execute within the configured constrained environment, from which software processes are unable to write to other areas of the system outside that constrained environment; this prevents malware (viruses, worms) from propagating outside the constrained environment.

Additional hardware protections, such as read-only memory (ROM) and trusted platform modules (TPM) can be used to further isolate high-confidence, high-consequence code from untrusted code. Use of ROM rather than random access memory (RAM) memory assigned to trusted, critical functions can prevent malicious logic from corrupting that memory. TPMs can be used to run trusted critical system and application software in a physically isolated environment that is physically impenetrable by malicious code downloaded to system areas outside the TPM.

3.1.3 Eradication

Eradication—removal of malware and recovery from its effects on operational systems/environments—focuses on sanitizing all systems and devices suspected of harboring the malicious code to eliminate all traces of that code, and to restoring the affected systems to their pre-malware state. The technologies for accomplishing eradication are often built into the same tools that are used to detect malware. However, in the majority of cases, at least some operational restoration measures will also be needed, such as restoration of the system from backup, reinstallation of clean versions of affected software, and also strengthening of detection and prevention countermeasures to reduce the likelihood of future malware infections.

3.2 Integrating Anti-Malware Countermeasures into IT Security Programs

At the system development level, the security architecture for all servers and clients should include the types of hardware/software constrained environments that will minimize those systems' susceptibility to malware installation, uncontrolled execution, and propagation, and will also accelerate and ease sanitization and restoration of operation after a malware incident. Software and system assurance measures should be included to minimize the possibility and increase the detectability of malicious code that enters the system during its development, distribution, and installation.

At the system operational level, countermeasures for detecting and eradicating malware should become standard components of the system's security "arsenal," along with firewalls, intrusion detection and prevention systems, *etc.* Such countermeasures should include network-based, server-based, and client-based countermeasures. At the network level, firewall policies should be adjusted as described below to block inbound traffic suspected of carrying malware. At the server level, countermeasures should include such features as scanning by the email server of inbound and outbound email attachments. At the client/endpoint level, robust anti-virus and anti-spyware tools should be installed, and their usage—including updating of signature files—should be made as easy, transparent, and non-bypassable as possible, so that as little as possible of the organization's anti-malware effectiveness depends on the end users. The same is true of system configuration and backups that support the lowest-impact recovery from malware incidents. Ideally, the end user's role should be limited to not getting in the way of the operation of anti-malware tools and related countermeasures. The user should not be expected to participate, except in the most basic, minimal way, in anti-malware tool operation and updating, malware eradication, or post-incident system recovery.

Information technology (IT) security programs' non-procedural elements should also be extended to include physical, policy, and training/awareness countermeasures that focus on malware prevention. For example, to prevent malicious insiders from inserting malware into stored backups of executables, all media containing software executable images and backups should be stored in locked cabinets or safes to prevent unauthorized physical access. In addition, all servers and network devices should be located in physically access-controlled facilities, to prevent unauthorized physical access by malicious insiders who may abuse direct access to install malware on those servers/devices.

Policies that expressly focus on minimizing risk of malicious code being brought into the system from outside should be developed and enforced. For example—

- Firewall policy should be adapted to require blocking of inbound files that are encrypted, steganographically obfuscated, or compressed. This will reduce the risk posed by files that may have been encrypted or obfuscated to prevent malware detection, or files compressed to obscure the true size of their contents (*e.g.*, files containing executable code).
- Email policy should limit the size of inbound email attachments (with appropriate sizes set for both uncompressed and compressed—if allowed—attachments), HyperText Transfer Protocol *(HTTP)* and FTP downloads, *etc.* This will reduce the risk that executable code can be downloaded from the Internet in violation of software installation policies.
- Digital media policies should prohibit the use of thumb drives, removable hard drives, CDs, Digital Versatile (or Video) Discs (DVD), *etc.*, to minimize the likelihood of users inadvertently installing malware carried in "infected" files on removable media brought from home.
- Software installation and monitoring policies should strongly deter users from installing unapproved software downloaded from the Internet or copied from CDs. Such policies are enforced through active monitoring of all network-connected systems to ensure that they contain only authorized software.

- Patch management should be beefed up, with security patches distributed on as aggressive a timetable as possible, to narrow the window of opportunity for malware such as Conficker to exploit known vulnerabilities in unpatched systems. Patching will not eliminate zero-day vulnerabilities, but it will significantly reduce risks posed by long-standing vulnerabilities that malware writers will still opportunistically exploit. According to security expert Roger Thompson, government, corporations, and academia are particularly notorious for not applying security patches in a timely manner, if at all. [6]
- Similarly, other aspects of security vulnerability management need to be reviewed and enhanced. For example, according to Paul Ducklin, head of technology for Sophos Asia-Pacific, warned in March [7] that organizations with weak password construction and management policies would be particularly vulnerable to Conficker, which, if it cannot exploit an unpatched vulnerability, resorts to password cracking to gain access privileges and install itself on a vulnerable system. Clearly virus writers have become very resourceful in finding and exploiting vulnerabilities in the systems they target. Closing obvious holes should be an established policy and practice of every organization and individual computer user.
- User training in cyber security and "safe" computing should include specific information on issues, such as recognition of malicious code indicators, avoiding cross-site scripting exploits, anti-virus and anti-spyware tool usage, and signature updating.
- Administrator training should include anti-virus/anti-spyware tool updating (if such updates are centrally served to users), patching of vulnerabilities that make systems malware-susceptible, response to and recovery from malware incidents, *etc.*
- Developer and integrator training should include software and system assurance principles and best practices, such as secure configuration control, security analysis of custom-developed and third-party components (commercial off-the-shelf [COTS] and open source), and peer reviews and testing to decrease the possibility of malicious code being added to the system, either unintentionally or intentionally, in the first place, but also that any that does get added will be detected and removed before the system is deployed.

References

6 See Thompson's quote at the beginning of the PCMagazine Security Watch blog, "Infected with Conficker? Here's What to Do," dated 1 April 2009 and accessed 31 May 2009 at *http://blogs.pcmag.com/securitywatch/2009/04/infected_with_conficker_heres.php*

7 Ducklin was quoted by Vivan Yeo of ZDNet Asia in her article "Conficker woes call for strong passwords," 31 March 2009. Accessed 31 May 2009 at *http://www.zdnetasia.com/news/security/0,39044215,62052730,00.htm*

SECTION 4 ▶ Anti-Malware Tools

4.1 Classification of Tools

The tools described in the IATAC IA Tools Database can be classified using two different classification methodologies. The first set of classification determines how the tool is used within an organization—

- **Host- or endpoint-based**—Used to protect individual computer systems.
- **Network-based**—Monitor an organization's networks for signs of malicious code activity, by actively recording network traffic, analyzing firewall, router and application logs, or performing scans of systems over the network. They may also operate at the network boundary to detect and block malware from entering the network.
- **Tools-as-a-service**—Access to tools in the form of a malicious code detection service accessible over the Internet. Such services are most useful when they augment the use of host/endpoint-based and network-based tools, in order to gain better coverage. Often tools-as-a-service are provided for detection only, with the user required to purchase a license or service in order to eradicate threats found by those tools

The second set of classification is based on the mechanisms the tools use to perform their anti-malware detection and response activities—

- **Malware detection and removal**—Tools that primarily perform detection and removal of malware; subcategories include: virus detection and removal, Trojan detection and removal, spyware detection and removal, and rootkit detection and removal.
- **Detection of malware indicators**—Tools that rely primarily on behavioral and heuristic anomaly detection and analysis to identify system or program behaviors that are indicative of infection by malicious code
- **Trace detection**—Tools that scan systems for API hooks and other common traces of the presence of malicious code on the system
- **Malicious code analysis**—Malware research tools that focus on analyzing malicious code to determine how it is structured and how it operates, usually in support of generating new malware signatures or removal techniques
- **Malware honeypot**—Tool that captures code originating from a suspicious source or code of an unknown type, and monitors the behavior of that code to determine whether it is, in fact, malicious
- **Hidden process detection**—Tools that detect hidden processes running in the OS or kernel, as such processes often indicate the presence of malicious code

4.2 Tool Selection Criteria

The tools selected for inclusion in this Report satisfy the following three criteria—

- **Definition**—These tools satisfy the objective, approach, and methodology of an anti-malware tool based on the definition of malware.
- **Specificity to malware**—The primary and explicit function of these tools is to reduce the risks and adverse impacts associated with malware, either operationally, by detecting, blocking, isolating and constraining, or removing and recovering from malware attacks, or by enabling analysis and better understanding of malware structure and behavior.
- **Current availability**—The tools that are included in this report are currently available from the Government, academia, or commercial sources, or as freeware on the Internet.

In addition to these criteria, the tools selected do not meet any of the criteria for exclusion described in Section 1.2. This means that none of the selected tools—

- Addresses only a single malware instance;
- Is an anti-malware capability built into a larger security tool suite or other software application;
- Has been reported to be or to contain malicious code;

- Addresses only delivery vectors for malware rather than malware itself;
- Is intended for other or broader purposes, but coincidentally happens to be helpful in reducing malware risk or analyzing malware;
- Is known or strongly suspected to no longer be supported by its supplier or any third party.

4.3 Descriptions of Current Anti-Malware Tools

The remainder of this document summarizes pertinent information, providing brief descriptions of available anti-malware tools with contact information for the tool supplier. For the most part, these descriptions are direct copies or adaptations of the suppliers' own published descriptions of their tools, except when the supplier provided little or no description, in which case third-party information sources such as *http://www.chkrootkit.org* and *http://www.antirootkit.com/* were consulted. Hardware specifications provided here indicate minimum requirements.

As stated earlier, IATAC does not endorse, recommend, or evaluate the effectiveness of these tools. Any qualitative judgments implied in the tools' descriptions originate with the supplier. It is up to the reader to further investigate those tools that appear useful, and to assess their actual capabilities and quality against the claims made by their suppliers.

The tools are categorized as follows, and presented in the following sections—

- **Anti-malware tools**, including—
  - Anti-virus tools,
  - Anti-spyware tools,
  - Anti-rootkit tools,
  - Antibot, antibotnet, and antizombie tools;
- Installation blocking, execution termination, and isolation and constraint tools;
- Malware analysis tools;
- Other anti-malware tools that fall outside the categories above.

For each tool, the following information is captured:

- Abstract describing the tool;
- Table that includes the information about the tool described below.

Tool Name

Type	The type of tool, or category in which this tool belongs, *e.g.,* "Trojan detection and removal"
Operating System	The operating system(s) on which the tool runs. If the tool is an appliance, this field will contain a "not applicable" symbol (N/A) because the operating system is embedded in the tool.
Hardware	The third-party hardware platform(s) on which the tool runs, plus any significant additional hardware requirements such as minimum amount of random access memory or free disk space. If the tool is an appliance, this field will contain a "not applicable" symbol (N/A) because the hardware is incorporated into the tool.
License	The type of license under which the tool is distributed, *e.g.,* Commercial, Freeware, GNU Public License
NIAP Validated	An indication of whether the product has received a validation by the National Information Assurance Partnership (NIAP) under the Common Criteria, Federal Information Processing Standard 140, or another certification standard for which NIAP performs validations. If no such validation has been performed, this field will be blank.
Common Criteria	If the tool has received a Common Criteria certification, the Evaluation Assurance Level and date of that certification. If no such certification has been performed, this field will be blank.
Developer	The individual or organization responsible for creating and/or distributing the tool
URL	The Uniform Resource Locator of the Web page from which the tool can be obtained (downloaded or purchased), or in some cases, the Web page at which the supplier can be notified with a request to obtain the tool

A note about licenses—Some vendors of tools that have commercial licenses offer free "demo" versions with fixed usage expirations. Only those tools that are truly free (*i.e.,* with no fixed usage duration or other usage restrictions) are listed as "freeware." Vendors that offer both commercial and freeware versions of their tools, the latter without usage restrictions, are noted as offering commercial tools with freeware versions available.

4.3.1 Malware Detection and Removal Tools

4.3.1.1 "Broad Spectrum" Anti-Malware Tools

The tools described in this section are understood to address more than one category of malware.

Agnitum® Outpost Antivirus Pro

Abstract

Outpost Antivirus Pro protects digital assets against viruses and spyware, and provides proactive blocking of suspicious and unauthorized behaviors often associated with malware. Outpost Antivirus Pro also ensures that Web sites the user visits cannot surreptitiously serve malware to the user's PC.

Agnitum also includes all Outpost Antivirus Pro capabilities in their Outpost Security Suite, Outpost Network Security, and Outpost Firewall Pro products.

Outpost Antivirus Pro

Type	Malware detection and termination
OS	Windows Vista, XP, Server 2008, Server 2003, 2008, 2000
Hardware	450 Megahertz (MHz) central processing unit (CPU) (x-86/x-64/multi-core), 256 Megabytes (MB) RAM, 100 MB free disk space
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	Agnitum Ltd. (Cyprus or Russian Federation)
Availability	*http://www.agnitum.com/products/antivirus/index.php*

ALWIL Software avast! anti-virus Professional Edition

Abstract

avast! anti-virus Professional Edition is a collection of tools aimed to protect computer systems from viruses, spyware, and rootkits. avast! anti-virus leverages the GMER toolkit (described later in this section) to perform scans for and remove rootkits on a system. Coupled with avast!'s virus and spyware database, users are provided continuous protection against malware.

avast! anti-virus Professional Edition

Type	Malware and rootkit detection and removal
OS	Windows 95 and later, Linux, Mac OS X 10.3 and later
Hardware	
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	ALWIL Software, A.S. (Czech Republic)
Availability	*http://www.avast.com/eng/avast_4_professional.html*

Ashampoo® AntiSpyware 2

Abstract

Ashampoo AntiSpyware 2 provides comprehensive protection against hijackers, dialers, spyware, worms, adware, Trojans, keyloggers, and rootkits. The AntiSpyware Guard feature provides automatic updates and daily signature updates. Whitelisting enables individual folders, files, and even "infections" to be excluded from scanning to prevent false alarms; internal encryption algorithms prevent malicious threats from secretly adding themselves to the whitelist. Scans can be scheduled to run automatically or on demand.

Ashampoo AntiSpyware 2

Type	Malware detection and removal
OS	Windows 2000, XP, Vista
Hardware	
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	Ashampoo GmbH (Germany)
Availability	*http://www2.ashampoo.com/webcache/html/1/product_2_0149___USD.htm*

The tool protects against unknown threats that are detected and blocked with the aid of sophisticated heuristic-analysis algorithms that identify them by their behavior. All suspicious files are moved into quarantine to enable the user to decide whether they should be deleted. A direct online connection to a malware database provides user access to information on detected infections.

AutoStart Manager identifies and disables unwanted auto-start programs. The tools also includes a System Process Monitor for monitoring all system processes and disabling them as necessary; the Monitor also monitors Browser Helper Objects (BHO), Winsock Layered Service Providers (LSP), Windows Hosts file, Autostart entries, *etc.* The LSP-Viewer enables the user to identify installed Winsock attributes, which are often used as an import mechanism for parasite programs. The Hostsfile Checker reports suspicious entries in Hosts file and allows for cleaning up.

Internet Cleaner removes up all tracks from the user's Internet activities, while the File Wiper erases files and folders permanently so they cannot be recovered. IP Spam Blocker provides protection against desktop popup ads.

Authentium® Command Anti-Virus v5

Abstract

Command Anti-Malware scans for viruses, spyware, malware, and other potentially unwanted programs. The tool implements a four-phase detection system to significantly minimize incidence of false-positives. The tool uses heuristics to identify threats based on behavior that uses a neural network learning capability to recognize and block novel threats. The tool's anti-virus engine simulates the execution of programs to determine which Windows OS calls they attempt to make; this capability runs in a fully quarantined environment entirely segregated from the host OS. The tool provides real-time scanning. Authentium advertises that its malware signature database contains over 800,000 discrete pieces of malicious code.

Command Anti-Virus v5

Type	Anti-malware detection
OS	*Client*—Windows Vista, XP, 2000; *Server*—Windows XP, Server 2003, 2000
Hardware	
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	Authentium, Inc.
Availability	*https://www.authentium.com/mainv2/command.htm*

AVG 8.5 Internet Security

Abstract

AVG 8.5 Internet Security includes the following tools—

- **Anti-Virus and Anti-Spyware**, to detect and remove viruses, worms, spyware and Trojans;
- **Identity Protection**, to help protect against identity theft;
- **Anti-Rootkit**, to detect and remove rootkits;
- **Web Shield**, to scan downloaded files and instant messages for malware;
- **LinkScanner**, to block malicious Web sites;
- **Anti-Spam**, to filter junk mail and phishing mail;
- **Firewall**, to protect against network-based threats;
- **System Tools**, to control AVG Internet Security.

AVG 8.5 Internet Security leverages real-time scanning and automatic signature updates to protect computer systems against malicious code.

AVG 8.5 Internet Security

Type	Virus, spyware, and rootkit detection and removal
OS	Windows 2000 and later
Hardware	
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	AVG Technologies CY, Ltd. (Cyprus)
Availability	*http://www.avg.com/product-avg-internet-security*

Avira AntiVir®

Abstract

Avira's AntiVir detects and eliminates viruses, worms, Trojans, rootkits, phishing, adware, spyware, bots, and prevents dangerous "drive-by" downloads of viruses. The tool also protects against phishing attacks and hidden rootkits. The tool includes an EmailScanner, plus WebGuard protection that prevents connections to known malicious Web sites. The RescueSystem create a bootable rescue CD, while QuickRemoval eliminates viruses with a single mouse click. The tool also provides NetbookSupport for laptops with low resolution.

The product comes in Premium and Professional editions, and provides tools to support Windows and UNIX file servers, SharePoint and SAP NetWeaver Web portal servers, Exchange, MIMEsweeper, Domino, and Linux-based mail servers, Proxy servers, and Smartphones, personal digital assistants (PDA), and PocketPCs running Windows Mobile.

AntiVir	
Type	Malware detection, blocking, and removal
OS	*Desktop*—Windows 2000, XP, Vista *File server, Mail Server, Portal Server, MIMEsweeper*—Windows 2000 Server, Server 2003, Server 2008, Citrix® Presentation Server, Red Hat Enterprise Linux 4/5 Server, Novell SuSE® Linux Enterprise Server 9/10-10.2, Debian® GNU/Linux 4, Ubuntu® Server Edition 8, Sun Solaris 9/10, Novell Open Enterprise Server *Proxy server*—Windows 2000, 2003 *Mobile on PocketPC*—Windows 2000, XP, Vista on PocketPC *Mobile on Smartphone or PDA*—Windows Mobile 2003, 5, 6.1
Hardware	*File server for Solaris*—UltraSparc IIi 650 *Portal server for UNIX/Linux or Windows*—Pentium III 500 MHz *Portal server for Solaris*—UltraSparc IIi 650 *Mobile*—Pentium II+ PocketPC, Advanced Reduced Instruction Set Computer Machine, Intel x86 Smartphone, or PDA
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	Avira GmbH (Germany)
Availability	*http://www.avira.com/en/products/index.html*

AxBx Software Solutions VirusKeeper 2009

Abstract

VirusKeeper provides a real-time threat detection engine that monitors all executing processes and programs in memory, system files, registry, and input/output ports for suspicious activity. VirusKeeper® is compatible with other anti-malware software, enabling users to increase the effectiveness of their malware detection and removal countermeasures.

VirusKeeper 2009	
Type	Suspicious process detection and monitoring
OS	Windows
Hardware	
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	AxBx Software Solutions (France)
Availability	*http://www.viruskeeper.com/us/index.htm*

Beijing Rising International Software Rising Antivirus 2009

Abstract

Rising Antivirus protects PCs against viruses, Trojans, worms, rootkits, and other malicious programs by monitoring both active files and inbound (POP3) and outbound (simple mail transfer protocol [SMTP]) email messages and attachments, as well as Web communications (the tool automatically blocks malicious Web scripts and *HTTP-borne* viruses). The tool includes patented Unknown Virus Scan&Clean technology and patented Smartupdate technology. Users can communicate with the Beijing Rising virus lab to establish a rapid response network for quickly catching Trojans and other malware. The tool's System Reinforcement capability also monitors and protects OS vulnerabilities from exploitation by malware. Its Malicious Behavior Interceptor monitors the operational status of applications and running programs for signs of possible malicious behavior, which it blocks. The tool also scans and blocks malware on Universal Serial Bus (USB) media, CDs, DVDs, and network drives. The tool can be integrated with instant messengers, download managers, and other utilities and applications. Beijing Rising also offers an online "Express Edition" virus-scan-as-a-service using its Rising Antivirus software to systems running Internet Explorer® (IE); this service requires installation of an ActiveX application provided by Beijing Rising.

Rising Antivirus

Type	Malware detection and removal
OS	Windows 2000, XP, 2003, Vista
Hardware	*Vista*—1 Gigahertz (GHz) CPU (32- or 64-bit), 512 MB RAM (up to 4 Gigabyte [GB]); *Other OS*—Pentium 500 MHz, 64 MB RAM; *All*—SVGA monitor with 24-bit true color
License	Commercial (freeware version available; see Rising PC Doctor in Section 4.3.1.2)
NIAP Validated	No
Common Criteria	
Developer	Beijing Rising International Software Co., Ltd. (China)
Availability	*http://www.rising-global.com/products/Rising-Antivirus-2009.html*

BitDefender AntiVirus 2009, GameSafe, and Mobile Security v2

Abstract

AntiVirus 2009 uses separate scanning engines for different types of files and malware. These plug-ins are loaded on-demand as file systems or malware types are observed on the system. By leveraging a modular architecture, BitDefender's AntiVirus products can be run across a wide range of environments, including mobile devices.

AntiVirus 2009 scans all Web, email, and instant messaging traffic for viruses and spyware, updates itself hourly to ensure near-real-time detection, and uses heuristics to proactively protect against new virus and spyware outbreaks.

AntiVirus 2009 also includes a number of other cyber security features, such as anti-spam and anti-phishing protection, intended to reduce risks associated with Internet usage (and, in GameSafe, online gaming) that can make it easier for malicious code to enter a system.

BitDefender includes the same core anti-virus technology in its other standalone AntiVirus products, including—

- **Mobile Security v2**—provides virus scanning for mobile devices running the Symbian or Microsoft® Windows Mobile® OS;
- **GameSafe**—intended for use on computers used in online computer gaming. It adds to the BitDefender® AntiVirus capability the ability to detect and remove rootkits;
- **Free Edition**—a "lightweight" version of AntiVirus 2009 that provides the same anti-virus capabilities, but none of the additional cyber security features of AntiVirus 2009. Free Edition provides an on-demand and schedule-driven virus scanner that uses the same scanning engines and quarantine capabilities found in other BitDefender products.

BitDefender's anti-virus technology is also included in the company's multifunction Internet Security and Total Security cyber security and enterprise security management suites, and is used by BitDefender® Online Scanner (described in Section 4.3.7).

AntiVirus 2009	
Type	Virus and spyware detection and removal
OS	Windows XP, Vista, Home Server
Hardware	800 MHz CPU; 256 MB RAM for XP (512 MB recommended), 512 MB for Vista or Home Server (1 GB recommended); 170 MB free disk space (200 MB recommended)
License	Commercial (freeware option available with Free Edition)
NIAP Validated	No
Common Criteria	
Developer	BitDefender (Romania)
Availability	*http://www.bitdefender.com/PRODUCT-2216-en--BitDefender-Antivirus-2009.html* *http://www.bitdefender.com/PRODUCT-14-en--BitDefender-Free-Edition.html*

GameSafe	
Type	Virus, spyware, and rootkit detection and removal
OS	Windows 2000 with Service Pack 4; XP with Service Pack 2 (32/64 bit); Vista (32/64 bit)
Hardware	
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	BitDefender (Romania)
Availability	*http://www.bitdefender.com/PRODUCT-2213-en--BitDefender-GameSafe.html*

Mobile Security v2

Type	Virus detection and removal
OS	*AntiVirus*—Windows Mobile PocketPC 2002 and higher; Mobile Smartphone 2002 and higher; Symbian® 60 7.x/8.x; Symbian 80 7.x *Note: Symbian 60 9.x is not supported.* *PC Update Module*—Windows® 2000 or XP
Hardware	*AntiVirus software*—HP iPAQ 1915, HP iPAQ 3115, Dell Axim® x50v, T-Mobile MDA, Qtek S200, *etc.*; Motorola MPx220, Orange SPV C600, *etc.*; Nokia 3230, 6600, 6680, N70, N90, *etc.*; Nokia 9300, 9500, *etc.* *Note: The following Nokia phones are not supported—3250, 5500, 6290, E50, E60, E70, N91, N95* *PC Update Module*—Pentium MMX 200 MHz; 64MB RAM Memory (128MB recommended); 40 MB free disk space
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	BitDefender (Romania)
Availability	*http://www.bitdefender.com/PRODUCT-2149-en--BitDefender-Mobile-Security-v2.html*

CA [9] Anti-Virus Plus Anti-Spyware 2009

Abstract

This tool packages the CA Anti-Virus 2009 and Anti-Spyware 2009 products into a single integrated application. These tools are described individually in Sections 4.3.2 and 4.3.3.

Anti-Virus Plus Anti-Spyware 2009

Type	Malware detection and removal
OS	Windows 2000, XP, or Vista
Hardware	300 MHz CPU (800 MHz for Vista), 256 MB RAM (512 MB for Vista), 35 MB free disk space
License	GNU [10] Public License (GPL)
NIAP Validated	No
Common Criteria	
Developer	CA
Availability	*http://shop.ca.com/virus/anti-virus_plus.aspx*

Central Command Vexira® Antivirus

Abstract

Vexira Antivirus provides real-time protection of computers against viruses, worms, Trojans, adware, spyware, and hostile ActiveX and Java applications. The tool runs in interactive and automatic modes and performs both signature-based and heuristic virus scanning with definable levels. On UNIX/Linux, the tools performs multi-thread virus scanning, enables users/administrators to enable/disable boot scanning at will and use the configuration file for common task, and perform virus quarantine management *via* the command line.

Central Command offers Vexira Antivirus for Workstation/Desktop, Server, and Mail Server (including Sendmail, Milter, Postfix, Qmail, Courier, Groupwise [supported by Vexira Antivirus for Mail Server + i] and Postfix, Exim, Sendmail, SMTP/Relay [supported by Vexira Antivirus for Mail Server). Vexira Antivirus for Workstation/Desktop scans email messages and attachments and intercepts and scans Internet-accessed Web pages before allowing them to be rendered in the user's browser. The tool also enables users/administrators to lock down the tool's configuration, preventing tampering with or modification to the tool's preset data security profile. The Central Management Solution enables Vexira Antivirus for Windows Workstation/Desktop clients at several physical sites to be centrally managed from a single management station.

Vexira Antivirus

Type	Malware detection and removal
OS	*For Workstation/Desktop*—Windows 98, ME, NT, 2000, XP; *for Windows Server*—Windows NT 4 Server, 2000 Server, 2003 Server; *for Novell Server*—Netware 4.1+ latest Support Pack; Groupwise version requires Groupwise 5.x; anti-spam capabilities requires Novell Netware 5.1+ latest Support Pack 4 or Netware 6 Support Pack 1; *for Samba Server*—Linux (i386) glibc 2.2.5 Kernel 2.2.1+; SunOS 5.7+; Solaris 7+ with Samba 2.2.1-3.0.11 (Samba 2.2.1-2.2.2 need export symbols); *for Solaris Server*—Sun Solaris 9 or SunOS 5.9; *for Advanced Interactive eXecutive (AIX®) Server*—AIX 4.3.3, 5.2 + Maintenance level 10; *for Linux/UNIX Server*—Linux (glibc 2.2.5, kernel 2.2.x), FreeBSD 4.9 or 5.3,, OpenBSD 3.4 or 3.6; *for Mail Server* (Postfix, Exim, Sendmail, SMTP/Relay)—Linux (i386) glibc 2.2.5 Kernel 2.2.1+, FreeBSD 4.9, 5.3, OpenBSD 3.4, 3.6, Sun Solaris 9 / SunOs 5.9, AIX 4.3.3 + Maintenance level 10; for Mail Server + i—Linux (i386) glibc 2.2.5 Kernel 2.2.1+; FreeBSD 4.9, 5.3 (2005 version only); OpenBSD 3.4, 3.6; AIX 4.3; Solaris. Sendmail from version 8.12; Qmail from version 1.03; Groupwise 7 (on Linux); *Central Management Solution*—Windows NT 4 Server, 2000 Server, 2003 Server; Microsoft Jet 4 database engine required
Hardware	*Versions for Windows/NetWare*—Intel-compatible 200 MHz+ CPU, 64 MB RAM, 30 MB free disk space (Groupwise version requires 40 MB); *for Samba Server*— Intel-compatible 300 MHz+ CPU or Ultra SPARC IIe 500 MHz, 64 MB RAM (Intel)/128 MB RAM (SPARC), 30 MB free disk space; *for Solaris Server*—UltraSparc IIe 500 MHz, 128 MB RAM, 10 MB free disk space; *for AIX Server*—PowerPC II (G3), 256 MB RAM, 10 MB free disk space; *for Linux/UNIX Server*—Pentium 200 MHz CPU, 32 MB RAM, 10 MB free disk space; *for Mail Server on Linux*—Pentium 200 MHz with 32 MB RAM; On Solaris—UltraSparc IIe at 500 MHz with 128 MB RAM; *for Mail Server on AIX*—PowerPC II (G3) with 256 MB RAM; All—50 MB free disk space; f*or Mail Server + i*—Pentium 300 MHz, 128 MB RAM, 32 MB free disk space; *Central Management Solution*—Pentium 400MHz, 128 MB of RAM, 150 MB free disk space + 2 MB of temporary space
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	Central Command, Inc.
Availability	*http://www.centralcommand.com*

ClamWin Free Antivirus 0.95.1

Abstract

Free Antivirus features a high detection rate for viruses and spyware *via* on-demand and scheduled scans. Free Antivirus uses ClamAV® (described later in this section) as its anti-virus engine, to which it adds a Windows-based interface for ease of use. The product provides both on-demand and scheduled scans for viruses and spyware.

Free Antivirus 0.95.1

Type	Virus detection and termination
OS	Windows® 98, ME, 2000, XP, 2003, Vista
Hardware	
License	Freeware
NIAP Validated	No
Common Criteria	
Developer	ClamWin Pty. Ltd. (Australia)
Availability	*http://www.clamwin.com*

Comodo Security Solutions BOClean

Abstract

BOClean automatically detects and removes malware from memory, hard disks, and registries. BOClean installs itself as part of the OS, allowing it to detect and prevent malware from installing itself instantaneously. BOClean comes with the following features—

- Destroys malware and removes registry entries;
- Does not require a reboot to remove all traces;
- Disconnects the threat without disconnecting the system from the network;
- Generates optional report and a safe copy of evidence;
- Automatically scans in the background;
- Configurable "Stealth Mode" hides BOClean from users;
- Updates automatically from a network file share;
- Protects itself from tampering and shutdown by malware;
- Daily malware database updates from Comodo's Web site;
- Update file can be shared/pushed from a central server to ease maintenance;
- Enables optional rollback to earlier versions of the tool.

Comodo also includes BOClean in its Internet Security tool suite.

BOClean

Type	Malware detection and removal
OS	Windows 2000 and XP (all versions)
Hardware	
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	Comodo Security Solutions, Inc.
Availability	*http://www.comodo.com/boclean/boclean.html*

CurioLab Exterminate It!

Abstract

Exterminate It! performs comprehensive detection and removal of worms, Trojans, rootkits, and other malware, including the most recent and previously unknown (undetected) threats. Exterminate It! includes "Submit State" functionality, which enables the user to generate and submit detailed info on the state of his/her PC to CurioLab, which will include a remedy for the detected malware in the next database update (database updates are sent to subscribers every 24 hours).

Exterminate It!	
Type	Malware detection and removal
OS	Windows 2000, XP, Vista
Hardware	
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	CurioLab
Availability	*http://www.exterminate-it.com*

Doctor Web Dr.Web Anti-virus

Abstract

Dr.Web Anti-virus detects viruses, Trojans, spyware, all known rootkits, stealth viruses, and other types of malware. The tool can be launched from a removable medium (CD or USB drive) without being installed on the target system. It can then operate on even an infected computer, to scan boot sectors, RAM, hard drives, and removable drives, and sanitize infected files, restoring them to their original state instead of deleting them, without use of additional utilities. The tool's virus databases can be updated during installation, and can be set to update automatically, on demand, or according to a schedule.

Dr.Web Anti-virus includes SpIDer Mail, which scans mail traffic "on the fly" to ensure that only clean messages are forwarded to recipients, free of malicious code or infected attachments. The Virus activity control feature protects a system against mass mailings performed by mail worms. SpIDer Mail examines components of a message and considers sending time to determine if an outgoing message is a part of malicious activities in a system. Individual rules can be created for different types of malicious programs, including viruses, riskware, adware, hack tools, paid dialers, and jokers. SpIDer Mail supports SMTP, Post Office Protocol (POP), Network News Transfer Protocol (NNTP), and Internet Message Access Protocol (IMAP) mail protocols.

The tool comes in versions for Windows, Linux, Novell NetWare, Windows Mobile, and a package for Windows + Linux. The tool also comes in versions for email servers, including Microsoft Exchange, IBM Lotus Domino, UNIX mail systems (multiple), and ClearSwift MIMEsweeper. There are also Dr.Web Antivirus products for SMTP Web Mail gateways and Internet gateways. Dr.Web's Antivirus software is also included in their more extensive Security Space and Enterprise Suite cyber security products. Dr. Web also provides console scanners are available for older OSs, including Microsoft Disk Operating System (DOS), OS/2, and older versions of Windows.

Dr.Web Anti-virus

Type	Malware detection and removal
OS	*Windows*—Windows 95, 98, ME, NT, 2000, XP, Vista (32-bit only) *Linux*—All distributions with glibc-2.2-2.7 (32-bit only). *NetWare*—NetWare v.3.12-6.5 *Windows Mobile*—Windows Mobile 2003, 2003 SE, 5.0, 6.0-6.1 *Exchange, Lotus Domino, MIMEsweeper*—Windows Server 2000, 2003, or later *UNIX Mail*—All distributions with glibc 2.2-2.7 *Web Mail, UNIX Internet gateway*—All distribution with glibc 2.2-2.7, FreeBSD 4.x+, Solaris 10 *Kerio WinRoute Internet gateway*—Windows 2000, XP, 2003, 2008
Hardware	*Linux*—2.5 MB free disk space *NetWare*—25 MB RAM + 25 RAM for each extra scanning process, 20 MB free disk space *Windows Mobile*—any Communicator or PocketPC running Win Mobile OS *Exchange*—Pentium 133 MHz (733 MHz recommended), 256 MB RAM (512 MB recommended), 20 MB free disk space (+50 MB for logs, 500 MB for log archives) *Lotus Domino*—Pentium 133, 64 MB RAM (128 MB recommended), 20 MB free disk space *MIMEsweeper*—35 MB free disk space *Kerio WinRoute Internet gateway*—30 MB free disk space *Note: Solaris 10 supported on Pentium only, not on SPARC.*
License	Commercial [11]
NIAP Validated	No
Common Criteria	
Developer	Doctor Web Ltd. (Russian Federation)
Availability	*http://products.drweb.com/win/choose*

DriveSentry SecuritySuite and GoAnywhere

Abstract

DriveSentry provides anti-virus, anti-malware, and anti-spyware protection for PCs and for removable storage devices (such as USB memory keys, portable drives, flash cards), and network drives. Subscribers receive real-time signature updates (lifetime—no subscription required). SecuritySuite and GoAnywhere recognize over one million unique malware signatures, and automatically block and quarantine known viruses, Trojans, and malicious code. The tool's patented Tri-Security technology detects the latest threats that bypass traditional security software even without regular signature updates.

Users are also able to control which applications and software access their systems and personal data *via* combined white-listing technology and real-time black-listing advice from the DriveSentry Advisor Community; this ensures that only trusted programs can access the protected PC or device and prevents damage from zero day threats that go undetected by conventional anti-virus software.

SecuritySuite also provides "drag and drop" Advanced Encryption Standard (AES) 256-bit data encryption, file synchronization, and backup of data stored on removable devices to PC.

SecuritySuite and GoAnywhere

Type	Malware detection and removal
OS	*SecuritySuite*—Windows 2000, XP, Server 2003, Vista
Hardware	*Devices supported*—compact Flash, SecureDigital (SD) card, Sony MagicGate, iPod®, other memory cards, media players, mobile phones, digital camera media, removable PDA memory. USB flash drives.
License	*SecuritySuite*—Commercial; *GoAnywhere*—Freeware
NIAP Validated	No
Common Criteria	
Developer	DriveSentry, Inc.
Availability	*http://www.drivesentry.com/drivesentry-security-suite.html* *http://www.drivesentry.com/AntiVirus-Firewall-gofeatures-for-computers-and-removable-media.html*

Emsi Software A-squared

Abstract

A-squared relies on both signature-based and behavior-based detection to identify malware on users' systems. A-squared blocks access to known-malicious Web sites and provides signature updates at least five times per day to ensure that users' protection is fully up-to-date. A-squared uses the Malware Intrusion Detection System (available as a pure malware detection tool as Mamutu), which does not rely on heuristics. The Malware Intrusion Detection System watches important system files and gives the user the option to allow or deny any changes to those files.

A-squared	
Type	Malware detection and removal; Behavior analysis for malware indicators
OS	Windows XP and later
Hardware	
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	Emsi Software, GmbH (Austria)
Availability	*http://www.emsisoft.com/en/software/anti-malware*

Emsi Software Mamutu 1.7.0.27

Abstract

Mamutu monitors all active programs for dangerous behavior, and recognizes and blocks all potentially dangerous programs, including new, zero-day, and unknown Trojans, worms, and viruses for which signatures are not yet available. Mamutu's behavior-based detection and analysis does not use a fingerprint or signature to recognize dangerous software, but rather detects it on the basis of the behavior of the software. This approach enables Mamutu to recognize new malware without daily updating of the tool, and long before other tools' signature databases have been updated.

Mamutu 1.7.0.27

Type	Malware detection and removal
OS	Windows 2000, XP, 2003 Server, Vista
Hardware	
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	Emsi Software GmbH (Austria)
Availability	*http://www.mamutu.com/en/software/mamutu*

ESET® NOD32® Antivirus

Abstract

NOD32 Antivirus 4 provides comprehensive protection against viruses, Trojans, worms, adware, spyware, rootkits, and other malware threats. The tool's ThreatSense® technology provides protection against novel and unknown threats. In addition to scanning standard Web and email channels, NOD32 Antivirus inspects secure sockets layer (SSL)-encrypted communication channels (*e.g., HTTPS* and POP3S) and scans compressed files to find hidden threats. The tool provides email scanning for Microsoft Outlook®, Outlook Express, Mozilla® Thunderbird®, Windows Live Mail, Windows Mail, and other POP3/IMAP mail clients.

For self-running media, NOD32 Antivirus scans *autorun.inf* and associated files when the medium is inserted, as well as any file on any removable device when it is accessed, or during a full-scan of the media. Users can adjust NOD32 Antivirus to perform additional customized and on-demand scans of removable media.

The tool also includes SysInspector and SysRescue functions for diagnosis and sanitization of infected systems *via* deep scans of system processes to find hidden threats, and creation of a bootable rescue CD/DVD or USB drive to help in the repair of an infected computer. The tool's built-in Self Defense technology prevents malicious software from corrupting or disabling the tool itself.

The Business Edition of NOD32 Antivirus includes all the features described above plus host-based intrusion prevention, remote administration *via* a single console, external drive access control and scanning, Cisco® Network Admission Control compatibility, and enhanced logging and reporting functions to support compliance requirements.

The Mobile Antivirus version detects, quarantines, and removes known viruses, spyware, adware, Trojans, worms, rootkits, and other unwanted software carried by email attachments and other files accessed *via* wireless links (*e.g.,* Bluetooth, WiFi, General Packet Radio Service, Enhanced Data rates for Global system for mobile Evolution) by smartphones and PocketPCs. Heuristic-based detection protects against unknown threats between signature updates. Mobile Antivirus scans memory and running processes, onboard files, and removable media. It also enables use of whitelists and blacklists to blocks text messages and short message service (SMS) spam from unknown and unwanted senders. Mobile Antivirus has low CPU, memory requirements, and compact updates that minimize data bandwidth usage. Signature updates can be downloaded on-demand or at pre-set intervals (daily, weekly, monthly).

NOD32 Antivirus

Type	Virus and anomaly detection and termination
OS	*Antivirus 4*—Windows 2000, XP, Vista (32-/64-bit) *Antivirus 4 Business Edition*—Windows 2000 Professional and Server 2000, Server 2003, Server 2008, XP, Vista (32-/64-bit) *Mobile Antivirus*—Windows Mobile 5.0, 6.0, 6.1
Hardware	*Antivirus 4*—Intel or Advanced Micro Devices (AMD) x86/x64 CPU, 44 MB RAM, 63 MB available disk space *Mobile Antivirus Tested on*—HP iPAQ 116 PDA, HTC Advantage/Faraday (Cingular® 2125, unlocked)/Touch (Verizon XV6900)/ TyTN® (Cingular 8525)/TyTN II (AT&T Tilt), Palm Treo® 750, Pantech® Duo (unlocked), Samsung BlackJack II (unlocked), Sony Xperia® X1 (unlocked), UTStarcom® XV6700 (Verizon® XV6700), XDA Atom Life *All*—1 MB RAM *Note: Incompatible with Asus® MyPal A696 PDA, iMate SPL (PhoneOne S101), Samsung SGH-i900 (Fplayer Addict)*
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	ESET (Slovakia)
Availability	*http://www.eset.com/products/nod32.php* *http://www.eset.com/products/mobileantivirus.php*

Filseclab Twister Anti-TrojanVirus

Abstract

Twister Anti-TrojanVirus is an anti-Trojan, anti-virus, anti-rootkit, and anti-spyware tool that uses a combination of signature-based scanning and behavior analysis to detect Trojans, spyware, viruses, hackers, adware, and other malware threats. It supports the Windows Security Center and right-click scanning from the Explorer context menu. It supports scanning of files compressed using the following compression formats: zip, rar, ace, cab, chm, and eml. Twister's Registry Protector protects the PC's Windows registry in real time, and its Registry Fix Tools can quickly fix many frequently occurring problems in Windows and IE. The Spyware Removal Assistant utility simplifies removal of stubborn Trojans and spyware. The virus definition live update and automatic update enables the tool to detect and remove the most recent Trojans, spyware, and viruses.

Twister Anti-TrojanVirus

Type	Malware detection and removal
OS	Windows
Hardware	
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	Filseclab (China)
Availability	*http://www.filseclab.com/eng/products/twister.htm*

Finport Technologies Simple Antivirus v2.1 and Corporate v2.4 Beta

Abstract

Simple Antivirus detects all known viruses, worms, adware, spyware, and other malware and monitors RAM and file system for malware-related activity. Updating the virus definition database can be performed *via* a direct network connection to the virus definitions database or through a proxy-server.

Simple Antivirus

Type	Malware detection
OS	Windows XP and Vista
Hardware	
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	Finport Technologies (Ukraine)
Availability	*http://www.simple-avr.com.ua/*

FireEye® 4200 Web Malware & Botnet Security System

Abstract

The FireEye 4200 is a self-contained, rack-mountable network security appliance that detects botnets and Web-based malware, including malware that uses techniques like polymorphism and obfuscation. Using the FireEye Analysis & Control Technology engine, the FireEye 4200 can analyze real-time network traffic replayed within virtual machines to accurately detect zero-day malware and botnets, and to capture inbound malware forensics to aid in infection analysis and remediation. Outbound callback fingerprinting enables identification of previously infected PCs calling out to malicious parties. The appliance connects to the FireEye Malware Analysis & Exchange Network to gain additional signatures, callback coordinates, and botnet intelligence.

FireEye 4200 Web Malware & Botnet Security System

Type	Malware and botnet detection and removal
OS	n/a
Hardware	n/a
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	FireEye, Inc.
Availability	*http://www.fireeye.com/products/index.html*

F-Secure Anti-Virus 2009

Abstract

Anti-Virus 2009 includes an anti-virus tool, anti-spyware tool, and a personal firewall to protect computer systems against malware. Leveraging F-Secure's DeepGuard 2.0 technology, which uses network-enabled pre-recognition of malicious and benign software, Anti-Virus 2009 aims to reduce the level of user interaction required to protect against unknown malware outbreaks.

F-Secure also includes Anti-Virus 2009's capabilities in its Internet Security 2009 product, which adds a Web firewall that prevents browsers from connecting to malicious Web sites—thereby avoiding the installation of malicious code *via* "drive-by downloads."

Anti-Virus 2009

Type	Virus and spyware detection and removal
OS	Windows 2000, Vista (32- and 64-bit), XP
Hardware	*XP/2000*—Pentium III 600 MHz or higher, 256 MB RAM; 600 MB available disk space; high-speed Internet connection *Vista*—512 MB RAM; 600 MB available disk space; high-speed Internet connection
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	F-Secure Corporation (Finland)
Availability	*http://www.f-secure.com/en_EMEA/products/home-office/antivirus*

Greatis Software UnHackMe 5.0

Abstract

The main difference between UnHackMe and other anti-rootkit software is the detection method. UnHackMe tries to detect the hidden rootkits by watching the computer from early study of the boot process until the normal Windows mode. Most modern anti-rootkit programs try to detect the rootkits when the rootkit is already active. They use the very complex methods for detecting hooked system functions, but the rootkit author creates the new tricks, and the process repeats.

UnHackMe 5.0

Type	Malware detection and removal
OS	Windows 2000/2003/XP/Vista; Windows NT 4.0 may or may not still be supported
Hardware	Pentium 100 CPU or better with 8 MB RAM and 1-2 MB of free disk space
License	Commercial (older version free with registration). *Available licenses*—single user, family, business, family+business, roaming, and professional
NIAP Validated	No
Common Criteria	
Developer	Greatis Software (Russian Federation)
Availability	*http://www.greatis.com/unhackme/download.htm*

HAURI ViRobot Desktop 5.5, GatewayWall, Exchange 3.0, Windows Server 3.5, SDK

Abstract

ViRobot performs real-time monitoring and filtering of email, IM, files, and Internet transmissions found to contain viruses, worms, spam, malicious scripts, *etc.* Its Viruswall function enables virus scanning and logging policy to be configured at the shared folder, process, or network level. The tool also detects and removes spyware and adware. The tool includes quarantine functions that move infected files and email messages, as well as spam messages, to a secure isolated area. Finally, the tool performs vulnerability analyses to ensure that the system's patches are all up to date, to minimize the presence of vulnerabilities that are exploitable by malware.

ViRobot GatewayWall blocks spam and virus-infected email at the mail server to prevent them from ever reaching the user's desktop. The tool can scan 14 compression file types, including .zip, .jar, .lha, .rar, .cab, .ace, .zoo, .gz, .tar, .z, .tgz, and .taz, as well as UUencoded and MIME-encoded email attachments, at each level of compression or encoding of multi-compressed/multi-encoded files. When viruses are found, they are removed at all levels. ViRobot Exchange provides comparable functions on Microsoft Exchange mail servers, on which ViRobot's anti-virus engine is tightly integrated with Microsoft's virus scanning API (2.0 or 2.5); the tool scans mail transmitted by all major protocols, including SMTP, MAPI, HTTP (Webmail), POP3, and IMAP4, and supports all mail clients using those protocols, including Outlook Express, and Outlook.

ViRobot Windows Server 3.5 performs comparable virus detection for files stored on Windows file servers

ViRobot Software Development Kit (SDK) enables developers or integrators to port, customize, and/or integrate (*e.g.,* with IE-mail, USB mass storage, other data storage, knowledge management, electronic document management systems, Web servers, firewalls, proxy servers, groupware) ViRobot's anti-virus engine, quarantining, and other function modules.

ViRobot Desktop 5.5, Gateway Wall, Exchange 3.0, Windows Server 3.5, SDK

Type	Malware detection, blocking, and quarantine
OS	*Desktop*—Windows Vista, XP, 2000, NT, running IE 6.0, TCP/IP networking; *GatewayWall*—Windows 2000 Server or 2003 Server, Linux, UNIX; *Exchange*—Windows 2000 Server/Advanced Server/ Exchange Server, Windows Server/ Exchange Server 2003; *Windows Server*—Windows Server 2000, 2003, 2008, IE 5.5, TCP/IP networking; *SDK*—HP-UX 11.x, AIX 3.x.x, FreeBSD, Solaris v5-v8, Linux 6.x-7.x, Windows (XP, 2000, NT 4.0)
Hardware	*Desktop*—Pentium III 500 MHz, 512 MB RAM, 300 MB free disk space; *GatewayWall*—Pentium III 800 MHz, 256 MB RAM, 1 GB free disk space, mouse, CD drive, network connection; *Exchange*—Pentium 500 MHz, 256 MB RAM, 100 MB free disk space, CD drive, network connection; *Windows Server*—Pentium III 300 MHz, 256 MB RAM, 800 MB free disk space
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	HAURI Inc. (Korea)
Availability	*http://www.hauri.net/product*

iolo® AntiVirus

Abstract

iolo AntiVirus provides integrated email protection that automatically scans inbound and outbound email messages for viruses, worms, Trojans, and other malware threats, and removes discovered malware from infected messages. AntiVirus also performs on-demand, full-system anti-virus scanning to find and remove malware that is already installed and running on the PC. iolo® provides hourly updates to their virus threats database.

iolo AntiVirus	
Type	Malware detection and removal
OS	Windows 2000, SP, Vista
Hardware	256 MB RAM, 30 MB available hard disk, CD or DVD drive, Internet connection
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	iolo technologies, LLC
Availability	*http://www.iolo.com/ss/*

Jiangmin Antivirus Software KV2009

Abstract

KV2009 provides a "highly optimized" anti-virus engine and a combination of proactive defense techniques that enable it to detect and remove over one million kinds of viruses, including Trojans, worms, backdoors, spyware, and hijackers. Its "Anti-Trojan for Webpage" feature prevents PCs from visiting Web pages that might infect them.

Jiangmin also offers a version of their product for removable devices (Moving Picture Experts Group [MPEG] audio layer Three [MP3] players, USB Flash disks, removable storage devices) and for smartphones (viruses spread *via* multimedia dissemination protocols).

Antivirus Software KV2009

Type	Malware detection and removal; malicious site blocking
OS	Windows NT, 2000, XP, ME, Server 2003, Vista
Hardware	*XP*—Pentium 800 MHz, 256 MB RAM *Vista*—Pentium 800 MHz 32 bit (x86)/64 bit (x64), 512 MB RAM *All*—50 MB free disk space; CD-ROM drive, computer mouse, Internet connection
License	Commercial (freeware version available)
NIAP Validated	No
Common Criteria	
Developer	Jiangmin SciTech (China)
Availability	*http://global.jiangmin.com/productskv.htm*

K7 Computing AntiVirus 7.0

Abstract

AntiVirus 7.0 scans PCs and email to detect viruses, worms, Trojans, spyware, and adware, with potential threats cross-referenced with the latest virus databases. AntiVirus 7.0 makes regular automatic updates and background system scans. All new files accessed, downloaded, created, or modified are automatically scanned in real time. The anti-spyware feature prevents unwanted programs from installing themselves without user approval. Additional anti-malware functionality stops the installation of malware such as Trojans, worms, rootkits, adware, and keylogger exploits.

AntiVirus 7.0

Type	Malware detection and removal
OS	Windows 98 2nd Edition, ME, 2000 Professional, XP, Vista
Hardware	128 MB RAM, 60 MB free disk space, Internet connection
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	K7 Computing (India)
Availability	*http://www.k7computing.com/index.php/anti-virus/k7-antivirus-70.html*

Kaspersky® Anti-Virus 2009

Abstract

Anti-Virus 2009 provides anti-virus and anti-spyware protection to guard against viruses, Trojans, and worms, spyware , adware, and rootkits, as well as identity theft and phishing attacks. Features include—

- Scanning of files, email, and internet traffic;
- Protection for instant messengers;
- Protection against unknown threats;
- Analysis and remediation of IE vulnerabilities;
- Disabling of links to known malware and phishing sites;
- Global threat monitoring provided *via* Kaspersky® Security Network;
- Blocking of all types of keyloggers;
- Automatic updates of the tool's signature database.

Kaspersky Lab also includes its anti-virus technology in its Internet Security, Mobile Security, and Security for Ultra Portables products.

Anti-Virus 2009

Type	Malware detection and removal
OS	Windows XP, Vista
Hardware	*XP*—Pentium 800 MHz, 256 MB RAM *Vista*—Pentium 800 MHz 32 bit (x86)/64 bit (x64), 512 MB available RAM *All*—50 MB free disk space, CD-ROM, computer mouse, Internet connection *Note: Optimized for Intel Centrino® Duo.*
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	Kaspersky Lab (Russian Federation)
Availability	*http://usa.kaspersky.com/store*

Lavasoft® Ad-Aware®

Abstract

All commercial versions of Ad-Aware protect against viruses, spyware, Trojans, worms, malware, rootkits, dialers, and other malware. Ad-Aware Free protects only against spyware/adware. Ad-Aware's Pro core engine uses behavior-based heuristic detection techniques. The tool also blocks outbound connections to blacklisted IP addresses (*i.e.,* of known malicious Web sites) and blocks or suspends malicious processes and infected files detected on the system. Ad-Aware detects attempted registry changes and alerts the user when a program tries to make changes to the Registry, allowing the user to block the threat or allow access.

The tool scans not only the local system, but also any connected external storage devices, iPods, DVDs, USBs, or network drives. On-demand scans can be pinpointed down to the individual file level. The tool performs detection, removal, and clean-up after removal of malware.

Ad-Aware includes a rootkit removal system. The tool comes with the Lavasoft Toolbox of monitoring and reporting tools and system utilities. Ad-Aware's database includes over two million known threats, and provides continuous pulse updates.

Lavasoft offers Ad-Aware in four different packages—

- **Ad-Aware Plus**—Includes adware detection and removal and anti-virus protection;
- **Ad-Aware Pro**—Also includes adware detection and removal and anti-virus protection;
- **Ad-Aware Enterprise 2.1**—Proactively blocks and safely eliminates spyware, viruses, Trojans, rootkits, and other malware without slowing down the network;
- **Ad-Aware Free**—Provides only adware detection/removal.

Ad-Aware

Type	Malware detection, blocking, and removal
OS	*Enterprise 2.1 Client*—Windows Vista, XP, Server 2003, 2000 Pro *Enterprise 2.1 Server*—Windows 2000 Pro, 2000 Server, 2003 Server, XP *Enterprise 2.1 Console*—Windows Vista, XP, Server 2003, 2000 *Pro, Plus, Free*—Windows Vista, XP, 2000 Pro
Hardware	*Enterprise 2.1 Client*—Pentium P600, OS RAM + 150 MB, 150 MB free disk space *Enterprise 2.1 Server*—OS RAM+24 MB, 200 MB free disk space *Pro, Plus, Free*—Pentium 600 MHz, OS RAM+100 MB, 100 MB free disk space
License	Commercial (freeware version available)
NIAP Validated	No
Common Criteria	
Developer	Lavasoft AB (Sweden)
Availability	*http://www.lavasoft.com/products/ad_aware.php*

Lavasoft Anti-Virus Helix

Abstract

Anti-Virus Helix performs heuristic detection, quarantine, and removal of viruses, worms, Trojans, adware, and rootkits, and real-time detection of cyber threats such as botnets, phishing attempts, and drive-by downloads.

Anti-Virus Helix	
Type	Malware detection, blocking, and removal
OS	Windows 2000, XP, Vista
Hardware	Pentium 133 MHz, OS RAM+100 MB, 40 MB free disk space
License	Commercial (freeware version available)
NIAP Validated	No
Common Criteria	
Developer	Lavasoft AB (Sweden)
Availability	*http://www.lavasoft.com/products/lavasoft_anti-virus_helix.php*

Malwarebytes® Anti-Malware 1.37

Abstract

Malwarebytes Anti-Malware application is designed to quickly detect, destroy, and prevent malware. By monitoring every process, Anti-Malware can detect and prevent malicious processes from running immediately after they are launched. Anti-Malware is available in both a free and commercial version. The free license allows users to perform on-demand malicious code detection and removal, while the commercial license allows users to take advantage of real-time protection as well as support for scheduled scans.

Anti-Malware 1.37

Type	Malware detection and removal
OS	Windows 2000, XP, Vista
Hardware	
License	Commercial (freeware version available)
NIAP Validated	No
Common Criteria	
Developer	Malwarebytes Corporation
Availability	*http://www.malwarebytes.org/mbam.php*

Microsoft Forefront Client Security

Abstract

Microsoft's Forefront Client Security is a corporate-level anti-malware suite that puts an emphasis on managing and controlling a large number of systems. Forefront Client Security provides protection against viruses and spyware while offering central management consoles that integrate with an organization's existing enterprise security management infrastructure.

ForeFront Client Security

Type	Malware detection and removal
OS	Windows XP and later
Hardware	
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	Microsoft Corporation
Availability	*http://www.microsoft.com/forefront/en/us/default.aspx*

Microsoft Windows Malicious Software Removal Tool

Abstract

The Windows Malicious Software Removal Tool checks computers running Windows for infections by specific, prevalent malicious software and helps remove any infection found. When the detection and removal process is complete, the tool displays a report describing the outcome, including which, if any, malicious software was detected and removed.

Microsoft releases an updated version of this tool on the second Tuesday of each month, and as needed to respond to security incidents. The tool is available from Microsoft Update, Windows Update, and the Microsoft Download Center. The version of the tool delivered by Microsoft Update and Windows Update runs in the background and then reports if an infection is found. Customers who wish to run the tool more than once a month need to use the version available from the Web page listed below or to install the version that available from the Download Center.

Windows Malicious Software Removal Tool

Type	Malware detection and removal
OS	Windows Vista, XP, 2000, Server 2003
Hardware	
License	Free
NIAP Validated	No
Common Criteria	
Developer	Microsoft Corporation
Availability	*http://www.microsoft.com/security/malwareremove/default.mspx*

MicroWorld® Technologies eScan AntiVirus 9.0/10.0 and eScan for Linux 2.0

Abstract

eScan AntiVirus is a comprehensive virus solution intended to protect PCs from viruses, worms, Trojans, spyware, adware, keyloggers, rootkits, and other malware. The tool uses signature-based (with hourly updates) and heuristic scanning, and detects, monitors, and warns the user about registry changes and suspicious applications. The tool includes an on-demand scanner with caching for improved performance. The tool can scan files, applications, emails and attachments (SMTP and POP3 can be scanned in real-time), and USB drives. The tool also incorporates a PC firewall for monitoring and logging inbound and outbound network activity. eScan AntiVirus desktop editions are available for Windows and Linux (the latter recognizes over 120,000 viruses and variants). eScan also supports scanning of emails (Microsoft Outlook/Exchange .pst and .pab files, Microsoft Internet Mail .mbx files).

Licenses are available for home users, small- and medium-sized businesses, and large corporate- and enterprise-level organizations, for a variety of Windows and Linux-based desktops and servers.

eScan AntiVirus and eScan for Linux

Type	Malware detection
OS	*Windows editions*—2000, 2003 Enterprise/Standard/64-bit, 2008, XP Home/Professional/64-bit, Vista; IE 5.0; Microsoft *Small Business Server/Citrix Server edition/Proxy Server editions*—Windows 95, 98 SE/ME, NT 4.0, 2000, XP, Vista, 2008; *Linux editions*—RedHat Enterprise Linux 3/4/5 and RedHat 9, SuSe Linux Enterprise Server 9/10, Debian 3.1, Mandrake 9.2
Hardware	*Windows editions*—Pentium 200 MHz, 128 MB RAM (256 MB recommended), 150 MB free disk space, CD drive, monitor/console with 800x600 resolution; *Microsoft Small Business Server/Citrix Server/Proxy Server editions*—Pentium or AMD/Citrix 500 MHz, 128 MB RAM, 300 MB free disk space Internet connection, monitor/console with 800x600 resolution; *Linux editions*—30 MB free disk space
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	MicroWorld Technologies, Inc.
Availability	*http://www.mwti.com/products/escan/escan_antivirushomeuser/escanav_homeuser.asp* *http://www.mwti.com/products/escan/escan_linux_desktops/escan_linuxdesktops.asp* *http://www.mwti.com/products/escan/escan_antivirus_smbuser/escanav_smb.asp* *http://www.mwti.com/products/escan/escan_corporate/escancorporate.asp* *http://www.mwti.com/products/escan/escan_enterprise/escanenterprise.asp* *http://www.mwti.com/products/escan/escan_enterprise_mssbs/escan_ent_mssbs.asp* *http://www.mwti.com/products/escan/escan_citrix/escancitrix.asp* *http://www.mwti.com/products/escan/escan_linux_servers/escan_linuxservers.asp* *http://www.mwti.com/products/escan/escan_corporate_proxy/escancorporate_proxy.asp*

MIEL e-Security Labs Helios and Helios Lite

Abstract

Helios is a patent-pending malware detection system designed to detect, remove, and inoculate PCs against rootkits. Helios uses behavior-based detection, and so does not rely on a database of known signatures. This enables the tool to detect unknown malware and malware for which signature-based products do not yet have a signature definitions.

MIEL e-Security Labs' developers claim not to know whether Helios will actually detect specific instances of known malware, but they do assert that malware that exhibits behaviors of modern rootkits will be detected. Helios was not designed, however, to detect browser toolbars, dialers, and other types of malware that the tool's developers feel are adequately handled by other anti-virus products. Helios was designed to augment products, to detect advanced stealth malware that they cannot.

Helios 1.1a and Helios Lite

Type	Malware detection and removal, and behavior analysis for malware indicators
OS	Windows XP SP2 (Helios requires *Microsoft .NET* Framework 2.0; Helios Lite does not.)
Hardware	*Helios*—1 GHz CPU, 512 MB RAM *Helios Lite*—256 MB RAM
License	Freeware
NIAP Validated	no
Common Criteria	
Developer	MIEL e-Security Pvt. Ltd. (India)
Availability	*http://helios.miel-labs.com/2006/07/download-helios.html*

MooSoft Development The Cleaner 2010

Abstract

The Cleaner 2010 detects and removes Trojans, worms, keyloggers, spyware, adware, and other malware. It supports quarantining, whitelisting, advanced heuristics for unknown malware detection, and other features that have become standard in anti-malware products.

The Cleaner 2010

Type	Hidden malware detection and removal
OS	Windows® 2000, XP, Vista, Windows® 7
Hardware	
License	Commercial (freeware personal-use version available)
NIAP Validated	No
Common Criteria	
Developer	MooSoft Development, Inc.
Availability	*http://www.moosoft.com/TheCleaner/TheCleaner*

NictaTech Software Digital Patrol

Abstract

Digital Patrol is an anti-Trojan scanner that detects and eliminates more than 500,000 types of Trojan horses, viruses, worms, backdoors, porno-dialers, spyware, and malicious ActiveX® controls and Java® applets found "in the wild" spreading over the Internet. Digital Patrol deletes malware from the computer on which it is found, and performs heuristic analyses of files to detect new, previously unknown malware. The tool scans the most popular archive types and self-extracting executable files. The tool's "Rapidly Live Updating from the Internet" feature enables it to keep its anti-virus database and program components up to date.

Digital Patrol	
Type	Malware detection and removal
OS	Windows XP SP2 and Vista
Hardware	
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	NictaTech Software (Russian Federation)
Availability	*http://www.proantivirus.com/en/index.php*

NETGATE Technologies Spy Emergency 2009 Version 6.0.405

Abstract

Spy Emergency combines spyware, Trojan, virus, and spam detection and removal technologies into one solution for combating various malware threats and potentially unwanted software, including spyware, viruses, adware, Trojans, worms, spam, homepage hijackers, backdoors, remote administration tools, ActiveX components, dialers, scumware, keyloggers, data mining software, toolbars, tracking cookies, browser, hijackers/BHOs, and polymorphic malware. The tool also provides low-level anti-rootkit protection and automatic LSP stack repair.

The tool scans system memory, registry, data storage, and emails/attachments (including compressed files); it checks the last of these for malware and spam messages. Prevention shields and real-time memory shields ensure that spyware, Trojans, worms, and viruses are automatically blocked before they can execute. A browser shield (IE, Firefox, Opera) prevents drive-by downloads from malicious Web pages.

Spy Emergency includes heuristic behavioral analysis technology that runs in a virtualized environment to scans for suspicious and potentially harmful activity, detects, quarantines, and then removes unknown threats not yet in the Spy Emergency database of over 1,600,000 threat signatures.

The tool augments its graphical user interface with Shell Extension Scanning to support a command-line interface.

Spy Emergency	
Type	Malware detection, blocking, and removal
OS	Windows Vista (32-bit and 64-bit), XP (32-bit), 2000 (32-bit)
Hardware	*Desktop*—Pentium III 500 MHz, 512 MB RAM, 300 MB free disk space; *GatewayWall*—Pentium III 800 MHz, 256 MB RAM, 1 GB free disk space, mouse, CD drive, network connection; *Exchange*—Pentium 500 MHz, 256 MB RAM, 100 MB free disk space, CD drive, network connection; *Windows Server*—Pentium III 300 MHz, 256 MB RAM, 800 MB free disk space
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	NETGATE Technologies s.r.o. (Slovakia)
Availability	*http://www.spy-emergency.com/* *http://www.netgate.sk/content/view/18/41/*

Norman Security Suite, Virus Control, and Endpoint Protection

Abstract

Norman's anti-malware products feature the company's Sandbox technology, which detects and prevents execution of unwanted actions by new and unknown malware, and "DNA Matching" [12] technology, which determines whether detected programs have malicious, suspicious, or legitimate behaviors. If too much of a new program's "DNA" consists of malicious elements, DNA Matching indicates that the new program is most likely also malicious.

For their anti-spyware capability, Norman is a value-added reseller of Ad-Aware.

The complete list of anti-virus/anti-spyware products Norman offers includes—

- **Security Suite**—Virus protection recognizes, blocks, and removes viruses, worms, Trojans and other varieties of destructive program code. Spyware protection protects against malicious spyware as keyloggers, hijackers, rootkits and other malicious software jeopardizing user privacy, identity, or simply reducing computer performance. Rootkit protection provides enhanced protection, detecting and removing rootkits. Live Statistics provide an overview of files scanned and number of infections found. Proactive malware protection uses Norman SandBox technology to keep user data free from new unknown viruses, Trojans, worms, and other malicious programs. The Suite protects email, IM, Internet downloads and Web browsing. Background auto-updates are sent to all modules. A protective screensaver scans the computer for viruses and spyware when the screensaver is active. Instant file and folder scanning lets the user quickly and efficiently scan for malicious content by right-clicking a file or folder icon.
- **Virus Control**—A collection of anti-virus software applications and utilities that protect workstations, servers and gateways against malicious software, including viruses, worms, and Trojans through on-access and on-demand scanning. The Norman Internet Protection module scans incoming and outgoing email as well as files downloaded from newsgroups. Norman® offers its Virus Control product for the following platforms—
  - Virus Control for Linux,
  - FireBreak 4.5 (Virus Control) for Novell Netware,
  - Virus Control for Lotus Domino,
  - Virus Control for Exchange (for Microsoft Exchange mail servers),
  - Virus Control for AMaViS (for Linux-based mail servers that use AMaViS),
  - Virus Control for MIMEsweeper.
- **Endpoint Protection**—Endpoint malware protection combines anti-virus and anti-spyware to secure workstations, laptops, servers, and terminal servers. Virus Control recognizes, blocks and removes viruses, worm, Trojans, and other varieties of destructive program code. Anti-spyware capabilities protect against malicious spyware such as keyloggers, hijackers, rootkits, and other malicious software that jeopardizes user privacy. Rootkit protection includes a rootkit removal function.

Norman includes its anti-virus and anti-spyware capabilities in its Email Protection and Network Protection software and appliances.

Security Suite, Virus Control, Endpoint Protection

Type	Malware detection, analysis, and removal
OS	*Security Suite*—Windows Vista, XP, 2000 *Virus Control*—Windows 95, 98, ME, NT, 2000, 2003, Vista *Virus Control for Linux*—distributions with glibc v2.2+ *FireBreak 4.5 (Virus Control) for Novell Netware*—NetWare 4.11 and later *Virus Control for Lotus Domino*—Windows NT 4.0 or later, 2000, 2003 *Virus Control for Exchange*—Windows 2000, 2003 *Virus Control for AMaViS*—tested on CentOS 5.0 and Debian Etch *Virus Control for MIMEsweeper*—Windows 2000 *Endpoint Protection*—Windows 2000, 2003, XP, Vista, 2008
Hardware	*Security Suite*—450MHz Pentium *Virus Control*—Pentium
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	Norman ASA (Norway)
Availability	*http://www.norman.com/home/all_products/anti-virus/* *http://www.norman.com/smb/en-us* *http://www.norman.com/enterprise/en-us*

Norton® AntiVirus 2009 and Gaming Edition

Abstract

AntiVirus 2009 is a "for home use" product that detects and automatically removes viruses, spyware, Trojan horses, worms, bots, and rootkits. The tool includes a technology called Norton Insight, which enables it to scan only for files and processes at risk of malware infection. The tool is also able to scan emails and instant messages. The subscription also includes the separate Norton Recovery Tool that enables the user to reboot from the Recovery Tool disk (CD or DVD) and recover (sanitize) a severely infected PC.

AntiVirus Gaming Edition provides comparable anti-malware functionality, but adds the ability for the user to configure the tool to suspend alerts and notifications that would interrupt game play, and real-time monitoring that would reduce PC and network speed.

The tool comes with a one-year subscription to signature updates, which are downloaded to the protected PC every five to 15 minutes (or more often in some cases). In addition, the tool's real-time SONAR technology detects emerging spyware and viruses before signatures are available. Subscribers also receive one year of free technical support.

Norton®'s AntiVirus technology is also included in the company's Internet Security 2009 and Norton 360 Version 3.0 product lines, which also include network, host, and cyber security features to augment their anti-malware capabilities.

AntiVirus 2009 and AntiVirus Gaming Edition

Type	Malware detection and removal
OS	Windows Vista, XP; Mac OS X running Windows *via* Boot Camp® virtualization software
Hardware	*AntiVirus 2009*—300 MHz CPU, 256 MB RAM (512 MB with Recovery Tool), 150 MB free disk space, CD-ROM or DVD drive
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Symantec Corporation
Availability	*http://www.symantec.com/norton/antivirus* *http://www.symantec.com/norton/macintosh/antivirus-dual-protection* *http://www.symantec.com/norton/norton-antivirus-gaming-edition*

NovaShield Anti-Malware

Abstract

NovaShield Anti-Malware uses behavior-based detection technology to detect the presence of known, emerging, and unknown threats, including zero-day threats, including botnets, Trojans, keyloggers, rootkits, worms, and spyware. NovaShield monitors file, registry, process, and network events on a computer and analyzes them based on a set of security policies. If a program performs actions that violate any of the security policies, an alert will be raised on the suspicious program, which can then be stopped and removed from the computer (quarantined). NovaShield will also clean up any new files or registry keys installed by the malware. Development of NovaShield Anti-Malware was funded through two National Science Foundation grants.

NovaShield Anti-Malware

Type	Suspicious process detection and removal
OS	Windows XP an Vista
Hardware	*XP*—Pentium III 800 MHz, 256 MB RAM, 50 MB free disk space *Vista*—800 MHz CPU, 1 GB RAM, 50 MB free disk space
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	NovaShield, Inc.
Availability	*http://www.novashield.com/Anti-Malware.aspx*

ParetoLogic AntiVirus PLUS 6.0

Abstract

Anti-Virus PLUS finds and removes spyware, viruses, Trojans, rootkits, and other malware. The tool also blocks browser access to malware-related URLs and protects against malware embedded in scripts, thus preventing drive-by downloads. Scanning can be customized to scan certain areas on demand, and to skip certain areas (down to the granularity of individual files). AntiVirus PLUS can detect threats in compressed files.

ParetoLogic AntiVirus PLUS

Type	Malware detection and removal
OS	Windows 2000 SP4, XP SP2, Vista (all 32-bit); IE 6.0/7.0
Hardware	Pentium III, 256 MB RAM (512 recommended), 100 MB free disk space, monitor with 1024x764 resolution, Internet connection
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	ParetoLogic Inc. (Canada)
Availability	*http://www.paretologic.com/products/antivirusplus/index.aspx*

ParetoLogic Anti-Spyware

Abstract

ParetoLogic Anti-Spyware provides—

- Active Protection (Real-Time Blocking) that automatically detects a potentially unwanted application attempting to download to a computer, alerting the user to the threat and providing blocking options;
- Customizable scanning processes that enable the user to choose the depth of the scan, including scanning running processes, registry entries, files, and folders;
- Detection and removal of adware, spyware, pop-up ads, keyloggers, Trojans, hijackers, malware, and other potentially unwanted programs;
- Large, continually expanding databases of malware definitions;
- Automatically delivery of feature and definition database updates;
- Backup and Restore feature hat enables the user to restore previously removed items, thus preventing inadvertent permanent removal of benign files;
- Cycle Detection that prevents recurring loops wherein an alert message pops up repeatedly; the tool detects potential loops and presents their details so the user can terminate the notifications;
- Automated scheduled scanning, automatic restoration of browser pages, and automatic blocking and logging.

ParetoLogic Anti-Spyware

Type	Malware detection, blocking, and removal
OS	Windows 2000 SP4, XP SP2; IE 5.0
Hardware	Pentium III, 256 MB RAM (512 recommended), 20 MB free disk space, monitor with 1024x764 resolution, Internet connection
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	ParetoLogic, Inc. (Canada)
Availability	*http://www.paretologic.com/products/paretologicas/index.aspx*

PCSecurityShield The Shield Deluxe 2009

Abstract

The Shield Deluxe uses "Powered by BitDefender" technology to protect systems against viruses, spyware, adware, and rootkits. The tool receives hourly updates to ensure that it always scans based on up-to-date signatures.

The Shield Deluxe 2009

Type	Malware detection and termination
OS	Windows XP, Vista, Home Server
Hardware	*XP*—800MHz or higher CPU, 256 MB RAM (1 GB recommended), 170 MB free disk space (200 MB recommended) *Vista*—800MHz or higher CPU, 512 MB RAM (1 GB recommended), 170 MB free disk space (200 MB recommended) *Home Server*—800MHz or higher CPU, 512 MB RAM (1 GB recommended), 170 MB free disk space (200 MB recommended)
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	PCSecurityShield
Availability	*http://www.pcsecurityshield.com/lp/shield-deluxe-25.aspx*

PC Tools ThreatFire® 3 4.5.0

Abstract

Unlike traditional anti-malware software, ThreatFire 3 detects malicious behavior such as keystroke logging and other behavioral analysis to determine whether the system is infected with malware. This allows ThreatFire 3 to protect against zero-day threats. ThreatFire 3 comes in two versions, Pro and Free; the only differences between them is that the Free license does not include automated updates and telephone support for users, nor does it allow for commercial/business use.

ThreatFire 3

Type	Malware detection (*via* behavior analysis for malware indicators)
OS	Windows XP, Vista, 2003
Hardware	20 MB free disk space
License	Commercial (freeware version available)
NIAP Validated	No
Common Criteria	
Developer	PC Tools, Ltd. (Ireland)
Availability	*http://www.threatfire.com/*

Prevx® 3.0 + Removal and + Real-time

Abstract

Prevx performs virus, adware, and rootkit detection and, using the commercial version, removes detected malware. Prevx is designed to supplement existing anti-virus software, increasing the level of protection against malicious code. Both versions perform detection and removal. Prevx with the Real-time capability also provides real-time and zero-day/zero-hour protection (through heuristics) for blocking of both known and unknown malware. The Real-time capability also protects against master boot record rootkits.

Prevx 3.0 + Removal and + Real-time

Type	Malware detection, termination, and removal
OS	Windows 98, XP, Vista, 2000, 2003, 2008, Windows 7
Hardware	Pentium II, 32 MB RAM, 10 MB free disk space
License	Commercial (freeware version available that performs detection only) [13]
NIAP Validated	No
Common Criteria	
Developer	PREVX, Ltd. (United Kingdom)
Availability	*http://www.prevx.com*

Proland Software Protector Plus 2009 for Windows, Exchange Server, and NetWare Server

Abstract

Protector Plus protects systems against viruses, Trojans, worms, spyware and other potential threats. On Windows, the tool performs real-time scans and continuously monitors the system, preventing malware from entering the during Web browsing, network access, and use of removable media (CD, USB, *etc.*). The tool also blocks infected emails at the incoming port before they read the mail server inbox. Protector Plus automatically downloads signature updates hourly in the background. Users can also submit suspicious files detected and quarantined by Protector Plus's heuristic scanning to Proland Software's virus analysis lab for further investigation; the lab will return a report to the user advising him/her as to whether the file is malicious and should be removed.

On NetWare, Protector Plus includes a real-time scanner Netware Loadable Module and also supports manual scans and remediations that can be targeted down to the volume and directory level. The NetWare tool's virus database is updated weekly.

Protector Plus for Exchange scans all incoming email/attachments before they reach the users' mailboxes, and blocks those that contain malware (viruses, worms, Trojans). The tool can be configured to disinfect, delete, or quarantine the infected mails. The tool can also be configured to send email alerts to the mail message's sender, intended recipient, the administrator, or a pre-configured list of multiple individuals. Remote management of Protector Plus for Exchange can monitor all activity performed by the tool on the Exchange server, and report details such as addresses of senders of infected mails, intended recipients of infected mails, and properties of the infected attachments. Online monitoring also enables the administrator to check the total number of mails received, the number that were infected, *etc.*; reporting also supports analysis of trends over time. The tool's quarantine facility stores infected files for further analysis. Infected files will be moved to the quarantine folder. The quarantined files will be encrypted and they cannot infect the system. These quarantined files can be restored for further scanning or deleted.

Protector Plus Console enables central management of multiple systems running Protector Plus. The console can remotely install the software and updates on the managed end systems.

Software Protector Plus 2009

Type	Malware detection, blocking, and removal
OS	*Windows*—Windows Vista, XP, ME, 2000, 98, 95 desktops; Windows 2000, 2003, NT and Netware 4.x-6.x servers; *Exchange*—Exchange 2000/2003 Server; *Console*—Windows NT/2000/2003 Server (must be a domain controller)
Hardware	
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	Proland Software (India)
Availability	*http://www.pspl.com/products/products.htm*

Protea AntiVirus Tools for Lotus Domino 2.09.271

Abstract

AntiVirus Tools for Lotus Domino is a toolset that integrates avast!, ClamAV, Quick Heal, and VirusBuster malware scanners (described elsewhere in this section) into Lotus Domino to ensure that mail messages and attachments are scanned as they traverse the Domino environment. The administrator can configure the tool to scan documents in Network File System (NFS) databases. Suspicious and infected mail messages, attached files and Object Linking and Embedding (OLE) objects, and documents (including Rich Text Format [RTF] fields, attached files, OLE objects) are either quarantined or deleted, and users and administrators notified about their status (which is also logged).

AntiVirus Tools for Lotus Domino 2.09.271

Type	Malware detection and removal
OS	Windows 2000, XP, 2003
Hardware	Pentium 133, 64 MB RAM (128 MB recommended), 30 MB free disk space
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	Protea Tools (South Africa)
Availability	*http://www.proteatools.com/products/antivirus_lotus_notes_domino/*

The components of the toolset include—

- **Monitor**, for scanning all inbound and outbound email;
- **Scanner**, for scanning all documents in NFS databases;
- **Updater**, for automatically updating the AntiVirus databases;
- **Configuration database**, for managing the AntiVirus toolkit;
- **Quarantine store**, for isolated storage of suspicious and infected objects.

Quick Heal Technologies AntiVirus Plus 2009

Abstract

AntiVirus Plus 2009 provides an anti-virus tool that automatically scans, detects, and removes viruses, worms and Trojans from email attachments and Internet downloads. AntiVirus Plus 2009 also includes an anti-spyware tool that blocks spyware before it can install itself on the PC, detects and removes already-installed spyware, and blocks spyware activity. AntiVirus Plus' anti-malware tool scans the registry, folders, and resident files to detect and remove spyware, adware, rogueware, dialers, riskware, and other potential threats. Finally, the AntiVirus Plus anti-rootkit tool performs proactive deep system scans of running processes, registry, and file system to detect suspicious rootkit-indicative activity hidden on the system, and locate and remove the responsible rootkit. The product also includes a PC firewall.

Quick Heal also provides the AntiVirus Plus capabilities in its—

- Quick Heal for Linux and Novell Netware,
- Quick Heal Mail Protection for Linux and Windows,
- Quick Heal Exchange Protection.

Quick Heal's anti-malware technology is also included in the company's Total Security 2009 PC security product. In India, the anti-virus product line is packaged somewhat differently, to include Quick Heal AntiVirus Plus 2009 Regular and Standard editions for desktop and server.

AntiVirus Plus 2009

Type	Malware detection and removal
OS	*AntiVirus Plus 2009*—Windows 2000, XP, Server 2003, Vista, Server 2008 *Quick Heal for Linux and Quick Heal Mail Protection for Linux*—Redhat Linux 8.0+, SuSe Linux 7.2+, Mandrake 8.0+ *Quick Heal for NetWare*—Novell Netware Server 4.0+ *Quick Heal Mail Protection for Windows*—Windows 2000, XP, 2003 *Quick Heal Exchange Protection*—Windows 2000, 2003; Console—Windows 98, 2000, XP, 2003, 2007
Hardware	*AntiVirus Plus 2009 for—* *Windows 2000 or XP*—300 MHz Pentium, 128 MB RAM *Windows 2003*—300 MHz Pentium, 256 MB RAM *Windows Vista*—1 GHz Pentium, 1 GB RAM *Windows Server 2008*—1 GHz Pentium, 512 MB RAM *All*—200 MB free disk space; DVD or CD-ROM drive *Quick Heal for Linux and NetWare*—133 MHz Pentium, 64 MB RAM, 40 MB free disk space, DVD or CD-ROM drive *Quick Heal Mail Protection for Linux and Windows*—300 MHz Pentium, 128 MB RAM, 40 MB free disk space, DVD or CD-ROM drive *Quick Heal Exchange Protection, Mail server*—300 MHz Pentium, 256MB RAM, 100 MB free disk space *Console for server versions*—800x600 dots per inch (dpi) with 256 colors *Note*—Those AntiVirus products with anti-rootkit capability require an additional 256 MB RAM to run.
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	Quick Heal Technologies (P) Ltd. (India)
Availability	*http://www.quickheal.com/*

Resplendence Software Projects SanityCheck 1.02

Abstract

SanityCheck is an advanced rootkit and malware detection tool for Windows that thoroughly scans the system for threats and irregularities that indicate malware or rootkit behavior. By making use of special deep inventory techniques, this program detects hidden and spoofed processes, hidden threads, hidden drivers, and a large number of hooks and hacks that are typically the work of rootkits and malware. It offers a comprehensible report that gives a detailed explanation of any irregularities found and offers suggestions on how to solve or further investigate any situation.

SanityCheck makes use of a special Windows feature (a GlobalFlag setting), which allows it to create a deep inventory of drivers, devices, processes, threads, and a lot of other information about your system. By making use of this feature in combination with other techniques, it is able to create a very thorough scan of irregularities on your system.

SanityCheck performs checks to detect processes that—

- Hide themselves from the Windows task manager and programming interfaces by using seven (unnamed) safe techniques to reveal hidden processes in both user mode and kernel mode;
- Attempt to obfuscate their names, a typical tactic associated with malware;
- Appear as standard Windows processes;
- Have obviously deceptive names, as is typical of malicious processes received as email attachments that try to appear as innocent document types;
- Have no associated product, company, or description resource information.

SanityCheck also verifies and validates checksums and digital signatures on processes and kernel modules.

SanityCheck performs checks to detect kernel modules that—

- Hook the system service descriptor table,
- Hook the entry points of exported kernel routines,
- Issue kernel object callout hooks,
- Attempt to hide.

Because there is no such thing as a clear distinction line between malware and legitimate products that use aggressive controversial techniques, such as anti-piracy measures that deter debugging or reverse engineering, or rootkit-like techniques such as hidden processes used by anti-virus and other security software to avoid detection by malware (which, in turn, morphs itself to avoid detection by the security software), SanityCheck does not include "one button" eradication of suspect processes or "fixing" of hooks in the kernel. Instead Sanitycheck leaves the system state unaltered, while providing a comprehensible report with suggestions on how to handle the tool's findings.

SanityCheck also provides an optional expert mode in which the user can display extensive information on drivers, devices, processes, threads, kernel objects, and system routines for further analysis; this is information that can only otherwise be obtained using a kernel debugger.

SanityCheck 1.02

Type	Malware detection and termination (*via* behavior analysis for malware indicators)
OS	Windows 2008 Server, Vista, XP, Server 2003, Server 2000
Hardware	
License	Freeware
NIAP Validated	No
Common Criteria	
Developer	Resplendence Software Projects Sp. (Italy)
Availability	*http://www.resplendence.com/sanity* *http://www.resplendence.com/downloads*

Sagyn Solutions SysIntegrity

Abstract

SysIntegrity protects computer against spyware, adware, and malware by performing real-time analysis of files as they are written to the hard disk. By comparing file signatures to a list of known malware, SysIntegrity is able to detect over 100,000 types of malware. If a malicious file is found, the user is prompted to either quarantine or delete the file. In addition to real-time protection, SysIntegrity includes a manual scanner that can be used to scan individual files or entire directories. This is useful for scanning data contained on other media, such as CDs or flash drives.

SysIntegrity	
Type	Malware detection and removal
OS	Windows XP, Vista
Hardware	500 MHz CPU with 256 MB RAM
License	Commercial (freeware version available, detection only)
NIAP Validated	No
Common Criteria	
Developer	Sagyn Solutions
Availability	*http://www.sysintegrity.net/*

Secure Resolutions Anti-CyberCrime 2009

Abstract

Anti-CyberCrime provides on-access and on-demand anti-malware scanning, removal, and quarantine. The tool provides comprehensive reports of its activities and findings. It has been optimized to support downloads of updates over Wi-Fi links.

Anti-CyberCrime 2009

Type	Malware detection and removal
OS	Vista, XP, Windows 2000 (client and server), Server 2003
Hardware	
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	Secure Resolutions, Inc.
Availability	*http://www.secureresolutions.com/Products/SecureResolutionsSuiteConsumer/tabid/115/Default.aspx*

Security Stronghold Security Suite

Abstract

Security Suite integrates Security Stronghold's True Sword anti-spyware and Active Shield anti-virus tools, described in Sections 4.2.3 and 4.2.2, into a single integrated anti-malware system.

Security Suite	
Type	Malware installation prevention and spyware detection and removal
OS	Windows 2000, XP, 2003, Vista
Hardware	
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	Security Stronghold (Russian Federation)
Availability	*http://www.securitystronghold.com/security_suite.html*

Smart PC Solutions 1-2-3 Spyware Free

Abstract

A free anti-spyware and anti-virus solution, 1-2-3 Spyware Free detects and removes all kinds of viruses, spyware, Trojans, and harmful components. 1-2-3 Spyware Free downloads all updates automatically on a schedule, providing a completely transparent and unattended operation. Real-time protection notifies the user about any suspicious activities that a malicious program may attempt, and allows you to block hazardous activities to prevent infection. Scheduled system scans and updates maintain security on a continued basis. The Undo option makes it possible to roll back any infected entries that were deleted.

1-2-3 Spyware Free

Type	Virus detection and removal
OS	Windows NT, 2000, XP, 2003, Vista®
Hardware	
License	Freeware
NIAP Validated	No
Common Criteria	
Developer	Smart PC Solutions, Inc.
Availability	*http://smartpctools.com/antispyware/*

Sourcefire ClamAV 0.95

Abstract

ClamAV is an open source command-line (and, in Linux and Free Berkeley Software Distribution [BSD], on-access) anti-malware scanner. As a command line tool, it is implemented as a multi-threaded daemon to be installed on UNIX/Linux-based mail gateways. ClamAV listens on a UNIX (local) socket or Transmission Control Protocol (TCP) socket for inbound email messages and their attachments. Features of ClamAV include—

- Ability to detect over 530,000 viruses, worms, and Trojans, including Microsoft Office macro viruses, mobile malware, and other threats;
- Milter [14] interface for sendmail;
- Database updater with support for scripted updates and digital signatures;
- Thread-safe virus scanner C library;
- Virus database updates multiple times daily;
- Built-in support for—
  - Compression/archive formats, including Zip, RAR, Tar, Gzip, Bzip2, OLE2, Cabinet, compiled HTML help (CHM), BinHex, and SIS;
  - Almost all email file formats;
  - Executable files (including portable executables) compressed by a variety of different compression tools and algorithms;
  - Popular document formats, including Microsoft Office and MacOffice files, HTML, RTF, and portable document format (PDF).

ClamAV 0.95

Type	Virus detection and termination
OS	GNU/Linux, Solaris, FreeBSD, OpenBSD, Mac OS X
Hardware	
License	GPL
NIAP Validated	No
Common Criteria	
Developer	Sourcefire, Inc.
Availability	*http://www.clamav.net/*

SRN Micro Systems Solo Antivirus

Abstract

Solo Antivirus detects and removes viruses (including boot sector, partition table, file, and macro viruses), worms, spyware, adware, Trojans, backdoors, and malicious Visual Basic® and JavaScript programs. Solo Antivirus includes the "Solo system integrity checker" that monitors the system registry, startup initialization (*.ini*) file, and other system files to identify and protect against new malware.

Solo Antivirus	
Type	Malware detection and removal
OS	Windows XP, Vista, ME, 2000, 98, 95
Hardware	
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	SRN Micro Systems (India)
Availability	*http://www.srnmicro.com/*

Sunbelt Software VIPRE® Antivirus + Antispyware, Enterprise, SDK

Abstract

Using signature matching, heuristic analysis, and behavioral analysis, VIPRE protects against complex known and unknown malware threats, including viruses, adware, spyware, and rootkits. VIPRE's Active Protection delivers real-time monitoring and protection against known and unknown malware threats by working inside the Windows kernel to watch for malware and stop it before it has a chance to execute.

The tool's protection against email viruses includes direct support for Outlook 2000+, Outlook Express 5.0+, and Windows Mail on Vista, and for any email program that uses POP3 and SMTP (*e.g.,* Thunderbird, IncrediMail, Eudora); SSL supported only in Outlook/Outlook Express. APIs to the tool can be accessed *via* a C library or Component Object Model interface.

VIPRE Enterprise provides the same anti-malware protection as Antivirus + Antispyware for single user, plus a central policy/configuration/installation management dashboard and integration with Network Access Control devices and SSL virtual private network devices from Cisco, Juniper, F5, *etc.*, enabling VIPRE endpoints to be automatically recognized and their security policies enforced by these security devices.

Sunbelt Software also offers the VIPRE SDK to enable original equipment manufacturers (OEMs) and service providers to integrate VIPRE Antivirus + Antispyware into their security gateway packages and appliances.

VIPRE Antivirus + Antispyware, Enterprise, SDK

Type	Malware detection and removal
OS	*Antivirus + Antispyware*—Windows Server 2008, Vista, Server 2003, XP, 2000; *Enterprise Administrator Console*—Server 2008, Vista Business/Ultimate, Server 2003, Small Business Server, XP Professional, 2000 Server/Professional; MDAC 2.6 SP2, IE *6.0, .NET* Framework 2.0; *Enterprise Agent*—Server 2008, Vista, Server 2003, Small Business Server 2003, XP, 2000 Server/Professional; IE 6.0; for email support add one of these—Vista Windows Mail, Outlook 2000+, Outlook Express 5.0+, SMTP+POP3 client
Hardware	*Antivirus + Antispyware*—512 MB RAM; *Enterprise Administrator Console*—Pentium III 400 MHz, 512 MB RAM, 300 MB free disk space, monitor with 1024x768 resolution; *Enterprise Agent*—512 MB RAM, 150 MB free disk space
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	Sunbelt Software, Inc.
Availability	*http://www.sunbeltsoftware.com/Home-Home-Office/VIPRE/ http://www.sunbeltsoftware.com/Business/VIPRE-Enterprise/ http://www.sunbeltsoftware.com/Government/VIPRE-Enterprise/ http://www.sunbeltsoftware.com/Developer/VIPRE-SDK/*

Symantec® Endpoint Protection and AntiVirus

Abstract

Symantec offers full range of tools for home and business use, all of which include anti-malware capabilities. The products described here are those that focus on anti-malware protection. All Symantec AntiVirus tools use the company's AntiVirus Scan Engine to detect viruses, worms, and Trojan horses in all major file types, including mobile code and compressed file formats The tool's virus definitions and engines are updated automatically *via* LiveUpdate with no interruption in virus scanning. Symantec also makes its Scan Engine 5.2 available to developers and integrators who wish to incorporate Symantec's AntiVirus scanning technology into their proprietary applications.

Below are descriptions of the capabilities of the individual products in the AntiVirus product line.

- **Endpoint Protection 11.0**—Anti-malware for laptops, desktops, and servers within larger enterprises. It provides a single software agent that is able detect and remove viruses, worms, Trojans, spyware, adware, bots, zero-day threats, and rootkits. Within the tool, TruScan® Proactive Threat Scan performs heuristic/behavior-based scanning for unknown and zero-day threats, scoring both the good and bad behavior of unknown software to enable more accurate malware detection by reducing the number of false positives. This enables the tool to accurately detect malware without present rules-based configurations.

  The tool also incorporates VxMS (Veritas® Mapping Service) technology to gain access at the kernel level (below the OS) for detection, analysis, removal, and repair of even very-difficult-to-find/eradicate rootkits, eliminating the need to re-image rootkit-infected machines. Signature file updates and other updates are centrally stored in a dedicated database and distributed from a Management Server, with all endpoints administered from a single Management Console.

  The management console enables the administrator to control user and application access to specific processes, files, and folders, and to perform application analysis, process control, file and registry access control, and module and DLL control. It enables administrators to restrict certain activities deemed as suspicious or high risk.

  The tool also controls which peripherals can be connected to a machine and how the peripherals are used. It locks down endpoints to prevent connections from thumb drives, CD burners, printers, and other USB devices. These administrative controls significantly hamper malware from spreading to other endpoints, from PCs, servers, or peripherals; it has the coincidental advantage of helping to prevent data leakage.
- **Endpoint Protection Small Business Edition**—This tool is intended for small businesses. It provides the same anti-malware capabilities, but simplifies the management and administrative sophistication, with the capabilities and needs of small businesses in mind.
- **Endpoint Protection for Windows XP Embedded**—This tool is designed specifically for embedded devices running Windows XP Embedded 5.1 and Windows Embedded Point of Sale with limited hard drive or flash memory size, to defend them against worms, Trojan horses, viruses, and other malicious code attacks and infection. Such devices include thin clients, point-of-sale terminals, automated teller machines, and medical devices. To block malware attacks from reaching these devices, the tool also provides an application-layer firewall and intrusion detection and prevention system. The tool is administered by the Symantec Policy Manager's Java-based console.
- **AntiVirus for Caching**—Provides scalable virus protection for HTTP and *FTP/HTTP* traffic served through or stored on caching devices, including Blue Coat ProxySG®, Network Appliance NetCache,

and Cisco's Application and Content Networking System Content Engines. The tool supports version 1.0 of the Internet Content Adaptation Protocol 1.0 for deployment of anti-virus services at the gateway with minimal network latency.

- **AntiVirus for Messaging**—Scalable virus protection for email traffic passing through various messaging solutions.
- **AntiVirus for Network Attached Storage**—Scalable virus protection for Network Attached Storage (NAS) devices. Tested and verified by several NAS vendors to operate with their devices.
- **Mobile AntiVirus for Windows Mobile**—Mobile AntiVirus provides on-device, automatic, real-time scanning to protect devices running the Windows Mobile OS, such as Windows PocketPCs and smartphones, against threats downloaded from the Web, sent *via* email or a Wi-Fi connection, or received *via* Bluetooth or infrared ports. The tool is able to quarantine viruses for later review, and includes an SMS listener to enable administrators to remotely initiate on-device actions. Event logging also enables administrators to generate an on-device eXtensible Markup Language (XML) file of event logs more detailed than the on-device activity log.

Symantec has also purchased the Norton AntiVirus tool, covered earlier in this report, which it still markets under the Norton brand.

Endpoint Protection 11.0

Type	Malware detection and removal
OS	*Client Workstations and Servers*—Windows 2000 Server; XP; Server 2003; Server 2008; Vista; Small Business Server; Essential Business Server; Red Hat Enterprise Linux 3.x-5.x; SuSE Linux Enterprise (server/desktop) 9.x-10.x; Novell Open Enterprise Server (OES/OES2); VMWare® ESX 2.5-3.x; Ubuntu 7.x-8.x; Debian 4.x *Management Server*—Windows 2000 Server; XP Professional; Server 2003; Server 2008; Small Business Server; Essential Business Server *Management Console*—Windows 2000 Professional or Server; XP Professional; Server 2003; Vista
Hardware	*Client Workstations and Servers*—32- or 64-bit Pentium; 256 MB RAM; 600 MB free disk space *Management Server*—32- or 64-bit Pentium; 1 GB RAM; 2 GB free disk space (+4 GB for database support) *Management Console*—32- or 64-bit Pentium; 512 MB RAM; 15 MB free disk space *Note—Itanium not supported*
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Symantec Corporation
Availability	*http://www.symantec.com/business/endpoint-protection*

Endpoint Protection Small Business Edition

Type	Malware detection and removal
OS	*Client Workstations and Servers*—Windows 2000 Professional/Server; XP; XP Embedded; Vista; Server 2003; erver 2008 *Symantec Protection Center Management Server*—Windows 2000 Server; XP; Server 2003; Server 2008
Hardware	*Client Workstations and Servers*—32- or 64-bit 1 GHz Pentium III; 256 MB RAM (1 GB recommended); 700 MB free disk space *Symantec Protection Center Management Server*—32- or 64-bit 1 GHz Intel Pentium III; 1 GB RAM (2 GB recommended); 4 GB free disk space *Note—Itanium® not supported.*
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Symantec Corporation
Availability	*http://www.symantec.com/business/endpoint-protection-small-business-edition*

Endpoint Protection for Windows XP Embedded

Type	Malware detection and removal
OS	Windows XP Embedded 5.1, Windows Embedded for Point of Service
Hardware	Pentium 133, 128 MB RAM, 40 MB free disk space
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Symantec Corporation
Availability	*http://www.* symantec.com/business/endpoint-protection-for-windows-xp-embedded

AntiVirus for Caching

Type	Malware detection and removal
OS	Red Hat Linux Enterprise Server 3/4; Red Hat Linux Advanced Server 3/4; Red Hat Enterprise Linux 5; SuSE Linux Enterprise Server 9/10; Solaris 9/10; Windows 2000 Server, Server 2003, Server 2003 R2
Hardware	*Linux*—Pentium 4 1 GHZ, 1 GB RAM, 500 MB free disk space; Solaris—SPARC, 1 GB RAM, 500 MB free disk space; *Windows*—Pentium 4 1 GHz, 1 GB RAM, 500 MB free disk space 1 TCP/IP network interface card with static IP address, 100 Mbps Ethernet link (1 Gigabit per second recommended)
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Symantec Corporation
Availability	*http://www.* symantec.com/business/anti-virus-for-caching

AntiVirus for Messaging

Type	Malware detection and removal
OS	Same as AntiVirus for Caching
Hardware	Same as AntiVirus for Caching
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Symantec Corporation
Availability	*http://www.symantec.com/business/anti-virus-for-messaging*

Mobile AntiVirus for Windows Mobile

Type	Malware detection and removal
OS	Microsoft Windows Mobile 6 Professional or Standard, 5.0 PocketPC or Smartphone
Hardware	PocketPC, smartphone, or other device that supports Windows Mobile; 2.5 MB memory
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Symantec Corporation
Availability	*http://www.symantec.com/business/mobile-anti-virus-for-windows-mobile*

TrendMicro AntiVirus + AntiSpyware

Abstract

An anti-virus/anti-spyware tool that features automatic scans, updates, and outbreak alerts. The tool scans PC and incoming emails for malicious viruses, worms, Trojan horse programs, and spyware, and also provides anti-rootkit protection and proactive intrusion blocking.

Trend Micro's AntiVirus and AntiSpyware technologies are also incorporated into the company's Worry-Free Business Security, OfficeScan Client-Server Suite, InterScan Messaging Hosted Security, and ScanMail Suite products for small, medium, and large businesses.

AntiVirus + AntiSpyware

Type	Malware detection and removal
OS	Windows Vista, XP
Hardware	*Vista*—Pentium 800 MHz, 512 MB (1 GB recommended) RAM *XP*—350 MHz Pentium—256 MB (512 MB recommended) RAM *All*—300 MB free disk space; for console—Extended Graphics Array (XGA) monitor with 1024x768 dpi
License	Commercial
NIAP Validated	no
Common Criteria	
Developer	TrendMicro, Inc.
Availability	*http://us.trendmicro.com/us/products/personal/anti-virus-plus-anti-spyware/index.html*

Trojan Remover 6.7.9

Abstract

Trojan Remover aids in the removal of malware, including Trojan horses, worms, adware, spyware. Trojan Remover examines all the system files, the Windows Registry, and the programs and files loaded at boot time, as well as services hidden by rootkit techniques. Trojan Remover can be instructed to remove the specific malware-related files and to disable the malware upon request.

Trojan Remover 6.7.9

Type	Hidden malware detection and removal
OS	Windows 98, ME, 2000, XP, Vista, Windows 7
Hardware	
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	Simply Super Software
Availability	*http://www.simplysup.com/*

TrustPort Antivirus 2009, USB Edition, U3 Edition

Abstract

TrustPort Antivirus 2009 uses multiple scanning engines to perform anti-virus and anti-spyware detection and removal. Signature-based scanning with regular automatic virus sample updates combines with heuristic analysis and virtual computer testing that reveal unknown threats. In addition, the tool performs anti-spam filtering to reduce the risk of users inadvertently opening of infected email attachments or being directed to malicious Web sites, detection of viruses on Web sites to which the user connects, and Web site blacklisting to prevent drive-by downloads. Emails and inserted media are automatically scanned, and detected malware is quarantined. The tool also generates a rescue boot disk to ease recovery after a malware infection. The tool comes in PC and Server editions; USB and U3 Editions are also available to scan USB and U3 flash media.

TrustPort Antivirus 2009

Type	Malware detection, blocking, and removal
OS	Windows 2000, 2003, 2008 Server, XP, Vista
Hardware	Pentium 4, 512 MB RAM, 250 MB free disk space; USB and U3 editions require the appropriate USB connections
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	TrustPort, a.s. (Czech Republic)
Availability	*http://www.trustport.com/index.php?id=593,1118,0,0,1,0*

VirusBuster®

Abstract

The VirusBuster line of anti-virus products include—

- **VirusBuster Professional for clients and VirusBuster for Linux/FreeBSD clients**—Resident protection and content filter with pre-defined protection levels from which the user can choose, or which he/she can modify as needed. The resident protection module provides protection for all files on the computer. The content filter protects the computer against all Internet-borne viruses, worms, Trojans, backdoors, scripts, macro viruses and other harmful code by scanning incoming email (POP3, SMTP, IMAP) and data transmitted *via* HTTP and *FTP;*
- **VirusBuster for Servers**—Uses VirusBuster's heuristic analysis-based scan engine to detect harmful programs, known viruses, and malicious code;
- **VirusBuster for Mail Servers**—Zero Hour Virus Protection and Extended Spam Protection technologies detect the attacking/spreading wave itself connecting and communicating permanently to a central server. These filters are able to reveal the virus and spam mail attacks minutes after they have been started and block these emails long before the first virus or spam database updates are released. The tool can also block I-Worms in real time.

VirusBuster offers a command line-based VirusBuster Scanner product line for use on older OSs. VirusBuster includes its anti-malware technology in its Internet Security Suite cyber security product.

VirusBuster also offers the VirusBuster anti-malware software development kit, which enables integrators to include VirusBuster's anti-malware engine in the systems they develop.

VirusBuster	
Type	Malware detection and removal
OS	*VirusBuster Scanners*—Windows 2000, 95, 98, ME, XP, NT4 Workstation; FreeBSD, Linux, OpenBSD, Solaris, AIX *VirusBuster Professional*—Windows 95, 98, ME, NT4 Workstation, 2000, XP, Vista *VirusBuster Personal*—Windows 95, 98, ME, 2000, XP, Vista *VirusBuster for Linux/FreeBSD*—FreeBSD, Linux *VirusBuster for Samba Servers*—Linux, Solaris *VirusBuster for NetWare Servers*—Novell NetWare *VirusBuster for Windows Servers*—Windows NT4 Server, 2000 Server, Server 2008 *VirusBuster for Mail Servers (SMTP or Sendmail, Qmail, Linux GroupWise, Courier)*—Linux, FreeBSD, OpenBSD, Solaris, AIX *VirusBuster for Mail Servers (NetWare GroupWise®)*—Novell NetWare GroupWise
Hardware	
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	VirusBuster (Hungary)
Availability	*http://www.virusbuster.hu/en/product/antivirus/index* *http://www.virusbuster.hu/en/product/antivirus/oem/sdk*

Webroot® AntiVirus with AntiSpyware 6.1, AntiSpyware Corporate Edition 3.5 with AntiVirus

Abstract

Webroot's AntiVirus combines anti-virus detection based on Sophos' anti-virus technology with Webroot's own Spy Sweeper (discussed in Section 4.3.2) to provide comprehensive protection against complex threats including viruses, worms, Trojans, rootkits, spyware, adware, and keyloggers.

AntiSpyware Corporate Edition with AntiVirus combines Webroot's AntiSpyware Corporate Edition, discussed in Section 4.3.1.3, with Webroot's AntiVirus product, discussed in Section 4.3.1.2.

TrustPort Antivirus 2009

Type	Malware detection and removal
OS	*AntiVirus with AntiSpyware*—Windows Vista, XP; *Corporate Edition*—Windows Vista, 2000 Professional or Server (SP 4), XP Professional (SP 2), 2003 Standard, Enterprise, R2, or Small Business Server (SP1)
Hardware	*AntiVirus with AntiSpyware*—300 MHz CPU, 256 MB RAM, 100 MB free drive space; *Corporate Edition*—1 GHz CPU, 1 GB RAM, 1 GB free disk space
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	Webroot Software, Inc.
Availability	*http://www.webroot.com/En_US/consumer-products-antivirus.html* *http://www.webroot.com/En_US/business-antispyware-ce-with-antivirus.html*

WenPoint HiddenFinder v1.5.3

Abstract

HiddenFinder is an advanced security utility that detects and kills processes and drivers hidden by attack code. Such processes and drivers may be associated with spyware, backdoors, rootkits, or viruses. HiddenFinder explorers the system at the kernel level and displays all running processes and drivers, including those that are hidden. The user can then terminate the detected hidden processes/drivers, which will coincidentally stop the execution of most spyware, viruses, and Trojans.

HiddenFinder v1.5.3

Type	Malicious process termination
OS	Windows 2000 and XP
Hardware	Pentium II; 128M RAM
License	Freeware
NIAP Validated	No
Common Criteria	
Developer	WenPoint Corporation
Availability	*http://www.wenpoint.com/download/download.php*

Zemana AntiLogger

Abstract

AntiLogger relies on its own unique technology to detect when malware is running on a user's PC—without malware signatures. This technology detects when malware runs on the computer, then terminates that malware before it can damage the system or steal data. Zemana's AntiLogger eliminates threats from keyloggers, SSL banker Trojans, spyware, and other malware, including sophisticated zero-day malware and other viruses, worms, Trojans, spyware executables, and rootkits that elude signature-based tools.

AntiLogger

Type	Malware detection and termination
OS	Windows XP
Hardware	
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	Zemana Ltd. (Turkey)
Availability	*http://www.zemana.com/AntiloggerOverview.aspx*

4.3.1.2 Anti-Virus Tools

The tools described in this section are understood to address viruses, worms, and Trojans delivered to (rather than built into) the targeted system.

AhnLab Mobile Security

Abstract

AhnLab Mobile Security uses AhnLab's V3 antivirus engine technology to provide anti-virus protection for WiFi devices. The tool supports manual, real-time, and .sis and .cab file attachment scanning and sanitization.

AhnLab Mobile Security

Type	Malware detection and removal
OS	*Devices*—Symbian OS 7.0s, Symbian OS 8.0a, Symbian OS 8.1a; Windows Mobile 2003, 2005; *Host*—Windows XP, 200, ME, 98 Server Edition running Activesync 3.7 or higher
Hardware	*Devices*—Symbian OS 8.1, OS 8.0a, 7.0s; Windows Mobile; Nokia 3230, 6600, 6620, 6670, 6260, 7610 (Symbian OS 8); Nokia 6630, 6680, 6681, 6682 (Symbian OS 7); Samsung Phaeton I (Symbian OS 8.1); Microsoft Pocket PC 2003, 2005 (Win Mobile)
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	Zemana Ltd. (Turkey)
Availability	*http://global.ahnlab.com/global/prod_detail.ESD* ?parmProd _class= C&parmProd_type =CM&prod_seq=1023

AnVir Virus Destroyer

Abstract

AnVir Virus Destroyer supplements existing anti-virus and anti-malware tools by providing users with additional capabilities, including—

- Full information about processes, services, Internet connections, drivers, and running DLLs;
- Detailed information for over 70,000 binary executables;
- Security analysis of application behavior to aid in the detection of malware;
- Monitors for CPU, memory, disk usage, and battery power.

AnVir Virus Destroyer is also included in the AnVir Security Suite and Task Manager Suite products.

AnVir Virus Destroyer

Type	Virus detection and removal
OS	Windows 95 and later; Linux; Mac OS X 10.3 and later
Hardware	
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	AnVir Software (Russian Federation)
Availability	*http://www.anvir.com/virusdestoyer/*

ArcaBit ArcaVir® 2009 Antivirus Protection

Abstract

ArcaVir comprises an anti-virus engine (which includes a database of different variants of viruses, worms, Trojans, and other malware exploits), signature-based and heuristic scanning (detects and disarms novel threats), and quarantine of detected viruses. The tool supports both an monitoring of network/Internet connections, AntiStealth detection of hidden processes and objects, and scanning of email attachments, CDs, and floppy disks. The tool's ArcaNix system enables ArcaVir to control the computer's boot sequence and to scan all drives and Windows NT File System partitions.

The tool comes in editions for home use and for Pocket PC, and business editions for Microsoft Windows Server and Exchange Server, and for Lotus Notes, Linux/FreeBSD, and Novell Netware. ArcaBit also offers ArcaVir On-line, which enables users to use a ArcaVir-as-a-Service to scan their PCs and remediate any malware detected.

ArcaVir 2009 Antivirus Protection

Type	Malware detection and removal
OS	*Home edition*—Windows XP, Vista (earlier versions of ArcaVir are still available for Windows 2000, NT 4.0, ME, and 98); *Windows Server edition*—Windows Server 2000, 2003, 2008; *Pocket PC edition*—Windows CE, Symbian OS
Hardware	
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	ArcaBit Sp. z o.o. (Poland)
Availability	*http://www.arcabit.pl/content/view/142/164/lang,english/*

Ashampoo AntiVirus

Abstract

Ashampoo AntiVirus provides comprehensive protection against viruses, worms, Trojans, and dialers. The tool scans all critical system areas, memory, emails, and files. It provides a very intuitive user interface, and places a very low overhead load on the system so is transparent to the user. The virus signatures are updated several times a day and the program checks for updates automatically, and can be configured to do so every hour. The tool also supports multiple scan modes, including automatic real-time scanning, manual scans, and scheduled scans. Quarantining moves infected or suspicious files to a locked quarantine area. The tool also provides an integration option whereby the tool can scan files for viruses directly in Windows Explorer.

Ashampoo AntiVirus

Type	Virus detection and removal
OS	Windows 2000, XP, Vista
Hardware	
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	Ashampoo GmbH (Germany)
Availability	*http://www.ashampoo.com/frontend/products/php/product.php?session_langid=2&idstring=0045*

Australian Projects Zondex Guard

Abstract

Zondex Guard is a highly automated anti-virus utility that enables real-time scanning and continuous monitoring, detection, and remediation of viruses, as well as blocking of unauthorized executables. The tool's built-in self-management system automatically updates the virus definition files and upgrades the tool's control engine.

Zondex Guard

Type	Malware detection and removal
OS	Windows 2000, XP (also runs on 95, 98, and ME, but no technical support is provided for the tool on these OSs)
Hardware	
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	Australian Projects Pty Ltd. (Australia)
Availability	*http://www.apro.com.au/products/zondex-guard.html*

Beijing Rising International Software Rising PC Doctor

Abstract

Rising PC Doctor performs automatic malware analysis and immunization. The tool can detect and remove most Trojans, spyware, and a significant amount of other malware, detecting the malicious programs when they attempt startup and "defusing" them before they can execute their malicious functions. The tool's Trojan blocking technology prevents computers, including infected computers, from downloading additional viruses and Trojans, thereby preventing their propagation. Rising PC Doctor automatically scans programs loaded at boot time, system drivers, ActiveX controls, and other software that influences the computer's operation for unknown malware, which the user can choose to have automatically transferred to Beijing Rising's Automated Malware Analyzer for detailed analysis and reporting back to the user.

The tool also performs a vulnerability scan of Windows and its security settings, and of third-party software from many vendors, to detect vulnerabilities that can be exploited malware. Rising PC Doctor can also configure IE to avoid visiting Web pages that have been corrupted by malware or which permanently display adware. The tools can also repair the PC system registry, system settings, and host file. Also provided are additional "expert user" tools for disk cleanup, system startup management, service management, network application management, layered service profile repair, file shredding, and special virus removal.

Rising PC Doctor

Type	Malware detection and removal
OS	Windows 2000, XP, 2003, Vista
Hardware	
License	Freeware
NIAP Validated	No
Common Criteria	
Developer	Beijing Rising International Software Co., Ltd. (China)
Availability	*http://www.rising-global.com/products/rising-pc-doctor.html*

BullGuard® Mobile Antivirus

Abstract

Protects Pocket PCs and smartphones from viruses, worms, and Trojans that target mobile platforms. The tool scans all incoming traffic (*e.g.,* SMS and multimedia messaging service [MMS] messages, Bluetooth, emails, downloads) for malicious programs. The user can launch a scan of a mobile device at any time. Automatic over-the-air updates ensure your device is protected against the latest threats. BullGuard provides 24/7 support free to customers. BullGuard also includes its Antivirus technology in BullGuard Internet Security 8.5.

BullGuard Mobile Antivirus

Type	Malware detection and removal
OS	Windows Mobile 5 or later
Hardware	Symbian S60 v9.x or UIQ v3.X; 4 MB free storage space
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	BullGuard Ltd. (United Kingdom)
Availability	*http://www.bullguard.com/why/bullguard-mobile-antivirus.aspx*

CA® Anti-Virus 2009

Abstract

CA's Anti-Virus 2009 protects against viruses, worms, and Trojans that can invade unprotected PCs *via* email, downloads, instant messages, and Web page accesses, and can erase computer files, damage the hard drive, and destroy information contained in documents, image files, audio files, and other files. The tool performs real-time scanning of files whenever they are opened, closed, or saved, and automatic scans of email upon receipt. The tool is able to scan files archived by a variety of compression techniques and formats. The tool includes both signature-based and heuristic scanning (to detect new threats before virus signature updates are created), and sends all suspect files to a secure quarantine area. Users can configure the tool to exclude certain files from being scanned. CA provides daily, fully automatic updates of the tools and its virus signatures. Anti-Spyware 2009 has been certified by ICSA Labs, West Coast Labs, and Virus Bulletin as providing effective virus protection. Anti-Virus 2009 is also included in the CA Internet Security Suite.

Anti-Virus 2009

Type	Malware detection and removal
OS	Windows 2000, XP, or Vista
Hardware	300 MHz CPU (800 MHz for Vista), 256 MB RAM (512 MB for Vista), 35 MB free disk space
License	GPL
NIAP Validated	No
Common Criteria	
Developer	CA
Availability	*http://shop.ca.com/virus/anti-virus.aspx*

Deerfield.com VisNetic® MailScan

Abstract

VisNetic MailScan features comprehensive, flexible anti-virus protection tools to protect the network from email viruses and email content filtering technology designed to reduce unwanted messages. The tool's scanning features include—

- Automated, fast virus signature updates;
- Real-time email scanning;
- Attachment blocking;
- Automatic worm deletion;
- Scans HTML emails and attachments for scripts, also termed IE vulnerabilities;
- Scans multipart/partial messages for viruses;
- Detects and disinfects viruses traveling *via* Transport Neutral Encapsulation Format attachments, a standard delivery method used in Microsoft Outlook;
- Features the option to specify certain domains as "approved" or "verified safe," thereby reducing the amount of total scanning required.

In addition, MailScan performs the content filtering to prevent spam by blocking email from suspicious or unwanted senders or source addresses.

MailScan comes in versions that support SMTP (*e.g.,* Microsoft Exchange, VisNetic MailServer, MDaemon®, FTGate®, NTMail, Merak Mail Server) and MDaemon email servers.

VisNetic MailScan

Type	Virus detection and removal
OS	Windows 95, 98, ME, NT4, XP, 2000 Server and Professional
Hardware	166 Mhz CPU, 64 MB RAM, 50 MB free disk space
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	Deerfield Communications, Inc.
Availability	*http://www.deerfield.com/products/mailscan/*

DiamondCS WormGuard

Abstract

WormGuard provides deep-scanning generic, heuristic detection technology driven by a smart analysis engine that includes intelligent rule-sets that are used to detect and block worms, including worms of which the tool has no prior knowledge. Specifically, the tool determines what the suspect executable actually does and alerts the user if it is potentially harmful. The user can then analyze the output from WormGuard to determine whether the suspect file is safe to open/suspect executable is safe to run.

WormGuard can perform detection on all executable files and file types. WormGuard also provides extended universal detection and analysis of macros across all Microsoft Macro formats and of command files. Other objects detected by WormGuard include password stealers, keyloggers, IRC worms, and references to known worm authors.

WormGuard employs a non-resident execution hook method to render itself immune to *TerminateProcess* and *SuspendProcess* vulnerabilities found in other active security systems.

WormGuard	
Type	Worm detection
OS	Windows 95, 98, ME, NT, 2000, XP, Server 2003
Hardware	
License	Commercial (freeware versions available)
NIAP Validated	No
Common Criteria	
Developer	DiamondCS (Australia)
Availability	*http://www.diamondcs.com.au/wormguard/*

e-Frontier Virus Killer Internet Security, Virus Killer Zero

Abstract

e-Frontier's Virus Killer products scan for known and unknown viruses and variants, and use a variety of disinfection techniques. The tools runs a background monitor that senses whenever a new virus definition file becomes available, and automatically downloads it. There appears to be a gaming edition that does not require installation on the target PC but runs from a USB drive.

e-Frontier's Virus Killer product line includes Virus Killer Internet Security "Hokuto No Ken," "Ragunarokuonrain," Limited Edition, and "Tokimekihuantajirateru," and Virus Killer Zero Internet Security Limited Edition and Special Edition. Each license supports up to three target PCs.

Note—The e-Frontier and Virus Killer Web sites are only provided in Japanese. The information here is based on automated translations into English by Google Translate and Yahoo! Babel Fish. The authors of this report apologize for any inadvertent misinformation due to inaccurate translation.

e-Frontier Virus Killer Internet Security, Virus Killer Zero

Type	Malware detection and removal
OS	*All Editions except "Ragunarokuonrain"*—Windows 2000 Professional, Vista, XP (all 32-bit) running IE 5.0 (6.0 recommended); *for mailbox scanning add*—Windows Mail, Outlook Express 4.0, Outlook 98, Netscape Mail 4.7.2, or Lotus Notes. Encrypted email not supported; "*Ragunarokuonrain" Edition*—Windows 200 Professional, XP, Vista (all 32-bit only); *if running Win 2000/XP*—DirectX 8.0; *if running Vista*—DirectX 9.0; *All*—operating system and application versions must be Japanese.
Hardware	*On Vista*—Pentium 1 GHz, 512 MB RAM; on XP/2000—Pentium 500 MHz, 256 MB RAM (512 MB recommended); *Both*—400 MB free disk space, monitor/console 1024x764 resolution with 24+-bit color depth, broadband Internet connection (*e.g.,* ADSL 1.5 Mbps); *Virus Killer Gaming edition*—on XP/2000—Pentium III/AMD 650 MHz, 3 dimensional graphics card with 16 MB video RAM; *on Vista*—Pentium 4 3 GHz/Athlon64 3500, Vista 3 dimensional graphics card with 128 MB video RAM; *Both*—2 GB free disk space, USB port
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	e-Frontier Inc. (Japan)
Availability	*http://www.viruskiller.jp/*

FRISK Software International F-PROT® Antivirus v6

Abstract

FRISK offers home editions (for Windows and Linux) and business editions (for Windows, Linux, BS, Solaris, IBM eServers, and Exchange mail servers) of F-PROT Antivirus. The tool detects and removes viruses, worms, Trojans, and other malware from files (including archives, Microsoft Office, and ActiveX controls) and emails (Microsoft Outlook supported)—automatically and in real-time.

New and unknown threats are detected by the tool's heuristic's technology. The tool quarantines infected and suspicious files are quarantined and supports automatic and manual scanning (with user able to configure certain files, folders, and/or extensions for exclusion from scanning). FRISK offers a separate license for F-PROT Antivirus for Windows when used on mail servers.

F-PROT for Linux and UNIX workstations scans for nearly 1.4 million known viruses and their variants (the IBM server [Advanced Interactive eXecutive (AIX) and Linux on eServer] versions scan for over 540,000), and in addition to hard drives and network drives (file system directories down to the granularity of individual files), scans CDs and diskettes. The tool on Linux scans for boot sector viruses, macro viruses, and Trojans. FRISK's Solaris series of products include F-PROT for Solaris on x86 and SPARC workstations, file servers, and mail servers (Sendmail, Postfix, Qmail, other popular Solaris-based mail servers).

On all operating systems, the tool includes an optional command line interface for users who prefer it; on Solaris and AIX, the tool also includes a daemon scanner. FRISK also uses its F-PROT Antivirus technology in its AVES managed online email security service.

F-PROT Antivirus

Type	Malware detection and removal
OS	Windows 2000 Professional and Server, XP Home and Professional, Server 2003, Vista, Home Server; must run IE 5.0 to enable automatic updates; *Mail servers supported on Windows*—Microsoft Exchange 2000 or 2003 on Windows 200 Server, Exchange 2003 on Windows 2003 server; SuSE, Red Hat, and Debian Linux; FreeBSD, NetBSD, HomeBSD; Solaris 8/9/10; AIX 5.3; must have Perl 5.8 interpreter installed; Linux/BSD systems must have Dazuko installed in kernel; on IBM eServer, Linux must also have glibc 2.3.2.
Hardware	*Windows versions*—20 MB RAM, 80 MB free disk space, monitor/console with 800x600 resolution (1024x768 recommended) and 32-bit color; *Linux versions*—Pentium or AMD K5, 10 MB of free disk space or IBM zSeries s/390 eServer, 50 MB free disk space; *Solaris versions*—SPARC or Intel x86 compatible, 50 MB free disk space; *AIX versions*—IBM pSeries (RS/6000), 75 MB free disk space
License	Commercial (exception—Linux/BSD workstation/home use versions are Freeware)
NIAP Validated	No
Common Criteria	
Developer	FRISK Software International
Availability	*http://www.f-prot.com/products/*

G DATA® AntiVirus 2010

Abstract

G DATA AntiVirus runs undetected in the background, using two scanning engines, signatures updated hourly, and self-learning to perform fingerprinting for detection and blocking/removal of viruses, spyware, Trojans, dialers, rootkits, *etc.* The tool's OutbreakShield uses behavior blocking, heuristics, and "cloud security" to detect and block known and unknown viruses in infected emails (the tool supports Outlook, Outlook Express, Mozilla, and other POP3/IMAP clients) including attached files and archives. It supports whitelisting by the user to improve tool performance. The tool also supports anti-phishing protection (*i.e.,* blocks connections to known-malicious Web sites). G DATA offers private user, business, and enterprise editions. Enterprise edition includes an AntiVirus ManagementServer for centrally managed installation, scanning, updating, reporting, *etc.*

G DATA AntiVirus

Type	Malware detection and removal
OS	*Private Use*—Windows Vista or XP; *Business/Enterprise*—Windows 2000 (client only), Server 2008, Vista, 2003, XP at least SP2
Hardware	*Private Use*—Intel 32-bit or 64-bit CPU. 512 MB RAM; *Business/Enterprise*—all versions except Windows 2000 (32-bit only) run on Intel 32-bit or 64-bit CPU with 256 MB RAM and an Internet connection
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	G DATA Software AG (Germany)
Availability	*http://www.gdata-software.com/online-shop/anti-virus-produkte/shop/46-private-users/966-g-data-antivirus-2010.html*

GFI MailSecurity v.10

Abstract

GFI MailSecurity implements multi-engine virus checking using the Norman and BitDefender anti-virus engines, and provides the customer with the option of adding the AVG, McAfee, and Kaspersky engines. The toolset checks all inbound and outbound email messages and attachments, with quarantining of potentially dangerous attachment types (*e.g.,* .exe, .vbs) that may contain unexpected/undesired executables or Trojans. Exchange, SMTP, and Lotus mail are supported.

The HTML Sanitizer function scans email and Webmail body parts and .htm/.html attachments for presence of scripting code, which it removes. The tool includes a decompression filter that can decompress and analyze compressed archives attached to emails to detect and block password-protected archives, corrupted archives, recursive archives, and archives that contain too many files or files that are too large (indicating potential presence of malicious executables).

GFI MailSecurity

Type	Malware detection and removal
OS	Windows Server 2003, Server 2008, 2000 (Professional, Server, Advanced Server), XP
Hardware	
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	GFI Software Ltd.
Availability	*http://www.gfi.com/mailsecurity/*

Ikarus Security Software virus.utilities

Abstract

A comprehensive anti-virus package, Ikarus virus.utilities enables remote scanning of PCs for viruses, worms, Trojans, and other malware. In addition to the virus scanning utilities, which support manual scanning, the package includes Online Guardian Protector, which runs continuously in the background to monitor every read and write transaction, scanning the data (including files compressed using any of 17 different compression formats, including .zip, .arj, and .rar, which it can recursively decompress) for the presence of known and unknown (through heuristics) malware. Searches can be customized, and the tool can be automatically updated, with new signature updates delivered within minutes after virus outbreaks. Moreover, the tool can participate in a Europe-wide sensor network to provide rapid screening and response to detected threats.

Note—The Ikarus Web site is provided only in German and in Russian translation. The authors of this report apologize for any inadvertent inaccuracies in our translation to English.

Ikarus virus.utilities

Type	Malware detection and removal
OS	Windows 2000, 2003 Server (limited support), XP, Vista (32-bit/64-bit)
Hardware	
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	Ikarus Security Software GmbH (Austria)
Availability	*http://www.ikarus-software.at/products/virus%20utilities.htm*

ISecSoft Anti-Trojan Elite

Abstract

Anti-Trojan Elite is a malware remover that includes a real-time malware firewall that monitors the system and cleans malware upon discovery. It also enables the user to view and control processes and TCP/IP network connections. Anti-Trojan Elite recognizes over 35,000 Trojans, worms, and keyloggers.

Anti-Trojan Elite	
Type	Trojan detection and removal
OS	Windows 98, ME, 2000, XP, 2003, Vista
Hardware	
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	ISecSoft Inc. (China)
Availability	*http://www.remove-Trojan.com/index_ate.php*

Liao Pecong's USB Drive AntiVirus

Abstract

USB Drive AntiVirus blocks and remove threats to the system from the USB drive without relying on anti-virus signatures, allowing it to protect offline systems from viruses introduced by USB drives. USB Drive AntiVirus will automatically scan any USB drive inserted into the computer, and remove all detected threats.

USB Drive AntiVirus also provides anti-data leakage protection, whereby the user can set the USB port status to "read-only" or "readable/writable" on the machine and can disable use of specific USB storage devices to prevent leakage from one USB drive to another.

USB Drive AntiVirus can scan and remove threats from pen drives, iPods and iPhones, USB flash cards, USB MP3 players, USB audio players, external hard drives, PocketPCs, mobile phones, other USB mass storage devices

USB Drive AntiVirus

Type	Hidden malware detection and removal
OS	Windows
Hardware	
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	Liao Pecong (China)
Availability	*http://www.usbantivirus.net/default.htm*

Loaris Trojan Remover 1.1

Abstract

Trojan Remover aids in the removal of malware (including Trojans, worms, adware, and spyware) that has not been eliminated by other anti-malware programs. Trojan Remover is designed specifically to disable/remove malware without the user having to manually edit system files or the Windows registry. The program also removes the system modifications performed by some malware—modifications ignored by some other anti-virus scanners. Trojan Remover scans all the files loaded at boot time, performing either a standard scan that requires no user configuration of the scan parameters or a custom scan that enables the user to select specific folders to be scanned.

Trojan Remover 1.1

Type	Virus detection and removal
OS	Windows
Hardware	
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	Loaris, Inc. (Bulgaria)
Availability	*http://www.loaris.com/trojanremover/*

McAfee® VirusScan

Abstract

VirusScan for PCs and servers proactively stops and removes malicious software and extends coverage against new security risks by blending anti-virus, firewall, and intrusion prevention technologies to cover a broad range of threats. Advanced heuristics and generic detection capabilities find new, unknown viruses, even when hidden in compressed files. McAfee VirusScan looks for exploits known to target Microsoft applications and services, and can identify and block threats that take advantage of JavaScript and VisualBasic coding. The McAfee VirusScan database is updated daily with information from McAfee Avert Labs.

VirusScan for Mac performs non-intrusive, on-access scanning for viruses, worms, Trojans, and other malicious code, including new and unknown threats that target OS X. As with VirusScan for PCs, VirusScan for Mac is supported by McAfee Avert Labs' VirusScan database.

VirusScan USB detects and removes viruses that can delete files and data from a USB drive. Additionally, this software ensures that the USB drive does not transmit viruses and other threats to each PC that connects with the USB drive.

VirusScan Plus 2009 is McAfee's home user edition, which protects PCs from viruses and spyware (in addition, it includes a firewall and a subscription to McAfee's SiteAdvisor online safety guide and list of risky Web sites).

In addition to its standalone anti-virus products, McAfee includes its virus scanning technology in its other cyber security and external security manager (ESM) products and solutions, such as its WebShield SMTP and Email and Web Security appliances.

VirusScan

Type	Virus detection and removal
OS	*VirusScan 8.7i for Workstation, VirusScan Plus 2009, VirusScan USB (scanner platform)*—Windows 2000, XP, Vista *VirusScan 8.7i for Server*—Windows 2000 Server, Server 2003, Server 2003 R2, 2008 Server *VirusScan for Mac*—Mac OS X Tiger® (10.4.6 or later), Leopard ® (10.5 or later) *VirusScan for Windows*—Windows 2000, XP, Vista 32-bit
Hardware	*VirusScan 8.7i for Workstation*—Intel Pentium or Celeron® 166 MHz; 32 MB RAM; 38 MB free disk space *VirusScan 8.7i for Server*—Intel Pentium, Celeron, Itanium 166 MHz; 32 MB RAM; 38 MB free disk space *VirusScan Plus 2009*—800x600 dpi monitor; 256 MB RAM; 75 MB free disk space; Internet connection *VirusScan for Mac*—Intel or PowerPC Macintosh; 512 MB RAM; 45 MB free disk space *VirusScan USB devices scanned*—U3® platform (for Vista, U3 LaunchPad also required); scanner platform—Pentium 300 MHz, 128 MB RAM, U3 USB smart drive, 25 MB free disk space (SanDisk® preferred)
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	McAfee
Availability	*http://www.mcafee.com/us/small/products/virusscan_for_mac/virusscan_for_mac.html* *http://www.mcafee.com/us/small/products/virusscan/virusscan_enterprise.html* *http://home.mcafee.com/store/package.aspx?pkgid=276*

Mischel Internet Security TrojanHunter 5.1

Abstract

TrojanHunter is able to clean parasitic Trojans by working inside the infected process to kill all Trojan threads and then unload the loaded Trojan libraries. After this, TrojanHunter can safely clean the Trojan library, while the previously infected process can continue executing as if nothing happened.

TrojanHunter 5.1

Type	Trojan detection and removal
OS	Windows 95, 98, ME, NT, 2000, XP and Vista
Hardware	
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	Mischel Internet Security Ltd. (United Kingdom)
Availability	*http://www.misec.net/Trojanhunter/*

My Free Antivirus

Abstract

My Free Antivirus is a unique algorithm of scanning, high speed of detection, daily anti-virus base updates, protection from cyber viruses, Trojans, worms. The Free Antivirus real-time protection module allows you to prevent malware intrusion attempts. My Free Antivirus is undemanding toward computer resources and completely compatible with Microsoft Windows versions, including Windows Vista. The Free Antivirus has an easy-to-use interface and a small-size distributive that is a powerful anti-virus tool. The tool comes in versions for scanning PCs and for scanning U3 flash drives.

My Free Antivirus

Type	Virus detection and removal
OS	Windows NT, 2000, XP, 2003, Vista
Hardware	
License	Freeware
NIAP Validated	No
Common Criteria	
Developer	Smart PC Solutions, Inc.
Availability	*http://smartpctools.com/free_anti-virus/index1.html* *http://smartpctools.com/free_anti-virus_u3/index1.html*

New Technology Wave Virus Chaser

Abstract

Virus Chaser provides protection against executable virus files compressed up to 64 times with ASPack or Ultimate Packer for eXecutables into .zip, .arj, .rar, and .cab compression file formats. The took uses heuristic technology to detect unknown virus variants in system memory, emails/attachments, and HTML Web pages. Virus Chaser signature files are typically updated four to five times per day; during times of peak virus activity, updates may be as numerous as 200 to 400 per day.

Virus Chaser is offered in Client, Server, and USB editions. Virus Chaser USB is a USB 2.0 thumb drive (1 GB, 2 GB, or 4 GB) with a minimized version of Virus Chaser installed (that takes up 8 MB of space on the solid state memory chip). All files written to and read from the drive are automatically scanned and, if infected, blocked. Virus Chaser Management Server is also offered for central management, monitoring, and reporting on multiple endpoints running Virus Chaser.

Virus Chaser	
Type	Malware detection and removal
OS	*Client*—Windows 95/98/ME/2000 Professional/XP/Vista (32-bit); *Server*—Windows NT/2000 Server/2003; *USB*—PC must have one of the following installed for Virus Chaser to work—Windows 98/98SE/2000/XP/2003; if used with a Macintosh or Linux system, the device will function as a USB storage drive but Virus Chaser will not function. *Management Server*—Windows 2000 or later; *1-99 managed endpoints*—also need Microsoft SQL Server Desktop; *100-499 management endpoints*—also need Microsoft SQL Server 2000 7.0
Hardware	*Client*—Pentium 133 MHz, 16 MB RAM (32 recommended), 8 MB free disk space; *Server*—Pentium 133 MHz, 16 MB RAM (32 recommended), 8 MB free disk space; *Management Server—1-99 managed endpoints*—Pentium III 500 MHz, 128 MB RAM; *100-499 managed endpoints*—Pentium III 800 MHz, 256 MB RAM
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	New Technology Wave Inc. (Korea)
Availability	*http://www.viruschaser.com/enwi/2_01.jsp* *http://www.viruschaser.com/enwi/2_02.jsp* *http://www.viruschaser.com/enwi/2_03.jsp* ßhttp://www.viruschaser.com/enwi/2_04.jsp

PC Tools AntiVirus 6.0.0.19

Abstract

PC Tools AntiVirus is an anti-virus scanner with hourly signature updates. PC Tools AntiVirus can be obtained separately, or in combination with PC Tools' other cyber security products, including SpywareDoctor and Internet Security Suite.

AntiVirus 6.0.0.19	
Type	Virus detection and removal
OS	Windows Vista, XP, 2000
Hardware	
License	Freeware
NIAP Validated	No
Common Criteria	
Developer	PC Tools
Availability	*http://www.pctools.com/anti-virus/*

Smart PC Solutions Handy Antivirus

Abstract

This anti-virus solution has a unique algorithm of scanning, high speed of detection as well as daily updates. Handy Antivirus has a real-time protection mode that allows you to prevent malware intrusion attempts. The anti-virus has a user-friendly control, which includes a Handy Antivirus control bar in the upper menu of the browser. By a single click of the mouse, the user can update anti-virus base or check a file on the case of infection.

Handy Antivirus	
Type	Virus detection and removal
OS	Windows NT, 2000, XP, 2003, Vista
Hardware	
License	Freeware
NIAP Validated	No
Common Criteria	
Developer	Smart PC Solutions, Inc.
Availability	*http://smartpctools.com/handy_anti-virus/*

VirusBlokAda Vba32

Abstract

The Vba32 line of products produced by VirusBlokAda is based on the company's proprietary anti-virus engine. Vba32 detects and neutralizes computer viruses, mail worms, Trojan programs, and other malware (*e.g.,* backdoors, adware, spyware) in real time and on-demand on PCs running Windows, as well as workstations, file servers, mail servers, and a variety of anti-virus filters for Linux/FreeBSD mail servers.

The tool includes a heuristic analyzer that can detect unknown malicious programs and a dynamic code translation processor emulator to handle complex polymorphous viruses, packers, and encryptors. MalwareScope performs the actual malware detection. Program module and anti-virus database updates are done over the Internet using the tool's "delta-patch" technology. The Vba32 products include integrity control and automatic restoration of damaged modules to improve their reliability.

VirusBlokAda offers anti-virus scanners for PCs, consoles, networked workstations, file servers, and mail servers.

VirusBlokAda Vba32

Type	Trojan detection and removal
OS	*Vba32.P*—Windows 95, 98, ME, NT, 2000, XP, 2003 *Vba32.CL*—consoles in DOS, Windows, Linux, FreeBSD *Vba32.W*—Windows *Vba32.NT.S*—Windows NT, 2000, 2003 *Vba32.9X.N*—Windows 95, 98, ME *Vba32.LDS*—Windows and Linux *Vba32.MSE and VBA32.ME2K*—Windows *Vba32.SM, Vba32.MD, Vba32.EX, Vba32.CP, Vba32.QM, Vba32.PF, Vba32.IC*—Linux/UNIX
Hardware	
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	VirusBlokAda Ltd. (Belorussia)
Availability	*http://www.anti-virus.by/en/*

Your-Soft Anti-Virus&Trojan

Abstract

Anti-Virus&Trojan uses the same Guard Ghost system found in Your-Soft's Trojan Guarder to supervise all running processes in the memory system, Windows files, and open ports, searching them for viruses, worms, and Trojan horses. If malware appears, even hidden in other programs, Anti-Virus&Trojan displays a warning signal and eliminates the malware, then clears all linked files and relative registered files associated with the removed malware.

Anti-Virus&Trojan	
Type	Virus, worm, and Trojan detection and removal
OS	Windows
Hardware	
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	Your-Soft (United Kingdom)
Availability	*http://www.your-soft.com/*

Your-Soft Trojan Guarder 6.50 and Trojan Guarder Gold 7.74

Abstract

Trojan Guarder is designed to work with a system's existing anti-malware solution. Its Guard Ghost system supervises all running processes in memory system, Windows files, and open ports to locate and eliminate worms and Trojan horses as they run within the system.

Trojan Guarder Gold kills unknown Trojans, spyware, and viruses, and it includes an anti-Trojan firewall function and more robust virus-detection functions than the standard edition. This system, called IE Doctor, can recover any damage caused by JavaScript and ActiveX viruses, and can prevent hackers from attacking the PC's installed browser.

Trojan Guarder

Type	Virus detection and removal
OS	Windows
Hardware	
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	Your-Soft (United Kingdom)
Availability	*http://www.your-soft.com/download.htm*

ZoneAlarm® Antivirus 2009

Abstract

ZoneAlarm Antivirus 2009 has enhanced detection and removal capabilities to stop viruses before they infect the PC. The product combines anti-virus, with OS-, network-, and application-level firewalls.

ZoneAlarm Antivirus 2009	
Type	Virus detection and removal, plus system, network, and application level firewall functionality
OS	*Vista*—2 GHz CPU with 2 GB (32-bit) or 4 GB (64-bit) RAM, 250 MB of free disk space *XP*—1 GHz 32-bit CPU with 768 MB RAM, 250 MB of free disk space Requires Internet access.
Hardware	
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	ZoneAlarm Labs (owned by Checkpoint)
Availability	*http://www.zonealarmstore.com/products/zonealarm-anti-virus-2009/*

4.3.1.3 Anti-Spyware Tools

The tools described in this section are understood to address only spyware, including, but not limited to, keyloggers, adware, browser helper objects, and tracking cookies.

AdWareAlert

Abstract

AdWareAlert detects and removes adware, spyware, Trojans, dialers, worms, *etc.*, and scrubs programs on the infected system to ensure that no harmful remnants are left behind. AdWareAlert provides online updates to ensure protection from the latest threats.

AdWareAlert	
Type	Spyware detection, blocking, and removal
OS	Windows 98, ME, XP, 2000, Vista
Hardware	
License	Freeware
NIAP Validated	No
Common Criteria	
Developer	AdWareAlert.com
Availability	*http://adwarealert2009.com/index.php*

AhnLab SpyZero 2007

Abstract

SpyZero uses its proprietary anti-spyware engine to prevent spyware outbreaks and to detect and remove spyware and adware. The tool performs diagnostics such as registry scans and file size checking, and prevents reinstallation of spyware-infected ActiveX programs. The tool also protects against unexpected changes in users' Web browsers and blocks unwanted pop-up advertisement windows.

SpyZero 2007

Type	Spyware detection, blocking, and removal
OS	Windows 98, ME, NT 4.0 Workstation, 200 Professional, XP
Hardware	Pentium II (Pentium III recommended), 128 MB RAM (256 MB recommended), 100 MB free disk space (300 MB recommended)
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	AhnLab, Inc (China)
Availability	*http://global.ahnlab.com/global/prod_detail.ESD?parmProd_class=C&parmProd*_type= CM&prod _seq=1023

CA Anti-Spyware 2009

Abstract

CA Anti-Spyware 2009 performs spyware detection and removal to protect against a wide range of spyware, adware, keyloggers, browser hijackers, and similar threats. Real-time protection detects and removes spyware running in memory, and helps prevent spyware from making malicious changes to the Windows registry. Scheduled and on-demand scans enable the user to run a scan at any time, or schedule scans at pre-selected intervals. Scans can be customized, enabling the user to select specific drives, files and folders to scan, and to specify a file exclusion list of files and folders to skip. The scanner produces detailed results indicating the specific threat level of any spyware found, and enabling the user to access the CA Spyware Information Center for more details. CA provides frequent automatic updates of spyware signatures. The tool was certified by West Coast Labs as providing effective spyware protection. Anti-Spyware 2009 is also included in the CA Internet Security Suite.

Anti-Spyware 2009

Type	Malware detection and removal
OS	Windows 2000, XP, or Vista
Hardware	300 MHz CPU (800 MHz for Vista), 256 MB RAM (512 MB for Vista), 35 MB free disk space
License	GPL
NIAP Validated	No
Common Criteria	
Developer	CA
Availability	*http://shop.ca.com/spyware/anti_spyware.aspx*

Crawler Spyware Terminator

Abstract

Spyware Terminator scans for and removes known spyware on computers. Spyware Terminator supports customizable on-demand and scheduled scanning with reporting to the user of the system state. The tool removes all detected threats, including removing at system reboot those files that have been locked by the system, and which are therefore not removable by standard methods. It supports quarantine of potentially harmful items without full deletion to allow the user to investigate and determine whether or not those items are actually malicious and need to be deleted; users may send these files to the Spyware Terminator analysis team for deep inspection, with those found to be malicious added to the tool's threat signature database.

Up to ten Real-time Shields can be installed (32-bit computers only) to intercept and disable threats before they can install themselves. The tool also performs automatic updates from the Crawler, LLC spyware signature database. The product comes bundled with ClamAV, which provides real-time virus detection and removal, and with a host intrusion prevention system to block undefined threats from executing on the system.

Restoration capabilities include cooperation with Windows System Restore to return Windows to its pre-infection state, and browser restoration, which returns the sanitized browser to its original default settings. Automatic updating of the tool's installed signature database is performed in the background, and can also be performed on demand.

Spyware Terminator

Type	Virus and spyware detection and removal
OS	Windows XP 32-bit, XP 64-bit, Vista 32-bit and Vista 64-bit *Note—Real-time Protection operates on Windows XP 32-bit and Vista 32-bit only.*
Hardware	10 MB free disk space; monitor/screen with 800x600 pixel resolution or better
License	Freeware
NIAP Validated	No
Common Criteria	
Developer	Crawler, LLC
Availability	*http://www.spywareterminator.com/*

Enigma Software Group SpyHunter® v.3

Abstract

SpyHunter scans the computer hard drive for files, Windows registry settings, Message Digest 5 (MD5) file signatures, and other indicators of thousands of spyware (including keylogger, identity theft, tracking cookies, rogue anti-spyware, unwanted software, browser hijackers), Trojan, adware, worm, and malware threats. The tool also blocks phishing exploits (*e.g.,* browser hijackers), pop-ups, and malicious Web sites. Enigma also offers its Spyware Helpdesk service to SpyHunter users; if SpyHunter is unable to identify a suspicious object it provides the user with the option to transmit a diagnostic report to the Spyware Helpdesk Support Center, where the report is reviewed, and within 24 hours the user is sent a unique fix to remove the suspicious object and its traces from the user's system.

SpyHunter	
Type	Spyware detection, prevention, and removal
OS	Windows Vista, XP, 98, ME, 2000
Hardware	
License	Freeware (Spyware Helpdesk is a commercial service)
NIAP Validated	No
Common Criteria	
Developer	Enigma Software Group
Availability	*http://www.enigmasoftware.com/spyhunter_more_info.php*

iS3 STOPzilla®

Abstract

STOPzilla detects, blocks, and quarantines spyware, adware, rogue programs, keyloggers, malicious BHOs, dialers, Trojans, *etc.* The tool kills browser hijackers, removes rootkits, and prevents bots from installing. The tool also blocks pop-ups, messenger service ads, phishing exploits, drive-by downloads, and connections to known-malicious Web-sites. STOPzilla is designed to minimize the need for user interaction. Scans can be on-demand or automatic, and automatic updating can also be configured.

STOPzilla

Type	Spyware detection, blocking, and removal
OS	Windows Vista (32 bit), XP, 2000, ME, 98
Hardware	
License	Freeware (Spyware Helpdesk is a commercial service)
NIAP Validated	No
Common Criteria	
Developer	iS3
Availability	*http://www.stopzilla.com/products/stopzilla/home.do*

ISecSoft Anti-Keylogger Elite v3.3.3

Abstract

Anti-Keylogger Elite is a utility designed to detect keyloggers and give the user the power to disallow or allow the keylogger to function. The tool can prevent known and unknown keyloggers from infiltrating a computer and logging everything the user types on the keyboard and sees on the screen.

Anti-Keylogger Elite v3.3.3

Type	Keylogger detection and removal
OS	Windows 2000, XP, 2003
Hardware	
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	ISecSoft, Inc. (China)
Availability	*http://www.remove-keyloggers.com/*

McAfee AntiSpyware

Abstract

McAfee AntiSpyware catches spyware and other "potentially unwanted programs" (PUP) before they can install themselves, so that this unwanted software cannot spawn other programs or files that install themselves in PC applications or registry entries. Using behavioral-based methods and daily registry-signature updates, McAfee AntiSpyware finds and blocks both known and unknown spyware. The AntiSpyware and PUP database is maintained by McAfee Avert Labs.

In addition to its standalone anti-spyware product, McAfee includes its anti-spyware technology in its other cyber security and ESM products and solutions, such as its Web Security appliance.

AntiSpyware

Type	Spyware detection and removal
OS	*Workstation*—Windows NT 4, 2000, 2003, XP, Vista *Server*—Windows NT 4 Server, 2000 Server, Server 2003
Hardware	
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	McAfee
Availability	*http://www.mcafee.com/us/small/products/anti_spyware/anti_spyware.html*

Microsoft Windows Defender

Abstract

Windows Defender is a spyware detection and removal tool included with Windows Vista; it is also available for free download for use with previous editions of Windows. Windows Defender supports real-time analysis of running software to detect installed spyware while working to prevent spyware from successfully installing in the first place.

Microsoft Windows Defender

Type	Spyware detection and prevention
OS	Windows XP and later
Hardware	
License	Free
NIAP Validated	No
Common Criteria	
Developer	Microsoft Corporation
Availability	*http://www.microsoft.com/windows/products/winfamily/defender/default.mspx*

Neuber Software Anti-Spy.Info

Abstract

Anti-Spy.Info is intended to complement anti-virus and firewall tools by detecting and removing spyware, Trojans, keyloggers, and adware. Anti-Spy.Info reveals every hidden function of all running tasks or background processes currently active on the computer. The tool also—

- Prevents keyboard and mouse monitoring;
- Warns whether the registry is changed;
- Protects the registry from Trojans that add an autostart key;
- Eliminate traces of the user's Internet activity, such as cookies, cache, history, typed URLs, and temporary files;
- Eliminates traces of the user's work on the computer, such as a list of recent used programs (e.g. Word, ACDSee®, PDF, WinZip®, media player).

Anti-Spy.Info

Type	Spyware detection and removal
OS	Windows
Hardware	
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	Neuber Software GmbH (Germany)
Availability	*http://www.anti-spy.info/*

NoAdware 5.0

Abstract

NoAdware scans PCs for spyware, adware, dialers, and Web bugs. The user can run manual scans, or schedule scans to run automatically. The tool also enables the user to disable the "Do you want to install?" pop-up window associated with downloads, and instead the tool monitors all attempted downloads of adware/spyware and simply blocks installation of any code that appears on its "block" list. The tools enables the user to configure additional shields for their browsers and system, to prevent detected spyware/adware from executing, to prevent sites that serve spyware/adware from adding their URLs to the IE browser's "favorites" list, and to request explicit user authorization to add any URL to their IE "favorites" lists.

NoAdware 5.0

Type	Spyware detection, blocking, and removal
OS	Windows
Hardware	
License	Freeware
NIAP Validated	No
Common Criteria	
Developer	NoAdware.net
Availability	*http://www.noadware.net/*

ParetoLogic XOFTspy® Portable Anti-Spyware, XoftSpySE Anti-Spyware

Abstract

XOFTspy Portable is designed to be installed and run from U3 USB platforms and SmartDrives. The tool scans both the PC to which the USB drive is connected and the drive itself. Its features are otherwise the same as those of XOFTSpySE Anti-Spyware.

XOFTSpySE scans scan the entire PC to detect adware, spyware, pop-up generators, keyloggers, Trojans, hijackers, W32/Spybot, browser hijackers, and other malware, and quarantines any infected files it detects. The user is then able to review and remove the quarantined files.

XOFTspy Portable, XosftSpySE

Type	Spyware detection and removal
OS	*XOSFTspy Portable*—Windows 2000 or XP; IE 6.0; *XoftSpySE*—Windows 98, ME, 2000, XP; IE 6.0
Hardware	*XOSFTspy Portable*—Pentium II, 64 MB RAM; *USB device*—8 MB free SmartDrive space; *XoftSpySE*—Pentium II, 64 MB RAM, 10 MB free disk space
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	ParetoLogic Inc. (Canada)
Availability	*http://www.paretologic.com/products/xoftspypa/index.aspx* *http://www.paretologic.com/products/xoftspyse/index.aspx* *http://www.xoftspy.net/products.aspx*

PC Tools SpywareDoctor 6.0.1.441

Abstract

SpywareDoctor detects, removes, and protects PCs from spyware, adware, spyware Trojans, keyloggers, rogue anti-spyware, and other unwanted software, as well as identity theft, hijacking, phishing, and tracking threats, pop-ups, and bad Web sites.

It performs malware detection and termination, hidden process detection, and unauthorized hook detection.

SpywareDoctor can be obtained separately, or in combination with PC Tools AntiVirus, or in a PC Tools Internet Security Suite that includes all of PC Tools cyber security (SpamMonitor and FirewallPlus) and anti-malware components.

PC Tools SpywareDoctor 6.0.1.441

Type	Spyware detection and removal
OS	Windows Vista 64, XP, 2000
Hardware	
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	PC Tools
Availability	*http://www.pctools.com/spyware-doctor/*

Rnsafe Spyware Cleaner 2009 2.03

Abstract

Spyware Cleaner scans memory, registry, hard drives, and external storage to find and remove spyware, adware, Trojans, keyloggers, home page hijackers, and other malware threats. Scanning can be configured to scan only certain areas of the computer or to skip specified files/folders. Detected threats are quarantined, and the tool provides a Junk Files Cleaner and registry Cleaner for eliminating the traces of eliminated spyware. The Host Files Editor enables the user to specify (by IP address) ad sites and other sites to be blocked, including sites suspected of originating Web browser hijacking attacks. The tool also provides an Update Manager with an automated "check for updates" feature, and a "submit for analysis" feature that enables the user to send quarantined spyware to Rnsafe or another recipient (identified by email address) for deeper analysis.

Spyware Cleaner 2009 2.03

Type	Spyware detection and removal
OS	Windows NT, 2000, XP, 2003, Vista
Hardware	
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	Rnsafe (China)
Availability	*http://www.rnsafe.com/buy.html*

Safer Networking Spybot - Search & Destroy 1.6.2

Abstract

Spybot - Search & Destroy (Spybot-S&D) detects, "shreds" (destroys), and removes spyware, adware, browser helper objects, browser hijackers, dialers, keyloggers, Trojans, and other possibly unpopular software, as well as the user's computer usage tracks, and blocks threatening ActiveX downloads, tracking cookies and browser downloads (IE only). The tool backs up copies of all detected threats for analysis. Automatic scans can be scheduled, and tasks can be automated through a command line interface. Spybot-S&D provides the ability to fix some registry inconsistencies and to generate extended reports.

Spybot - Search & Destroy 1.6.2

Type	Spyware detection, destruction, and removal
OS	Windows 95, 98, ME, NT, 2000, XP, 2003, Vista, 2008, PE; Linux/UNIX (with Wine support)
Hardware	
License	Freeware
NIAP Validated	No
Common Criteria	
Developer	Safer Networking Ltd. (Ireland)
Availability	*http://www.safer-networking.org/en/download/index.html*

SecureMac® MacScan® 2.6.1

Abstract

MacScan detects, quarantines, and removes spyware Apple computers running Mac OS X. The tool recognizes over 8,000 known malicious tracking cookies. Scans can be performed on-demand or scheduled in advance. The tool's Blacklisted Cookie Scan feature enables the user to remove blacklisted tracking cookies without losing their saved usernames and passwords.

MacScan 2.6.1

Type	Spyware detection and removal
OS	Mac OS X
Hardware	
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	SecureMac.com, Inc.
Availability	*http://macscan.securemac.com/*

Security Stronghold True Sword

Abstract

True Sword protects computers against malicious programs that harm those computers and violate user privacy. These programs include spyware, Trojans, adware, trackware, dialers, keyloggers, and other kinds of threats. True Sword scans hard disks, registry, and processes and removes all malicious software found. It also removes malicious BHOs and tracking cookies.

The product comes in home/home office and corporate editions. The latter protects 10 to 10,000 networked computers from over 300,000 varieties of spyware, adware, Trojans, trackware, and other privacy-violating malware.

True Sword	
Type	Spyware detection and removal
OS	Windows 2000, XP, 2003, Vista
Hardware	
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	Security Stronghold (Russian Federation)
Availability	*http://www.securitystronghold.com/true_sword.html* *http://www.securitystronghold.com/business/true-sword-corporate/*

Sunbelt Software CounterSpy®, CounterSpy Enterprise, CounterSpy Gateway SDK

Abstract

CounterSpy shares the features of Sunbelt's VIPRE anti-malware tool, but focuses only on detecting spyware; it provides no anti-virus capabilities. CounterSpy uses an extensive spyware signature database, real-time security agents, and ThreatNet "neighborhood watch" for spyware, to protect against many types of spyware, adware, browser hijackers, search hijackers, keyloggers, ghost spammers, spy software, and other hazardous applications and files that violate the user's privacy. CounterSpy is powered by a hybrid engine that merges spyware detection and remediation with malware protection. FirstScan executes when triggered by a CounterSpy scan to root out deeply embedded malware before Windows loads.

When spyware is located, a results page is displayed, allowing the user to see details of every spyware threat found, along with descriptions of the threat, files and settings located on the computer, advice on handling the threat, risk rating associated with the threat, and a recommended course of action, with options to remove, ignore, or quarantine the threat. If quarantined, the threat is deactivated and removed to a safe data store, after which the user can either delete or restore the quarantined file.

The tool's real-time Active Protection agents monitor the computer 24/7, securing certain areas. When specific checkpoints are breached, the activity is immediately analyzed against CounterSpy's database of known file and setting signatures, allowing unthreatening changes to be made; and alerting the user to any potential spyware installations. In this way, Active Protection intercepts many potential hazards in real-time and helps the user decide what software should be allowed access to his/her system. As for browser support, CounterSpy's Active Protection currently only monitors browser-specific changes in IE.

CounterSpy Enterprise provides the same anti-spyware features as CounterSpy, but adds centralized management *via* the same dashboard found in VIPRE Enterprise (described in Section 4.3.1.1).

Sunbelt Software also offers the CounterSpy Gateway SDK to enable OEMs and service providers to integrate CounterSpy into their security gateway packages and appliances.

CounterSpy, CounterSpy Enterprise, CounterSpy Gateway SDK

Type	Spyware detection, blocking, and removal
OS	Windows 2000, Server 2003, Server 2008, XP, Vista
Hardware	IBM-compatible 400 MHz CPU, 512 MB RAM, 150 MB free disk space, 2x CD reader, Internet access (56 Kbps minimum) For console requirements, see VIPRE Enterprise (Section 4.3.1.1)
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	Sunbelt Software, Inc.
Availability	*http://www.sunbeltsoftware.com/Home-Home-Office/Anti-Spyware/* *http://www.sunbeltsoftware.com/Business/CounterSpy-Enterprise/* *http://www.sunbeltsoftware.com/Government/CounterSpy-Enterprise/* *http://www.sunbeltsoftware.com/Developer/CounterSpy-Gateway-SDK/*

SuperAntiSpyware® Professional Edition

Abstract

SuperAntiSpyware detects, quarantines, and removes spyware, adware, malware, Trojans, dialers, worms, keyloggers, hijackers, parasites, rootkits, rogue security products, and other threats. Detection is based on both recognition of code patterns and analysis of threat characteristics. The tool's Process Interrogation Technology enables detection of threats hiding anywhere on the system, including threats that use rootkits or kernel drivers to avoid detection. The tool blocks threats in real-time to prevent installation or re-installation of potentially harmful software. The tool automatically scans more than 50 critical areas of the PC when it starts up and shuts down to eliminate threats before they can infiltrate and infect the system. Scans can be manual, or scheduled daily or weekly, and can be "quick," "complete," or "custom." The tool provides the user the ability to easily repair broken Internet connections and desktops and edit registry entries.

SuperAntiSpyware Professional Edition

Type	Spyware detection, blocking, and removal
OS	Windows 98, 98SE, ME, 2000, XP, Vista or Windows 2003
Hardware	400 MHz CPU, 256 MB RAM
License	Commercial/Freeware (offered free for personal/home use; scheduling and daily signature updates only available with professional edition)
NIAP Validated	No
Common Criteria	
Developer	SUPERAntiSpyware.com
Availability	*http://www.superantispyware.com/*

SystemSoftLab Spyware Process Detector

Abstract

Spyware Process Detector is an anti-spyware tool that will detect all processes running on the computer and display their threat rating based on the intelligent analysis of all hidden properties. Another specialty of the program is its ability to detect a process that contains and executes alien code of another process. Users will at a glance see the detailed information about any selected process and detect all hidden threats, including spyware, malware, keyloggers, and Trojans. Seventeen methods of process detection are available.

Spyware Process Detector

Type	Spyware detection and removal
OS	Windows 2000, XP, 2003, Vista
Hardware	Pentium (Pentium II 500 MHz recommended)
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	SystemSoftLab (Russian Federation)
Availability	*http://www.systemsoftlab.com/spydetector.html*

Unlike standard Windows Task Manager, Spyware Process Detector will detect even those processes and tasks that are transparent to OS. The security rating is color-coded so that users can see the most dangerous processes at once. Red stands for the highest rating of danger, and green for the lowest one; any color between red and green stands for varying levels of security threat. The program shows other details about each process, such as process ID, parent ID, security status, *.exe* filename, file path, description, *etc.* Startup Manager shows details information about processes that run on Windows startup. Once there is a process marked out as red or yellow, users have to choose whether to delete it or mark as safe. The current list of processes can be exported to the Excel format for further analysis.

The program detects new (undetectable by typical anti-virus scanners) spyware, Trojans, and viruses.

TrendMicro Transaction Guard

Abstract

This free tool, intended for use when performing Internet banking, shopping, and similarly sensitive online transactions that involve transmission of personal and personally identifiable information, consists of—

- **Spyware Monitor**—Monitors for spyware and notifies the user of any intrusions;
- **Password ClipBoard**—An on-screen keyboard for securely entering user names and passwords to thwart keyloggers.

Transaction Guard	
Type	Spyware detection and avoidance
OS	Windows 2000, XP, Vista
Hardware	
License	Freeware
NIAP Validated	No
Common Criteria	
Developer	TrendMicro
Availability	*http://www.trendsecure.com/portal/en-US/tools/security_tools/transaction_guard*

Usec.at Nemesis Antispyware

Abstract

Nemesis protects PCs against a wide range of spyware threats *via* routine and advanced registry scans and repairs. Nemesis provides the following capabilities—

- Scans for spyware, adware, dialer attacks, and hijackers;
- Provides optional quarantine for later threat analysis;
- Provides registry backup for later investigation;
- Performs full-service scans whereby novice users can perform a one-click scan to find and eliminate all known infections, while advanced users can use granular control of individual scans and deletions.
- Scans memory, registry (including deep registry scanning), Windows startup regions, BHOs, file associations, Ini files, IE settings;
- Provides protection for IE settings and *hosts* file;
- Automatically blocks known bad servers in *hosts* file;
- Provides Winsock LSP fix for malware such as Webhancer or New.net;
- Includes a *hosts* file editor;
- Enables secure file deletion;
- Includes auto-update functionality;
- Provides an interface for sending detected spyware threats to an expert for thorough analysis;
- Includes reporting options, including "send," "mail," and "save" handling of reports;
- Enables configuration of report names for further processing;
- Point-and-click graphical user interface (GUI) for novice users.

Nemesis Antispyware

Type	Spyware detection and removal
OS	Windows
Hardware	
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	Usec.at (Austria)
Availability	*http://usec.at/downloads/Nemesis_installer.exe*

Webroot Software AntiSpyware Corporate Edition 3.5 and Spy Sweeper® 6.1

Abstract

Webroot AntiSpyware Corporate Edition is a centrally managed, scalable enterprise solution that uses Webroot's Spy Sweeper technology to protect against all types of malicious spyware, adware, and keyloggers. The tool comprehensively detects and removes existing spyware, and blocks new threats before they infect PCs.

Spy Sweeper provides detection and removal capabilities, even for difficult-to-eliminate spyware. Spy Sweeper's Smart Shields block sophisticated spyware threats in real-time, before they can infect a PC. Spy Sweeper also discovers and destroys rootkits. The user can configure the tool to perform a quick, full, or customized scan. Gamer Mode enables users to temporarily defer scheduled activities, alerts, and updates when they are playing online games, while continuing to run the tool's shield technology in the background. Webroot's VersionGuard automatically downloads and installs updates to Spy Sweeper as soon as they are released.

Webroot AntiSpyware

Type	Spyware detection and removal
OS	*AntiSpyware*—Windows Vista, 2000 Professional or Server (SP 4), XP Professional (SP 2), 2003 Standard, Enterprise, R2, or Small Business Server (SP1); Spy Sweeper—Windows Vista, XP
Hardware	*AntiSpyware*—1 GHz CPU, 1 GB RAM, 1 GB free disk space; Spy Sweeper—300 MHz CPU, 256 MB RAM, 100 MB free drive space
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	Webroot Software, Inc.
Availability	*http://www.webroot.com/En_US/business-antispyware-ce.html* *http://www.webroot.com/En_US/consumer-products-spysweeper.html*

Your-Soft Anti-Virus&Spyware

Abstract

Anti-Virus&Spyware detects and removes spyware, adware, and tracking files (such as tracking cookies and Web browser plug-ins).

Anti-Virus&Spyware

Type	Spyware detection and removal
OS	Windows
Hardware	
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	Your-Soft (United Kingdom)
Availability	*http://www.your-soft.com/*

4.3.1.4 Anti-Rootkit Tools

The tools described in this section are understood to address rootkits.

Andres Tarasco's RKDetector v2.0

Abstract

RKdetector is advertised as a "security analyzer, rootkit removal, and runtime forensic analysis" tool. It comprises two modules—

- **FILESYSTEM Module**, which performs detection and secure deletion of rootkits and data recovery subsequent to deletion;
- **IAT Analysis Module**, which performs analysis and "fixing" of the system IAT, plus scanning of the associated database.

For support, the user is directed to visit a Spanish-language security tools blog/portal at *http://www.shellsec.net/*.

RKDetector v2.0

Type	Rootkit detection
OS	Windows
Hardware	
License	Freeware
NIAP Validated	No
Common Criteria	
Developer	Andres Tarasco (Spain)
Availability	*http://www.rkdetector.com/*

Christian Hornung's OS X Rootkit Hunter 0.2

Abstract

OS X Rootkit Hunter is scanning tool that detects backdoors, rootkits, and local exploits on Macintosh computers running OS X by running such tests as MD5 hash comparisons and scanning for default files used by rootkits, inappropriate file permissions assigned to binary files, suspect strings in Linux Kernel Module (LKM) modules, hidden files, and scans within plaintext and binary files.

According to its developer, OS X Rootkit Hunter is adapted from Michael Boelen's UNIX/Linux-based Rootkit Hunter, which is described elsewhere in this Tools Report. Please refer to that tool's abstract for a more complete description of Rootkit Hunter's capabilities.

OS X Rootkit Hunter 0.2

Type	Rootkit detection
OS	Macintosh OS X 10.4 or later
Hardware	PowerPC (not yet tested on Intel-based Macintoshes)
License	Freeware
NIAP Validated	No
Common Criteria	
Developer	Christian Hornung (Germany)
Availability	*http://www.christian-hornung.de/*

DiabloNova's Rootkit Unhooker (RkU)

Abstract

Rootkit Unhooker can detect kernel hooks, hidden processes, hidden drivers, hidden files, and code hooks. If the tool finds an offending or suspect process, the user can terminate the detected process normally, force it to close, and/or erase the process' executable file. The user can even force a "blue screen of death" if the process cannot be killed by less aggressive means.

The tool's Virtual Machine Detector uses the time elapsed between two low-level CPU instructions to determine whether the OS is running directly on the hardware or in a virtual machine. This enables it to detect rootkits that wrap the victim OS in a virtual machine. Before running, Rootkit Unhooker conducts an integrity self-test to ensure that it is not itself being subverted by a rootkit.

Note—The Rootkit Unhooker project was discontinued when Microsoft purchased it in November 2007. However, as of October 2008, the Russian developer DiabloNova (also known as Alpha & Omega) claimed to still support the product, which was last updated September 2008.

Rootkit Unhooker (RkU) v3.8.342.554

Type	Rootkit detection
OS	Windows 2000, XP, 2003, Vista
Hardware	x86
License	Freeware
NIAP Validated	No
Common Criteria	
Developer	DiabloNova (Russian Federation)
Availability	*http://www.woodmann.com/collaborative/tools/index.php/Rootkit_Unhooker* *Note—This is one of many sites from which RkU can be downloaded.*

F-Secure BlackLight Rootkit Eliminator

Abstract

BlackLight Rootkit Eliminator detects hidden files, folders, and processes that are hidden from the user and other programs, including security tools. BlackLight also provides the user the option of removing the discovered hidden objects, which may include malware; it does this by renaming them so they can be detected and deleted. The main purpose of BlackLight is to find and eliminate active rootkits that are not detectable by standard anti-malware software, and to remove malware that uses rootkits.

BlackLight Rootkit Eliminator was developed for use by F-Secure's own Response Lab. F-Secure also makes the tool available for free download, but provides no product support to those who download it.

BlackLight Rootkit Eliminator

Type	Rootkit detection and removal
OS	Windows 2000, XP, 2003 Server, Vista
Hardware	
License	Freeware
NIAP Validated	No
Common Criteria	
Developer	F-Secure Corporation (Finland)
Availability	*http://www.f-secure.com/en_EMEA/security/security-lab/tools-and-services/blacklight/*

GMER v1.0.15.14972

Abstract

GMER is an application that detects and removes rootkits by scanning for hidden processes, threads, modules, services, files, alternate data streams, registry keys, and for drivers hooking system service descriptor table, interrupt descriptor table, and input/output request packet calls, as well as inline hooks. GMER makes it possible to monitor a variety of system functions, including process creations, driver loads, library loads, file functions, registry entries, and TCP/IP connections.

GMER v1.0.15.14972

Type	Rootkit detection and removal
OS	Windows NT, 2000, XP, Vista
Hardware	
License	Freeware
NIAP Validated	No
Common Criteria	
Developer	Not identified (Internet domain registered by "Domain Discreet" in Portugal)
Availability	*http://www.gmer.net/*

iDefense HookExplorer

Abstract

Detour-style hooks are often indicative of malicious code attempting to co-opt OS processes. HookExplorer scans all loaded DLLs associated with a process, then scans their import tables for hijacked function pointers in the import address table. The first instruction for each function pointer is then disassembled and examined to try to detect standard detour-style hooks that may be present. The tool can optionally also scan every function in the image export table for detour-style hooks, one of the few scans possible for dynamically-loaded DLLs.

iDefense HookExplorer

Type	Rootkit detection (unauthorized hook detector)
OS	Windows with VisualBasic 6 runtime libraries and Microsoft Common Controls Object Linking and Embedding Control eXtension
Hardware	
License	GPL
NIAP Validated	No
Common Criteria	
Developer	iDefense Labs (owned by VeriSign)
Availability	*http://labs.idefense.com/files/labs/releases/previews/HookExplorer/*

MANDIANT® Memoryze

Abstract

MANDIANT Memoryze is free memory forensic software that helps incident responders find malicious activity in live memory. Memoryze can acquire and/or analyze memory images, and on live systems can include the paging file in its analysis. In addition to rootkit and hook detection, Memoryze can also be used for reverse engineering, malware analysis and incident response, and traditional computer forensics.

MANDIANT Memoryze

Type	Rootkit detection
OS	Windows 2000, XP, 2003, Vista (beta support)
Hardware	
License	Freeware
NIAP Validated	No
Common Criteria	
Developer	MANDIANT
Availability	*http://www.mandiant.com/software/d/mmdld.htm*

McAfee Rootkit Detective Beta

Abstract

McAfee Rootkit Detective Beta is a program designed and developed by McAfee Avert Labs to proactively detect and clean rootkits that are running on the system. This program is not dependent on any signatures and can proactively detect most of the existing and upcoming rootkits and allow the user to clean them.

McAfee Rootkit Detective should only be used by knowledgeable individuals at the direction of, and with the support of, a representative from McAfee Avert Labs or McAfee Technical Support. Improper usage of this tool could result in damage to applications or an OS.

McAfee Rootkit Detective Beta

Type	Rootkit detection and removal
OS	Windows XP, 2000, 2003 Server
Hardware	
License	Freeware
NIAP Validated	No
Common Criteria	
Developer	McAfee Avert Labs
Availability	*http://vil.nai.com/vil/stinger/rkstinger.aspx*

Michael Boelen's Rootkit Hunter 1.3.4

Abstract

Rootkit Hunter is scanning tool that detects rootkits, backdoors, and their local exploits by running such tests as—

- MD5 hash comparisons,
- Scans for default files used by rootkits,
- Scans for inappropriate file permissions assigned to binary files,
- Scans for suspect strings in LKM modules,
- Scans for hidden files,
- String scans of plaintext and binary files within directories,
- Additional OS-specific scans and comparisons,
- Detection of port listeners on static ports.

Rootkit Hunter 1.3.4

Type	Rootkit detection
OS	AIX (4.1.5 and 4.3.3), ALT Linux, Aurora Linux, CentOS (3.1 and 4.0), Conectiva Linux 6.0, Debian 3.x, FreeBSD (4.3-4.4, 4.7-4.10, 5.0-5.2.1 and 5.3), Fedora® Core (1-3), Gentoo® (1.4, 2004.0, 2004.1), Macintosh OS X (10.3.4-10.3.8), Mandrake® (8.1-8.2, 9.0-9.2, 10.0-10.1), OpenBSD (3.4-3.5), Red Hat Linux (7.0-7.3, 8, and 9), Red Hat Enterprise Linux (2.1 and 3.0), Slackware (9.0-9.1 and 10.0-10.1), SME 6.0, Sun Solaris, SuSE (7.3, 8.0-8.2, and 9.0-9.2), Ubuntu, Yellow Dog Linux (3.0-3.01), CLFS, DaNix, PCLinuxOS, VectorLinux SOHO (3.2 and 4.0), CPUBuilders Linux, Virtuozzo (VPS). *Notes—NetBSD is not supported. The system must also run Bourne Again Shell.*
Hardware	*Note—Not tested on Intel-based Macintosh*
License	GPL
NIAP Validated	No
Common Criteria	
Developer	Michael Boelen (The Netherlands)
Availability	*http://www.rootkit.nl/projects/rootkit_hunter.html*

Microsoft Sysinternals RootkitRevealer v1.71

Abstract

RootkitRevealer is an advanced rootkit detection utility runs on Windows (NT 4 and higher). Its output lists registry and file system API discrepancies that may indicate the presence of a user-mode or kernel-mode rootkit. RootkitRevealer successfully detects many persistent rootkits including AFX, Vanquish, and HackerDefender (note—RootkitRevealer is not intended to detect rootkits like Fu that do not attempt to hide their files or registry keys).

RootkitRevealer executes its scans from a randomly named copy of itself that runs as a Windows service. Command-line options can be used to execute an automatic scan with results logged to a file. RootkitRevealer requires that the account from which its run has assigned to it the Backup files and directories, Load drivers and Perform volume maintenance tasks (on Windows XP and higher) privileges. The Administrators group is assigned these privileges by default. In order to minimize false positives, run RootkitRevealer on an idle system.

Microsoft also offers an online version of RootkitRevealer, which can be run remotely from their Sysinternals site.

RootkitRevealer v1.71

Type	Rootkit detection
OS	Windows Server 2003, XP
Hardware	
License	Freeware
NIAP Validated	No
Common Criteria	
Developer	Microsoft Sysinternals
Availability	*http://technet.microsoft.com/en-us/sysinternals/bb897445.aspx* *http://live.sysinternals.com/RootkitRevealer.exe*

Panda Security Anti-Rootkit v1.07

Abstract

Panda Anti-Rootkit is a program that uses latest generation technology to detect and remove rootkits. Panda Anti-Rootkit sifts through the files and registry items on a computer, looking for evidence of rootkit activity, and reports its findings in significant detail. It distinguishes rootkits that it recognizes from those it does not, and eliminates both.

Panda Anti-Rootkit v1.07

Type	Rootkit detection and removal Behavior analysis for malware indicators
OS	*Clients*—Windows 2000, XP *Servers*—Panda Tech Support provides scans-as-a-service for systems running Windows 2003 and 2000
Hardware	
License	Freeware
NIAP Validated	No
Common Criteria	
Developer	Panda Security, S.L. (Spain)
Availability	*http://www.pandasecurity.com/homeusers/downloads/docs/product/help/rkc/en/rkc_en.htm* *http://research.pandasecurity.com/archive/New-Panda-Anti_2D00_Rootkit-_2D00_-Version-1.07.aspx* *http://research.pandasecurity.com/blogs/images/AntiRootkit.zip*

The tool does not need to be installed—just downloaded and run. It provides an option for an in-depth scan that requires the computer to be rebooted so the tool can detect rootkit activity during the boot process. The scan itself is fast, and checks processes, drivers, the registry, the file system, and any Alternate Data Streams it can detect. Output can be organized into a readable, detailed Advanced Report that specifies precisely what has been found by the tool and deemed suspicious; the report also indicates the relationships between found items.

Panda Anti-Rootkit distinguishes between unknown rootkits, which it detects solely by their behavior, and known rootkits, which it also matches to known signatures. Rather than removing only known rootkits, to avoid the possibility of damaging the Microsoft Windows installation, Panda Anti-Rootkit deletes all of the suspect "unknown" files *unless* they have legitimate digital signatures from Microsoft that indicate that they are "pure" and unmodified, and thus unlikely to be the source of rootkit behavior; the tool developers consider removing non-Microsoft files to be sufficient. Any file that has been modified, thereby invalidating the signature, is considered a danger that should be removed. Panda also offers the option of sending any unknown files to Panda Labs for further analysis before removing them.

After performing an in-depth scan and removing the detected active rootkits, and their associated hidden files and registry keys, Panda Anti-Rootkit does leave a large number of un-hidden registry keys of rootkits with known signatures.

Pangeia Informatica chkrootkit

Abstract

chkrootkit is a tool that checks for signs of a rootkit on UNIX-based systems (including Linux, BSD, Solaris and Mac OS X). It contains the following components—

- **chkrootkit**—Shell script that checks system binaries for indications of rootkit modification;
- **ifpromisc.c**—Checks whether the interface is in promiscuous mode;
- **chklastlog.c**—Checks for deletions from the UNIX *lastlog* file;
- **chkwtmp.c**—Checks for deletions from the UNIX */var/log/wtmp* (login/logout tracking) file.
- **check_wtmpx.c**—Checks for deletions from the Solaris */var/log/wtmp* (login/logout tracking) file;
- **chkproc.c and chkdirs.c**—Check for signs of LKM Trojans;
- **strings.c**—Replaces strings;
- **chkutmp.c**—Checks for deletions from the UNIX */var/run/utmp* (login/logout tracking) file.

chkrootkit	
Type	Rootkit detection and removal
OS	Linux 2.0.x-2.6.x, FreeBSD 2.2.x-5.x, OpenBSD 2.x-4.x., NetBSD 1.6.x, Solaris 2.5.1-2.6, 8.0-9.0, HP-UX 11, Tru64, BSDI, Mac OS X
Hardware	
License	Freeware
NIAP Validated	no
Common Criteria	
Developer	Pangeia Informatica LTDA (Brazil)
Availability	*http://www.chkrootkit.org*

Sophos® Anti-Rootkit

Abstract

Sophos Anti-Rootkit scans, detects, and removes any rootkit that is hidden on a computer. The tool scans running processes, windows registry, and local hard drives to identify known rootkits and to select, by default, files containing the rootkit component of malware for removal without compromising OS integrity. This enables users to remove unidentified hidden files, but does not allow removal of essential system files hidden by an identified rootkit. After the system has been scanned, the user is prompted through the steps needed to remove every detected rootkit.

The tool can be operated *via* a simple GUI or from the command line, and context sensitive and command-line help are both available.

Note that the same functionality is provided in Sophos's commercial Endpoint Security and Control product.

Anti-Rootkit

Type	Rootkit detection and removal
OS	Windows NT 4.0, 2000, XP, Server 2003
Hardware	128 MB RAM
License	Freeware
NIAP Validated	No
Common Criteria	
Developer	Sophos Plc. (United Kingdom)
Availability	*http://www.sophos.com/products/free-tools/sophos-anti-rootkit.html*

SysProt AntiRootkit v1.0.1.0

Abstract

SysProt AntiRootkit is a free tool to detect and remove rootkits. Some of the key features of the tool are—

- Hidden process detection and removal,
- Hidden driver detection and removal,
- SSDT hooks detection and removal,
- Kernel inline hooks detection and removal,
- Sysenter hook detection,
- TCP/User Datagram Protocol (UDP) port information,
- Hidden/locked files detection and removal.

SysProt AntiRootkit v1.0.1.0

Type	Rootkit detection and removal
OS	Windows 2000, XP, 2003, Vista
Hardware	
License	Freeware
NIAP Validated	No
Common Criteria	
Developer	swatkat (location unknown)
Availability	*http://sites.google.com/site/sysprotantirootkit/*

TrendMicro RootkitBuster v2.52 Beta

Abstract

RootkitBuster is a rootkit scanner that scans hidden files, registry entries, processes, drivers, and master boot record rootkits. In addition, RootkitBuster can also clean hidden files and registry entries.

RootkitBuster v2.52 Beta

Type	Rootkit detection and removal
OS	Windows 2000, Server 2003, XP, Vista *Note—Does not support 64-bit OSs*
Hardware	Pentium; 256 MB RAM (512 MB recommended); 50 MB free disk space
License	Freeware
NIAP Validated	No
Common Criteria	
Developer	TrendMicro
Availability	*http://www.trendmicro.com/download/rbuster.asp*

Usec.at Radix Rootkit Detector

Abstract

Radix Rootkit Detector detects a large number of publicly available rootkits, effectively revealing them to make it possible to delete them. The tool also repairs the damage rootkits cause. Radix Rootkit Detector uses efficient low-level coding and gathers evidence indicating a rootkit allowing the user to decide whether to attempt to remove the suspected rootkit automatically or to manually repair certain of its effects.

Radix Anti Rootkit 1.0.0.8

Type	Rootkit detection and remover
OS	Windows 2000, XP
Hardware	145 KB RAM
License	Freeware
NIAP Validated	No
Common Criteria	
Developer	Usec.at (Austria)
Availability	*http://www.usec.at/rootkit.html*

Xfocus IceSword 1.22

Abstract

IceSword is a kernel level tool that acts as a kernel proxy, so any action the user takes is a kernel-level action. By enumerating services, registry keys, processes, ports, *etc.*, the user can circumvent the majority of hiding methods employed by rootkits such as Klish, SinAR, BlueB8, and others.

IceSword has a Windows Explorer-like interface but displays hidden processes and resources that Windows Explorer would never show. It isn't a "click-here-to-delete-rootkits" product but a sophisticated discovery tool that can protect against sinister rootkits if used before they infect a machine.

IceSword has a dedicated following based on its apparent effectiveness in rootkit detection and removal, despite the fact that *PCWorld* reported that it had received so many complaints about problems using IceSword, that by September 2006, it was compelled to remove the software from the magazine's download site.

IceSword 1.22

Type	Rootkit detection
OS	Windows
Hardware	
License	Freeware
NIAP Validated	No
Common Criteria	
Developer	pjf_ at Xfocus (China)
Availability	*http://mail.ustc.edu.cn/~jfpan/download/IceSword122en.zip* (This is version 1.22.)

zeppoo 0.0.4 beta

Abstract

zeppoo allows you to detect rootkits on i386 and x86_64 architecture under Linux, by using */dev/kmem* and */dev/mem*. Moreover, it can also detect hidden tasks, (hidden) connections, (some) corrupted symbols, system calls, modules, *etc.* Anti-rootkit tools that do not use these methods can be fooled easily.

zeppoo 0.0.4 Beta

Type	Rootkit detection
OS	Linux
Hardware	
License	GPL
NIAP Validated	No
Common Criteria	
Developer	zeppoo (location unknown)
Availability	*http://sourceforge.net/projects/zeppoo*

4.3.1.5 Anti-Bot, Anti-Botnet, and Anti-Zombie Tools

The tools described in this section are understood to address bots and botnets. [15]

Damballa® Failsafe

Abstract

Failsafe network security appliances are placed at key Internet access points and network intersections to identify internal activity typical of bot-driven targeted attacks. Damballa notifies clients in real time whenever a new compromise is detected, providing details for administrators, including steps to contain and remediate the compromise.

Failsafe appliances provide real-time identification and remediation for bot-driven targeted attacks inside enterprise networks, without requiring malware signature databases or network behavior profiles. Failsafe operates both as an in-the-cloud service and as a standalone product with its own management console for automated capture and analysis of zero-day threats. Failsafe also integrates easily into existing IT and security management systems through a Structured Query Language interface.

Damballa appears to intend its Failsafe appliance to be marketed through OEMs, and does not provide a mechanism for direct purchase by end users.

Failsafe	
Type	Bot detection
OS	
Hardware	
License	OEM
NIAP Validated	No
Common Criteria	
Developer	Damballa, Inc.
Availability	*http://www.damballa.com/solutions/index.php*

SRI International BotHunter

Abstract

BotHunter is designed to track the two-way communication flows between internal assets and external entities, developing an evidence trail of data exchanges that match a state-based infection sequence model. BotHunter consists of a correlation engine that is driven by a customized and augmented release of Snort Version 2, which tracks the underlying actions that occur during the malware infection process—inbound scanning, exploit usage, egg downloading, outbound bot coordination dialog, outbound attack propagation, and malware P2P communication. The BotHunter correlator then ties together the dialog trail of inbound intrusion alarms with those outbound communication patterns that are highly indicative of successful local host infection. When a sequence of evidence is found to match BotHunter's infection dialog model, a consolidated report is produced to capture all the relevant events and event sources that played a role during the infection process. We refer to this analytical strategy of matching the dialog flows between internal assets and the broader Internet as dialog-based correlation (patent pending).

BotHunter

Type	Botnet detection
OS	*Tested on Linux*—Fedora, Red Hat Enterprise, Debian, Ubuntu, SuSE; FreeBSD 7.0; Mac OS X 10.4 Tiger, 10.5 Leopard; Windows XP
Hardware	
License	Freeware (with End-User License Agreement)
NIAP Validated	No
Common Criteria	
Developer	SRI International (sponsored by Army Research Office)
Availability	*http://www.bothunter.net/*

TrendMicro RUBotted (Beta)

Abstract

RUBotted monitors the computer for suspicious activities and regularly checks with an online service to identify behavior associated with bots. Upon discovering a potential infection, RUBotted prompts the user to scan and clean the computer with an effective anti-virus program.

RUBotted (Beta)	
Type	Bot detection
OS	Windows 2000, XP, 2003, Vista
Hardware	Pentium 350 MHz, 250 MB free disk space, IPv4 Internet connection
License	Freeware
NIAP Validated	No
Common Criteria	
Developer	TrendMicro
Availability	*http://www.trendsecure.com/portal/en-US/tools/security_tools/rubotted*

4.3.2 Malware Prevention, Termination, and Constraint Tools

The tools described in this section are understood to perform some function that either prevents malware from entering a system, or terminates its execution, or isolates and constrains it to prevent its execution and/or propagation.

Apocgraphy Security Bulldog

Abstract

Security Bulldog removes and quarantines all executable content, scripts, and formatted (*e.g.,* HTML) content from inbound emails and Web mails, as well blocking all email that attempts to download content from the Internet (*e.g.,* hyperlinks in spam mail). The tool alerts the user whenever it has quarantined an attachment and provides a risk assessment for that attachment, based on its file type. The tool includes a built-in database of over 7,000 different file types, each of which includes a description of typical contents and associated level of risk.

By informing the user of the risk level associated with a quarantined attachment, the tool enables the user to make a more informed decision as to whether to open the quarantined attachment or to delete it without opening. This combination of quarantine and content blocking minimizes the risks posed by file types that may contain embedded malicious code as well as those that act as vectors for transmitting or cross-linking to malicious code.

Security Bulldog

Type	Email attachment quarantine
OS	Windows 95, 98, NT, ME, 2000, XP
Hardware	
License	Free/Commercial
NIAP Validated	No
Common Criteria	
Developer	Apocgraphy (Canada)
Availability	*http://www.apocgraphy.com/SecurityBulldog/Default.htm*

Backfaces Process Master

Abstract

Process Master is an advanced utility for detecting and terminating ("killing") hidden processes (such processes are often associated with virus, spyware, or rootkit activity). Advanced viruses, spyware, and rootkits work by changing the results of the API is used by the Windows standard Task Manager. Process Master compares the API results with the results of advanced low-level system techniques to detect the presence of well-known rootkits and the modifications they make. It is intended to be used in conjunction with an anti-virus program, but can also be used without an anti-virus program.

Process Master

Type	Hidden process termination
OS	Windows 2000, XP, 2003
Hardware	1 MB of free disk space
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	Backfaces (Ukraine)
Availability	*http://www.backfaces.com/download/*

DiamondCS ProcessGuard

Abstract

ProcessGuard provides kernel-level protection that prevents the installation of rootkits, malicious drivers, rootkit stealth Trojans, and other malware; determines which programs are executing on the system and logs them for post-infection analysis, controls program execution on a per-program basis, and prevents execution of unknown and unwanted processes; protects processes and services against forced termination, suspension, and crashing; protects processes and executable code against modification; analyzes inter-process behaviors between programs, and determines which programs are attacking others on the system; protects physical memory against modification; prevents firewall leak-test bypass methods; and blocks hooks, code injections, and many other classes of attacks (including Windows file protection attacks and user spoofing attacks) and malware-related behaviors. ProcessGuard can also be used to protect firewalls, anti-virus programs, and other security tools from being attacked by Trojans and viruses.

ProcessGuard is available in two versions—a "lightweight" free version with fewer features and which provides weaker protection, and a commercial version that is fully featured.

ProcessGuard	
Type	Kernel-level execution constraint and malware blocking
OS	Windows 2000, XP, Server 2003
Hardware	
License	Commercial (freeware version available)
NIAP Validated	No
Common Criteria	
Developer	DiamondCS (Australia)
Availability	*http://www.diamondcs.com.au/processguard/index.php*

Leithauser Research Trojan Slayer

Abstract

Trojan Slayer uses machine learning to generate a baseline of the programs that are usually run on the system. Once trained, Trojan Slayer uses one of four enforcement modes to prevent any new processes from running on the system—Report Mode, in which Trojan Slayer informs the user of the program's presence, and prompts the user to allow or deny execution; Block Mode, in which Trojan Slayer informs the user that it has prevented a specific program from executing; Delete Mode, in which Trojan Slayer blocks and deletes the process file from the system; and Replace Mode, in which Trojan Slayer replaces the suspicious program file with a dummy file that has the same name to prevent the Trojan from restoring itself.

Trojan Slayer

Type	Trojan execution constraint
OS	Windows 95 and later
Hardware	
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	Leithauser Research
Availability	*http://leithauserresearch.com/ts.html*

Mocana® NanoDefender®

Abstract

Mocana's patent-pending NanoDefender is an anti-malware intrusion detection system designed to prevent malicious code execution in the context of an existing application or process. NanoDefender can shut down any exploit that is in the process of changing the function flow within running code before that exploit has a chance to do any damage. NanoDefender even provides protection from remote and local stack-based overflows, format string attacks/string exploits, heap overflows, and return-to-libc Integer overflows. NanoDefender is focused on recognizing previously unknown attacks, especially on handheld and wireless devices, and on eliminating "false positives."

Unlike other anti-malware products that rely on signatures, NanoDefender is not intended to run as an external program; it is meant to be integrated into the device or application to be protected during that device's/application's manufacturing or development process. NanoDefender is basically a set of tools and code designed to "wrap" and "harden" executable images against arbitrary code execution.

When a new application is compiled, NanoDefender performs a static analysis of the code to determine the call flow of the executable. In other words, NanoDefender determines which functions call which functions, and which functions make which system calls. Later, at link time, the executable is instrumented to track function calls. Finally, at runtime, NanoDefender runtime code and the (now specially modified) OS together enforce the proper call flow.

NanoDefender is CPU architecture- and platform-independent. Linux platforms are supported out of the box, and ports are expected to be easy to other common platforms (*e.g.,* BSD, Solaris, Windows, Mac OS X, as well as a number of special-purpose, embedded, and real-time operating systems). Processors supported include those from Intel, Hitachi, and several other manufacturers.

Mocana's intended customers are not end users, but device manufacturers, software developers, and OEMs.

NanoDefender

Type	Malware execution prevention
OS	
Hardware	
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	Mocana Corporation
Availability	*http://mocana.com/NanoDefender.html*

Security Stronghold Active Shield

Abstract

Active Shield is a heuristic armor that actively protects the PC from spyware, Trojans, adware, trackware, dialers, keyloggers, rootkits, and other kinds of malicious software. Where other anti-spyware and anti-malware utilities search for malicious programs on the hard drive and registry after the malware has already infected the system, Active Shield works actively like a firewall to intercept malicious programs that try to reach the PC, and block them from installing themselves there.

Active Shield

Type	Malware installation prevention
OS	Windows 2000, XP, 2003, Vista
Hardware	
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	Security Stronghold (Russian Federation)
Availability	*http://www.securitystronghold.com/active_shield.html*

Softmedia Publishing SpyCop® Cloak

Abstract

Cloak protects users' keystrokes and other private information from sniffing or capture by intercepting and suspending any program—be it keylogger, spyware, virus, Trojan, password recorder, chat recorder, email recorder, screen recorder, Web site recorder, or credit card number recorder—that attempts access to the user's chats, emails, credit card data, or other private information. The user is then alerted to the presence of the program, and must expressly grant that program permission to operate before SpyCop Cloak will allow it to continue executing.

SpyCop Cloak	
Type	Malware activity interception and suspension
OS	Windows 2000, XP, Vista
Hardware	
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	Softmedia Publishing, Inc. (Canada)
Availability	*http://www.spycop.com/*

Usec.at Ushields Systemshields

Abstract

Ushields Systemshields protects a computer by preventing the installation of spyware, adware, and BHOs (also known as phishing Trojans) by detecting and blocking registry attacks and installation of backdoors. Systemshields also logs all events to enable easier investigation of malware-related intrusion attempts.

Ushields Systemshields' specific functions include—

- Protection of autorun keys from being changed without the user's permission;
- Protection of legacy autorun Keys from having their settings changed;
- Protection of service keys from being deleted or changed;
- Protection of BHO keys to prevent remotely sourced installation of rogue code in the browser;
- Protection of IE settings against being changed to alter the browser's operation or cause it to download files without the user's permission;
- Protection of the *host* file from being edited to prevent address changes on sites visited by the user, *i.e.,* to prevent cross-site scripting type attacks used for identity theft;
- Prevention of legitimate programs from making registry changes with the user's permission;
- Display of all attempted changes by all programs, along with display of outcome of those changes if the user chooses to allow them to occur;
- Mechanism for creating a "white list" of programs approved to operate;
- Logging of all changes to the registry as they occur.

Ushields Systemshields

Type	Spyware installation prevention
OS	Windows
Hardware	
License	Freeware
NIAP Validated	No
Common Criteria	
Developer	Usec.at (Austria)
Availability	*http://usec.at/downloads2/SystemShield_installer_free.exe* *http://www.usec.at/ushields.html*

4.3.3 Malware Analysis Tools

The tools in this section are used to perform or enable various types of analyses on malware discovered on a system, either in aid of generating malware signatures or incident response/forensic investigation.

DiamondCS Deep System Explorer

Abstract

Deep System Explorer is an advanced security tool for Windows that examines the deepest levels of the system to provide as much information as possible that reveals different signs of infection by malware. The tool enables the user to target specific areas of the system for scanning at both kernel-mode and user-mode levels of the OS. Deep System Explorer can detect live Trojans by using the latest advanced anti-rootkit techniques, including techniques against novel rootkits. The tool is able to detect both existing and future rootkits and hooks without relying on a database of signatures.

Deep System Explorer is available in Standard (less fully-featured, and less expensive) and Professional editions. Standard Edition checks for significantly fewer hidden objects than does Professional Edition.

Deep System Explorer

Type	Malware indicator detection
OS	Windows 2000, XP, Server 2003, Vista
Hardware	
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	DiamondCS (Australia)
Availability	*http://www.diamondcs.com.au/dse/*

iDefense Malcode Analysis Pack

Abstract

The Malcode Analysis Pack contains a number of utilities found by iDefense's own malware researchers to be necessary for doing rapid malcode analysis. These utilities are—

- **ShellExt**—Adds shell extensions to Windows Explorer's right-click context menus that enable decompilation of CHM files on demand, display of file names/sizes/MD5 hashes, display of all American Standard Code for Information Interchange (ASCII) and Unicode strings from a target file, display of file names/sizes/hashes;
- **SocketTool (SckTool)**—Manual TCP Client for probing functionality by sending test/debug text and binary data to a server;
- **MailPot**—A small mail server "capture pot" tool that captures emails sent by Trojans and mass mailers. MailPot can be used to provide an email "honeypot" that spoofs an Outlook mail server;
- **fakeDNS**—A minimal domain name system (DNS) server that spoofs a real network DNS server; useful for forcing bots and other malicious code to use the fake DNS server's services (*e.g.,* email, Web, IRC) to enable observation and analysis;
- **Sniff_Hit**—Specialized *HTTP,* IRC, and DNS sniffer designed to capture and present target communication data, including traffic on unknown and undefined ports;
- **Sclog**—Provides overviews of unknown shellcode functionality by executing that code within a minimal sandbox implemented *via* API hooking;
- **IDCDumpFix**—Helps implement an RE shortcut for working with arbitrarily packed files; provides a way to get a clean readable disassembly of the packed program faster than possible with standard disassemblers;
- **Shellcode2Exe**—Generates executables on the fly by generating hexadecimal or %u-encoded [16] shellcode, then converting it into raw binary, enabling analysis of the resulting new shellcode buffers using Sclog.exe or any debugger;
- **GdiProcs**—Attempts to detect hidden processes by cycling through all elements in the Process Environment Block's *GDISharedHandleTable* and recording their unique process IDs.

Malcode Analysis Pack

Type	Malicious code analysis toolset
OS	Windows with Microsoft VBScript RegExp 1.0, *mscomctl.ocx, mswinsck.ocx, richtx32.ocx, vbDevKit.dll, and spSubclass.dll.* *Note—If running an early version of Windows 2000 or Windows 98, the provided Visual Basic 6 runtime libraries must also be installed. The tools also require IE 5 to run.*
Hardware	
License	GPL
NIAP Validated	No
Common Criteria	
Developer	iDefense Labs (owned by VeriSign)
Availability	*http://labs.idefense.com/software/download/?downloadID=8*

iDefense SysAnalyzer with ProcessAnalyzer

Abstract

SysAnalyzer is an automated malicious code run time analysis application that monitors various aspects of system and process states. SysAnalyzer was designed to enable analysts to quickly collect, compare, and report on the actions a binary took while running on the system.

The main components of SysAnalyzer compare snapshots of the system over a user-specified time interval. The reason a snapshot mechanism was used compared to a live logging implementation is to reduce the amount of data that analysts must wade through when conducting their analysis. By using a snapshot system, we can effectively present viewers with only the persistent changes found on the system since the application was first run.

While this mechanism does help to eliminate a lot of the possible noise caused by other applications, or inconsequential runtime nuances, it also opens up the possibility for missing key data. Because of this, SysAnalyzer also gives the analyst the option to include several forms of live logging into the analysis procedure.

SysAnalyzer can automatically monitor and compare running processes, open ports, loaded drivers, injected libraries, key registry changes, APIs called by a target process, file modifications, and *HTTP,* IRC, and DNS traffic. The SysAnalyzer ProcessAnalyzer tool can create a memory dump of target process, parse it for strings, parse string output for *.exe*, registry, and URL references, and scan the dump for known exploit signatures.

SysAnalyzer is designed to operate in conjunction with Process Analyzer, a stand-alone executable that complements SysAnalyzer's focus on system analysis by focusing on individual processes.

SysAnalyzer supports an API-Logger option to add real-time API logging to the analysis output. The API logger works by injecting a DLL into the target process. Once loaded, the DLL will insert a series of detour-style hooks into specific API calls. When these API are accessed by any code in the process, they will trigger a notification message, which is sent to the main SysAnalyzer interface.

SysAnalyzer with ProcessAnalyzer

Type	Process analysis detection and removal
OS	Windows 2000, XP Also requires *psapi.dll* and the following third-party libraries—*vbDevKit.dll, spSubclass.dll, mswinsck.ocx, mscomctl.ocx, tabctl32.ocx* *Note—Designed for Windows Native API, which is not supported by Microsoft; may operate erratically under later APIs supported by Microsoft.*
Hardware	
License	GPL
NIAP Validated	No
Common Criteria	
Developer	iDefense Labs (owned by VeriSign)
Availability	*http://labs.idefense.com/software/malcode.php*

MANDIANT Red Curtain V1.0

Abstract

Red Curtain is free software for incident responders that assists with the analysis of malware. Red Curtain examines executable files (*e.g.,* .exe, .dll) to determine how suspicious they are based on a set of criteria. It examines multiple aspects of an executable, looking at things such as the entropy (in other words, randomness), indications of packing, compiler and packing signatures, the presence of digital signatures, and other characteristics to generate a threat "score." This score can be used to identify whether a set of files is worthy of further investigation.

Red Curtain v1.0

Type	Malware detection based on binary code analysis
OS	Windows
Hardware	
License	Freeware
NIAP Validated	No
Common Criteria	
Developer	MANDIANT
Availability	*http://www.mandiant.com/software/d/mrcdld.htm*

Norman SandBox Analyzer and SandBox Analyzer Pro

Abstract

The SandBox Analyzer helps security professionals automate their malware analysis process. A complete analysis of the samples is available in a variety of formats, giving the user the freedom to see the information they prefer to see. The most useful outputs are the SandBox summary, available in both text or XML formats, and the API log of system calls. The Analyzer also offers the ability to extract dropped files, memory dumps, and URL content from the SandBox environment. The graphical interface, used for help desk and quick behavioral analysis situations, provides other information windows, including anti-virus engine signature scanning, statistics, lists of dropped files, network connections, and IRC servers found in the batch of suspicious files analyzed. SandBox Analyzer for Linux gives customers an important option to the popular Windows version of the SandBox Analyzer.

SandBox Analyzer Pro provides deep forensic analysis of executable code. Analyzer Pro is a complete reverse engineering environment developed on the stability of the powerful SandBox platform. Analyzer Pro combines the capabilities of many other reverse engineering tools into one product. The user has full control over the SandBox environment and the execution of the sample being analyzed. Registers, memory, disassembled code, virtual hard disk, and network activity can all be closely monitored and manipulated in order to understand the full potential of the suspicious code. Analyzer Pro includes many advanced debugging features like the ability to take snapshots, simulate execution in reverse, search and dump memory contents, log and save network packets, and many others. The user is able to see and work with code both at the application and kernel levels to see rootkit and exploit code behavior. The ability to connect to the live Internet allows analysts to quickly analyze and monitor botnets, network worms, downloaders, and other network-reliant code.

SandBox Analyzer and SandBox Analyzer Pro

Type	Malware analysis
OS	*Analyzer*—Windows 2000/2003 or XP *Analyzer Pro*—Windows 2000/2003 or XP; FreeBSD Linux
Hardware	Pentium PIII
License	Commercial
NIAP Validated	No
Common Criteria	
Developer	Norman ASA (Norway)
Availability	*http://www.norman.com/enterprise/all_products/malware_analyzer/norman_sandbox_analyzer/en* *http://www.norman.com/enterprise/all_products/malware_analyzer/norman_sandbox_analyzer_pro/en*

4.3.4 Other Tools

The tools described in this section do not fall into any of the other categories, but are still anti-malware specific.

iDefense Multipot v0.3

Abstract

Multipot is an emulation-based honeypot designed to capture malicious code that spreads through various exploits across the network. Design specifications for this project mandated that the captures be done in such a way so that the host machine would require only minimal supervision and would not become infected itself. Multipot was designed to emulate exploitable services to safely collect malicious code.

- MultiPot is intended to be used by—
- Internet service providers (ISP), to monitor their networks,
- Corporate security personnel, to be warned of infections,
- Security researchers, to build statistics of Internet health,
- Virus researchers, to collect new samples of malware in the wild,
- Hobbyists and students, to learn more about Internet security.

Multipot v0.3

Type	Honeypot for capturing malware code
OS	Windows
Hardware	
License	GPL
NIAP Validated	No
Common Criteria	
Developer	iDefense Labs (owned by VeriSign)
Availability	*http://labs.idefense.com/software/malcode.php*

Invisible Things System Virginity Verifier (SVV)

Abstract

SVV checks important Windows System components, which are usually altered by various stealth malware, in order to ensure system integrity and to discover possible system compromise. SVV—

- Verifies the integrity of in-memory code sections, which are intended to be read-only (in all modern OSs), and thus should not have their code modified by any program. The tool checks whether code sections of important system DLLs and drivers (kernel modules) are different in memory than they are in the corresponding portable executable files on disk;
- Allows for disinfection (malware removal);
- Strives not to generate false positives.

System Virginity Verifier (SVV) 2.3

Type	System integrity checking
OS	32-bit Windows 2000/XP/2003/Vista
Hardware	
License	Freeware
NIAP Validated	No
Common Criteria	
Developer	Invisible Things Lab (Poland)
Availability	*http://www.invisiblethings.org/code.html*

4.3.5 Malicious Code Detection and Analysis Services

In addition to the tools described above, there are some service providers who specialize in third-party analysis of organizations' computer systems or software for purposes of malicious code detection. These service providers are listed in Table 4-1, with short descriptions of their service offerings.

Table 4-1 Malicious Code Detection and Analysis Services

Service	Description	URL
BitDefender Online Scanner	Uses BitDefender's AntiVirus technology to perform a free virus scan over the Internet of any Windows XP (or later) system that uses Microsoft IE to connect to the BitDefender Online Scanner Web site	*http://www.bitdefender.com/scanner/online/free.html*
MessageLabs® Email Anti-Virus Service v5.1 and Web Security Anti-Spyware & Anti-Virus Protection	MessageLabs hosted Email Anti-Virus Service uses a combination of technologies to deliver protection against known and unknown viruses. To deal with known viruses, perimeter defenses deploy traffic and connection management to identify unwanted email from known sources, slow it down, and reject it. Unknown viruses are intercepted by MessageLabs' Skeptic technology. By following Web links, the service also identifies and blacklists virus-hiding URLs. Email Anti-Virus service is compatible with any SMTP-compliant email messaging platform including Exchange Server, Groupwise, and Lotus Notes-Domino. Web Security Anti-Spyware & Anti-Virus combines Web Anti-Virus service comparable to Email Anti-Virus with protection against spyware, *via* use of multiple scanning engines. MessageLabs is based in the United Kingdom, and owned by Symantec.	*http://www.messagelabs.co.uk/products/email/anti_virus.aspx* *http://www.messagelabs.co.uk/products/web-security-services/web_spyware*
Microsoft Windows Live Safety Scanner	A Web service provided by Microsoft that performs free scans of Windows XP (or later)-based systems to detect and remove viruses and junk files and to optimize PC performance	*http://onecare.live.com/site/en-us/default.htm?s_cid=sah*
New Technology Wave Virus Chaser Application Service Provider	Virus Chaser for Web online service does not require the user to download or install any virus program. Instead, the virus scan and remediation are obtained *via* the Internet. The service uses New Technology Wave's Virus Chaser technology, described in Section 4.3.1.2. New Technology Wave, Inc., is based in Seoul, Korea.	*http://www.viruschaser.com/enwi/2_05.jsp*
Norman Online Protection	A subscription software-as-a-service (SaaS) by which Norman intercepts and scans all emails before forwarding them to the subscriber's mail server.	*http://www.norman.com/smb/all_products/email/norman_online_protection/en*
Norman SandBox Online Analyzer	Norman's SandBox Analyzer is implemented as SaaS to enable users to analyze file behavior by uploading suspicious files for analysis from anywhere in the world. Norman's dedicated servers then provide a comprehensive analysis of the activities associated with those files. After a file has been processed, the service issues a report containing a summary, plus in-depth descriptions of the file's actions in an API log view *via* a Web interface.	*http://www.norman.com/enterprise/all_products/malware_analyzer/norman_sandbox_online_analyzer/en*
TrendMicro HouseCall	An online service that remotely scans certain PCs and other desktop systems to determine whether it has been infected by viruses, spyware, or other malware, and checks for and fixes vulnerabilities that would allow re-infection. The service has fairly stringent requirements for the hardware, OS versions, and software that must be installed on systems that it will scan, which implies that the service likely downloads certain software to the target system.	*http://housecall.trendmicro.com/*

Service	Description	URL
VeraCode Binary Executable Analysis Service	A third-party analysis of binary software executables for security vulnerabilities and presence of malicious logic, including time bombs and rootkits. VeraCode does not analyze operational computer systems, but rather software prior to its deployment.	*http://www.veracode.com*
VirusTotal	A free online service provided by Hispasec Sistemas (Spain), VirusTotal enables customers to upload suspicious files of 20 MB or smaller, which are scanned by multiple anti-malware engines to determine whether those files contain malicious code. VirusTotal is not intended as a substitute for anti-virus software installed on the PC, but can be used to augment the installed anti-virus software by enabling the customer to perform on-demand scanning of small files by a wide range of different anti-virus products.	*http://www.virustotal.com*
Zombie Detection System	A free online service provided by PineApp (an Israeli security appliance vendor) that automatically determines the user's computer's IP address. The user then has the option of submitting that IP in an online form, after which the tool checks the IP against its database of known zombies and reports back whether the system is clean, and also the system's "reputation," based on the amount of email traffic it generates, and also its level of risk, based on the presence of known zombies on the same network.	*http://www.rbltest.com*

References

8 The "MIME" referred to is the Multipurpose Internet Mail Extensions format for email attachments.

9 CA formerly stood for "Computer Associates."

10 GNU is a recursive acronym that amplifies to "GNU's Not Unix." GNU itself is not an acronym. The founders of the GNU software project adopted the gnu as its mascot and name, inspired, at least in part, by the Flanders and Swann comic song "The Gnu."

11 Export outside Russia permitted under licenses from Federal Service for Technology and Export Control of Russian Federation and Federal Security Service of the Russian Federation (Russia's federal security service).

12 DNA = deoxyribonucleic acid. Obviously, malicious software does not consist of actual DNA. The term is used here to imply that the wholly unique content and properties of a particular piece of malware are comparable to DNA in living species, and can be similarly used to identify that malware.

13 Licenses are available for "home and family" and "business" users.

14 A milter is an extension to the popular open source mail transfer agents Sendmail and Postfix. A milter enables the administrator to insert mail filtering for spam, viruses, etc., into the mail processing chain. For more information see—*https://www.milter.org.*

15 At this time, botnet detection is an area of active research in the academic, industry, and government Science and Technology communities. Botnet detection services are offered by a number of network and Internet service providers for their customers. Because these are not tools or services widely available via the Internet, they have not been included in this report. See Meinel, Carolyn. "Botnets II—Emerging Threats, Tactics, and Defenses," published by InformIT, 19 December 2008. Accessed 29 May 2009 at *http://www.informit.com/articles/printerfriendly.aspx?p=1312663.* A number of secure email tools and systems include zombie detection based on detection of quantity of outbound emails based on the recognition that one typical indicator of zombie status is the use of the hijacked system to disseminate large quantities of spam, phishing emails, and malware in email attachments.

16 %u encoding is a technique whereby Unicode bytes are preceded by the character sequence %u. This prefix obfuscates commands to Web servers in a way that prevents those commands from detection by RealSecure, Dragon IDS, and Snort intrusion detection systems.

SECTION 5 ▸ Informational Resources

Table 5-1 lists some good general information resources on malware risks and mitigations, including tools.

Table 5-1 Reference Materials

Resource	URL
AV.Test [17] White papers	*http://www.av-test.org/index.*php?sub=Papers&menue=1&lang=0php?sub=Papers&menue=1&lang=0
Department of the Treasury Inspector General for Tax Administration. *While Controls Have Been Implemented to Address Malware, Continued Attention Is Needed to Address This Growing Threat,* Final Audit Report 2009-20-045, 10 March 2009.	*http://www.treas.gov/tigta/auditreports/2009reports/200920045fr.pdf*
Virus Bulletin	*http://www.virusbtn.com/virusbulletin/archive/index*
The Wildlist Organization International	*http://www.wildlist.org*
VX Heavens	*http://vx.netlux.org*
Cooke, Evan, Farnam Jahanian, and Danny McPherson. "The Zombie Roundup: Understanding, Detecting, and Disrupting Botnets," in *Proceedings of the USENIX Steps to Reducing Unwanted Traffic on the Internet Workshop,* Cambridge, MA, 7 July 2005.	*http://www.usenix.org/event/sruti05/tech/cooke.html* (no password required) —or— *http://www.eecs.umich.edu/~emcooke/pubs/botnets-sruti05.pdf* —or— *http://isis.poly.edu/~kurt/fm/feb_15/sruti05_final.pdf*
SANS InfoSec Reading Room. "Malicious Code"	*http://www.sans.org/reading_room/whitepapers/malicious*
Spyware-Assistance.org	*http://spyware-assistance.org*

Table 5-2 lists guidance documents for addressing malware risks both in operational environments and during the software development and maintenance life cycle.

Table 5-2 Anti-Malware Guidance

Document or Web Page	URL
NSA Malicious Code Tiger Team. Guidance for Addressing Malicious Code Risk, 10 September 2007.	*http://www.nsa.gov/ia/_files/Guidance_For_Addressing_Malicious_Code_Risk.pdf*
National Institute of Standards and Technology (NIST). Guide to Malware Incident Prevention and Handling, Special Publication 800-83, November 2005.	*http://csrc.nist.gov/publications/nistpubs/800-83/SP800-83.pdf*
United States Computer Emergency Response Team (US-CERT). Malware Threats and Mitigation Strategies	*http://www.us-cert.gov/reading_room/malware-threats-mitigation.pdf*
Ohio Office of Information Technology. Malicious Code Security Policy.	*http://www.oit.ohio.gov/IGD/Policy/pdfs_policy/ITP-B.4.pdf*
Pacific Northwest National Laboratory. Guide for Home Computer Security	*http://www.pnl.gov/media/homeguide_public.pdf*

With the increasing prevalence of malware—both on home users' systems and corporate enterprises, a number of organizations and initiatives are dedicated to researching and preventing the spread of malware. Among the most prominent initiatives are the research arms of the anti-malware vendors discussed in Section 4 of this report. While they perform a vital service to the anti-malware industry, their results feed directly into their own anti-malware products. By contrast, the organizations and initiatives listed in Table 5-3 were established by research institutions and other independent organizations in order to perform or distribute the results of their anti-malware research or practices. Please note, Table 5-3 does not attempt to be exhaustive. Instead, it is intended to provide a starting point for readers seeking anti-malware organizations or activities with which to become involved.

Table 5-3 Anti-Malware Organizations and Initiatives

Organization or Initiative	Description	URL
Microsoft Malware Protection Center	This initiative aims to provide a communication mechanism for the Microsoft Malware Response Center to include day-to-day "behind-the-scenes" information about malware research at Microsoft.	*http://blogs.technet.com/mmpc*
Malware Research Group	Provides testing of security applications, malware research, as well as a clearinghouse of information about new forms of malware. Specifically, Malware Research Group tests multiple anti-malware tools suites to measure their comparative effectiveness.	*http://malwareresearchgroup.com*
Software Assurance Forum Malware Attribution Working Group	This working group of the DHS/DoD/NIST co-sponsored Software Assurance Forum aims to examine the malware threat landscape and attempt to discern novel approaches to malware.	*https://buildsecurityin.us-cert.gov/swa/malact.html*
EICAR [18] Working Group 2 on Anti-Virus Practices	EICAR Working Group 2 on Anti-Virus Practices provides a forum for administrators and users of anti-virus products to exchange lessons learned and other information on their experiences.	*http://www.eicar.org*
Anti-Malware Testing Standards Organization (AMTSO)	This effort aims to provide an objective, quality anti-malware testing methodology that may be adopted by organizations to compare anti-malware products. In October 2008, AMTSO released an initial set of documents relating to testing anti-malware.	*http://www.amtso.org*
USENIX Workshops on Offensive Technologies	These workshops focus on malware-related vulnerability research, and malware exploit techniques, design, and implementation. The results from this research will be integrated into future anti-malware software.	*http://www.usenix.org/event/woot09*
StopBadware.org	This initiative is a partnership among academia, technology industry leaders, and volunteers to provide information on malware trends and distribution.	*http://www.stopbadware.org*
Antirootkit.com	This initiative is aimed at providing end users with information about rootkits as well as an understanding of the tools that can be used to detect and remove them.	*http://www.antirootkit.com*
Antispyware Coalition (ASC)	This is a group dedicated to building a consensus about definitions and best practices in the debate surrounding spyware and other potentially unwanted technologies. Composed of anti-spyware software companies, academics, and consumer groups, the ASC seeks to bring together a diverse array of perspective on the problem of controlling spyware and other potentially unwanted technologies.	*http://www.antispywarecoalition.org*
Shadowserver Foundation	This is an all-volunteer watchdog group of security professionals that gathers, tracks, and reports on malware, botnet activity, and electronic fraud. It is the mission of the Shadowserver Foundation to improve the security of the Internet by raising awareness of the presence of compromised servers, malicious attackers, and the spread of malware.	*http://www.shadowserver.org/wiki*
Chain of Trust Initiative	Developed by the ASC, the National Cyber Security Alliance, and StopBadware.org, the Chain of Trust Initiative will link together security vendors, researchers, government agencies, Internet companies, network providers, and advocacy and education groups in a systemic effort to stem the rising tide of malware.	*http://cdt.org/press/20090519press.php*

References

17 AV.Test is a security consulting firm that performs independent tests of anti-virus and other anti-malware tools and products.

18 Originally the European Institute for Computer Antivirus Research, when EICAR expanded its mission beyond anti-virus to address IT security in general, it began designating itself by its acronym only.

SECTION 6 ▸ References and Bibliography

The following documents and online resources were consulted in the development of this paper—

"Malware threat reported by Swiss cybercrime operation," in *IT Reseller,* 13 May 2008. Accessed 25 May 2009 at *http://www.itrportal.com/absolutenm/templates/default.aspx?a=5041&template=print-article.htm*

"Microsoft Says Recovery from Malware Becoming Impossible," in *eWeek,* 4 April 2006.

"Most Chinese Hackers Seek Passwords; More than half of the malware coming out of China aims to steal passwords, and nearly half of those attempts targeted online gaming login information during October," in *InformationWeek,* 28 November 2006.

"Net threats: Why going online remains risky," in *Consumer Reports,* September 2007.

"Sapphire/Slammer Worm Shatters Previous Speed Records for Spreading through the Internet," *ScienceDaily* Press Release, 5 February 2003. Accessed 30 July 2008 at *http://www.sciencedaily.com/releases/2003/02/030205073007.htm*

Abrams, Marshall D. and Harold J. Podell. "Essay 4: Malicious Software." Accessed 25 May 2009 at *http://www.cs.ucr.edu/~brett/cs165_s01/04.pdf*

Addington, Bill. "Slowing Down the Computer Patch Cycle," in *ComputerWorld,* 3 May 2004. Accessed 22 July 2008 at *http://www.computerworld.com/printthis/2004/0,4814,92037,00.html*

Arora, Ashish, Anand Nandkumar, and Rahul Telang. "Does information security attack frequency increase with vulnerability disclosure? An empirical analysis," in *Information Systems Frontier,* Vol. 8 No. 5, 2006, pp. 350-362. Accessed 22 July 2008 at *http://www.heinz.cmu.edu/~rtelang/vuln_freq_ISF.pdf*

Arora, Ashish, Ramayya Krishnan, Rahul Telang, Yubao Yang. "An Empirical Analysis of Software Vendors' Patching Behavior: Impact of Vulnerability Disclosure." January 2006. Accessed 10 June 2008 at *http://www.heinz.cmu.edu/~rtelang/disclosure_jan_06.pdf*

Australian Institute of Criminology. "Malware—viruses, worms, Trojan horses." High Tech Crime Brief No. 10, 2006.

AV.Test. Multiple publications. Accessed 28 June-10 July 2008 at *http://www.av-test.org/index.php?sub=Papers&menue=1&lang=0*

Avci, Ozan Okan. "Hacking Seminar: Malware Protection Techniques." Tutorial at Rheinisch-Westfälische Technische Hochschule Aachen (Germany), 10 June 2004.

Balepin, Ivan, University of California at Davis. Superworms and Cryptovirology: a Deadly Combination.

Barwinski, Mark Andrei. *Taxonomy of Spyware and Empirical Study of Network Drive-by Downloads.* Naval Postgraduate School Master of Science Thesis, September 2005.

Blair, Daniel. "Intro to Malware." Wellesley College Course Handout, 6 October 2006.

Brandt, Andrew. "The 10 Biggest Security Risks You Don't Know About," in *PC World,* 22 June 2006.

Carnegie Mellon University Software Engineering Institute Computer Emergency Response Team Coordination Center (CERT/CC). "Malicious Code Propagation and Antivirus Software Updates." CERT Incident Note IN-2003-01, 2 July 2003. Accessed 25 May 2009 at *http://www.cert.org/incident_notes/IN-2003-01.html*

CA Global Security Advisor Team. "2008 Internet Security Outlook," January 2008. Accessed 31 May 2009 at *http://ca.com/files/SecurityAdvisorNews/ca_security_2008_white_paper_final.pdf*

Cappelli, Dawn M., Randall F. Trzeciak, and Andrew P. Moore. "Insider Threats in the SDLC [Software Development Life Cycle]: Lessons Learned from Actual Incidents of Fraud, Theft of Sensitive Information, and IT Sabotage," presented at Software Engineering Process Group Conference, Austin, TX, 27 March 2007. Accessed 31 May 2009 at *http://www.cert.org/archive/pdf/sepg500.pdf*

Cappelli, Dawn M., Tom Caron, Randall F. Trzeciak, and Andrew P. Moore. "Spotlight on: Programming Techniques Used as an Insider Attack Tool," CERT/CC "Spotlight on" report, December 2008. Accessed 31 May 2009 at *http://www.cert.org/archive/pdf/insiderthreat_programmers_1208.pdf*

Chen, Thomas M. and Jean-Marc Robert. "The Evolution of Viruses and Worms," in *Statistical Methods in Computer Security* (New York, NY: Marcel Dekker, 2004). Accessed 1 August 2008 at *http://engr.smu.edu/~tchen/papers/statmethods2004.pdf*

Chen, Zesheng and Chuanyi Ji. "An Information-Theoretical View of Network-Aware Malware Attacks." Presented at the 26th Annual Institute of Electrical and Electronics Engineers (IEEE) Conference on Computer Communications (IEEE INFOCOM 2007), Anchorage, AK, 6-12 May 2007; updated 6 May 2008. Accessed 31 May 2009 at *http://arxiv.org/pdf/0805.0802*

Chen, Zesheng. *Modeling and Defending Against Internet Worm Attacks.* Georgia Institute of Technology doctoral thesis, May 2007. Accessed 31 May 2009 at *http://Web.eng.fiu.edu/zchen/paper/PhD_Thesis.pdf*

Chien, Eric and Péter Ször. "Blended Attacks, Exploits, Vulnerabilities, and Buffer-Overflow Techniques in Computer Viruses," in *Virus Bulletin Conference,* September 2002. Accessed 31 May 2009 at *http://www.peterszor.com/blended.pdf.* Also at *http://securityresponse.symantec.com/avcenter/reference/blended.attacks.pdf*

Christodorescu , Mihai and Somesh Jha, University of Wisconsin at Madison. "Static Analysis of Executables to Detect Malicious Patterns," in *Proceedings of the 12th USENIX Security Symposium,* Washington, DC, 4-8 August 2003, pp. 169-186. Accessed 18 May 2009 at *http://www.cs.wisc.edu/wisa/papers/security03/cj03.pdf*

Claburn, Thomas. "Malware Doubled In 2007; Next Year Isn't Looking Better; Analysts with F-Secure and Websense predict an explosive growth of malware, bot attacks, QuickTime exploits, and viruses that target the iPhone," in *InformationWeek,* 5 December 2007. Accessed 25 May 2009 at *http://www.informationweek.com/news/mobility/showArticle.jhtml?articleID=204701370*

Claburn, Thomas. "Adware and Mobile Phone Malware on the Rise," in *InformationWeek,* 3 April 2008. Accessed 25 May 2009 at *http://www.informationweek.com/news/mobility/messaging/showArticle.jhtml?articleID=207001403*

Claburn, Thomas. "CES Risk: Free USB Flash Drives; Security researchers warn that flash media given away at trade shows—or even bought off the shelf—may contain malware," in *InformationWeek,* 7 January 2008. Accessed 25 May 2009 at *http://www.informationweek.com/news/security/cybercrime/showArticle.jhtml?articleID=205210426*

Claburn, Thomas. "Fake MP3 Trojan Detected on 27% of PCs; McAfee Avert Labs says more than half a million of the adware programs disguised as media files have been detected in less than a week," in *InformationWeek,* 7 May 2008. Accessed 25 May 2009 at *http://www.informationweek.com/news/security/vulnerabilities/showArticle.jhtml?articleID=207600502*

Claburn, Thomas. "Google Groups Still Littered with Malware-Infected Explicit Videos; Sunbelt Software CEO Alex Eckelberry says the problem is directly tied to hacks of Google's CAPTCHA security," in *InformationWeek,* 9 April 2008. Accessed 25 May 2009 at *http://www.informationweek.com/news/internet/security/showArticle.jhtml?articleID=207100674*

Collins, Michael, Carrie Gates, and Gaurav Kataria. "A Model for Opportunistic Network Exploits: The Case of P2P Worms," in *Proceedings of WEIS 2006.* Accessed 22 July 2008 at *http://www.cert.org/netsa/publications/WEIS2006-mcollins-model-opportunistic-07132006.pdf*

Computer Economics. "2005 Malware Report: The Impact of Malicious Code Attacks." January 2006. Accessed 28 June 2008 at *http://www.computereconomics.com/article.cfm?id=1090*

Computer Economics. "2007 Malware Report: Annual Worldwide Economic Damages from Malware Exceed $13 Billion," June 2007. Accessed 25 May 2009 at *http://www.computereconomics.com/page.cfm?name=Malware%20Report*

Computer Emergency Response Team Coordination Center (CERT®/CC). "Overview of Attack Trends," April 2002. Accessed 31 May 2009 at *http://www.arcert.gov.ar/webs/textos/attack_trends.pdf*

Computer Security Institute and Federal Bureau of Investigation (CSI/FBI). *Ninth Annual Computer Crime and Security Survey 2004.*

Computer Security Institute and Federal Bureau of Investigation. *Tenth Annual CSI/FBI Computer Crime and Security Survey 2005.*

CSI/FBI. *Eleventh Annual CSI/FBI Computer Crime and Security Survey 2006.*

CSI. *CSI Survey 2007: The 12th Annual Computer Crime and Security Survey.*

CSI. *CSI Survey 2008: The 13th Annual Computer Crime and Security Survey.* Accessed 29 May 2009 (requires online registration) at *http://www.gocsi.com/forms/csi_survey.jhtml*

Consumer Reports. "State of the Internet Survey 2005." September 2005.

Consumer Reports. "State of the Net 2006." September 2006.

Danchev, Dancho. "Malware—Future Trends." 31 January 2006. Accessed 29 May 2009 at *http://www.linuxsecurity.com/docs/malware-trends.pdf.* Also at *http://www.windowsecurity.com/whitepapers/Malware-future-trends.html.* Also at *http://packetstormsecurity.org/papers/general/malware-trends.pdf*

Downs, Lawrence G., Jr., Commander, USN. "Digital Data Warfare: Using Malicious Computer Code as a Weapon." Research Report for Air University Air War College, April 1995. Cached version accessed 31 May 2009 at *http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.17.5730*

Dwaikat, Zaid. "Attacks and Countermeasures." *CrossTalk: The Journal of Defense Software Engineering,* October 2005. Accessed 21 December 2007 at *http://www.stsc.hill.af.mil/crosstalk/2005/10/0510Dwaikat.html*

Fernandez, José M. and Pierre-Marc Bureau, École Polytechnique de Montréal. "Optimising Malware," presented at ACM Malware '06, Phoenix, AZ, 10-12 April 2006. Accessed 31 May 2009 at *http://www.professeurs.polymtl.ca/jose.fernandez/optimising-malware-malware06.pdf.* Also at *http://isiom.wssrl.org/index.php?option=com_docman&task=doc_view&gid=17.* Also at *http://www.ccsl.carleton.ca/dss/materials/dss_paper_20060131.pdf*

Filiol, Eric. "Concepts and Future Trends of Computer Virology," presented as a Plenary Talk at the 20th International Conference on Computer, Information, and Systems Science, and Engineering, Nice, France, 28-30 September 2007. Accessed 31 May 2009 at *http:// www.waset.org/lectures/eric_barcelona07.pdf*

Filiol, Eric. "Malware of the Future: When Mathematics Work for the Dark Side," presented at Hack.lu Conference, Grand-Duchy of Luxembourg, 22-24 October 2008. Accessed 31 May 2009 at 2009. hack.lu/archive/2008/Malware%20of%20the%20 Future.pdf

Filiol, Eric. "Metamorphism, formal grammars and undecidable code mutation," in *International Journal of Computer Science,* Volume 2 Issue 1 Winter 2007 pg. 70. Accessed 31 May 2009 at *http://www.waset.org/pwaset/v20/v20-1.pdf*

Fortinet FortiGuard Center. "The State of Malware Today—The Year 2005." Accessed 31 May 2009 at *http://www.fortiguardcenter.com/report/roundup_2005.html*

Gabrielson, Bruce, Karen Mercedes Goertzel, Theodore Winograd, *et al. The Insider Threat to Information Systems: A State-of-the-Art Report* (U// FOUO). Herndon, VA: IATAC, October 2008. Available upon request to qualified readers from *http://iac.dtic.mil/iatac/form.html*

Garretson, Cara. "One in six PCs could be infected with malware; Study of 300,000 PCs showed 15% contained unwanted programs," in *Network World,* 2 November 2007. Accessed 31 May 2009 at *http://www.networkworld.com/news/2007/110207-one-in-six-pcs.html*

Gebhart, Glenn. "Worm Propagation and Countermeasures." GSEC Practical Assignment, Version 1.4b, 24 February 2004. Accessed 31 May 2009 at *http://www.sans.org/reading_room/papers/index.php?id=1410*

Geralds, John. "Hacker insurance set to rocket," on vnunet.com, 14 February 2003. Accessed 31 May 2009 at *http://www.vnunet.com/vnunet/news/2121538/hacker-insurance-set-rocket*

Golovanov, Sergey. "Trend of the year: the evolution of malicious programs targeting players of online games," on Viruslist.com, 26 February 2008. Accessed 31 May 2009 at *http://www.viruslist.com/en/analysis?pubid=204791985*

Goranin, Nikolaj and Antanas Čenys. "Genetic Algorithm-Based Internet Worm Propagation Strategy Modeling," in *Information Technology and Control,* Vol. 37 No. 2, 2008. Accessed 31 May 2009 at *http://itc.ktu.lt/itc372/Goranin372.pdf*

Gostev, Alexander. "Kaspersky Security Bulletin 2007: Malware Evolution in 2007," on Viruslist.com, 26 February 2008. Accessed 31 May 2009 at *http://www.viruslist.com/en/analysis?pubid=204791987*

Government Accountability Office. *Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats.* Report to Congressional Requestors, GAO-07-705, June 2007. Accessed 31 May 2009 at *http://www.gao.gov/new.items/d07705.pdf*

Government Accountability Office. Information Security: Emerging Cyber security Issues Threaten Federal Information Systems. Report to Congressional Requestors, GAO-05-231, May 2005. Accessed 31 May 2009 at *http://www.gao.gov/cgi-bin/getrpt?GAO-05-231*

Grimes, Roger A. "Spyware slips through the patches—A handful of malware programs wreak havoc on a fully patched Windows XP system," in *InfoWorld,* Volume 27 Issue 38, 19 September 2005, pg. 4. Accessed 31 May 2009 at *http://www.infoworld.com/d/security-central/spyware-slips-through-patches-235*

Gruber, Christian. "What Does Exploit Mean? and the Sasser Worm." Seminar presentation, 2 July 2008. Accessed 22 July 2008 at *http://staff.cs.utu.fi/opinnot/kurssit/SemSE/08/What-is-exploit.ppt*

Helmbrecht, Udo, Bundesamt für Sicherheit in der Informationstechnik (BSI). "Economic Dimension in Cyber Security," presented at the 36th Session of the World Federation of Scientists International Seminars on Planetary Emergencies, Erice, Italy, 19-24 August 2006. Accessed 31 May 2009 at *http://www.bsi.bund.de/bsi/reden/2006_08_18_Erice.pdf*

Hines, Matt. "Infrastructure threats: Botnets show DoS who's boss; Malware-infected botnet PCs have overtaken denial-of-service attacks as the top security issue facing ISPs and other Web hosting companies," in *InfoWorld,* 18 September 2007. Accessed 31 May 2009 at *http://www.infoworld.com/d/security-central/infrastructure-threats-botnets-show-dos-whos-boss-359*

IBM/Internet Security Systems. "X-Force 2006 Trend Statistics," January 2007. Accessed 31 May 2009 at *https://www-935.ibm.com/services/us/iss/pdf/x_force_2006_trend_brief.pdf.* Also at *http://www.iss.net/documents/whitepapers/X_Force_Exec_Brief.pdf*

infectionvectors.com. "Disposable Victory," July 2005. Accessed 30 June 2008 at *http://www.infectionvectors.com/library/disposable_iv.pdf*

IronPort Systems. "Malware Trends 2006." Accessed 29 June 2008 at *http://www.ironport.com/pdf/wsr_2006-09.pdf*

IronPort Systems. "Report on Spam, Viruses and Malware, Highlights Trends of 2007 and Predictions for 2008." Accessed 31 May 2009 at *http://www.ironport.com/securitytrends/*

IronPort Threat Operations Center and Web Security Report Staff. "The Business Impact of Malware," in *The Web Security Report,* September 2006. Accessed 31 May 2009 at *http://websecurityreports.messagingnews.com/9_06/index6.html*

James, Lance. "Trojans and Botnets and Malware, Oh My!" Presented at Schmoocon '06.

Jenik, Aviram. "Vulnerability Detection Systems," 5 October 2007.

Joint Security and Privacy Committee of the National Electrical Manufacturers Association, the European Coordination Committee of the Radiological and Electromedical Industry, and the Japan Industries Association of Radiological Systems. "Defending Medical Information Systems Against Malicious Software," December 2003. Accessed at *http://www.medicalimaging.org/documents/medical-defending.pdf*

Jones, Wayne. "Cyber Security Emerging Trends." 6 May 2008. Accessed 28 June 2008 at *http://dns-lessons.lanl.gov/Workshop/JonesOCIOCyberSecurity.pdf*

Kamluk, Vitaly. "The botnet business," on Viruslist.com, 13 May 2008. Accessed 31 May 2009 at *http://www.viruslist.com/analysis?pubid=204792003*

Kannan, Karthik and Rahul Telang. "An Economic Analysis of Market for Software Vulnerabilities." 3 May 2004. Accessed 22 July 2008 at *http://www.dtc.umn.edu/weis2004/kannan-telang.pdf*

Kaspersky Lab's Virus Encyclopedia. Accessed 19 June 2008 at *http://www.viruslist.com/en/viruses/encyclopedia*

Kennedy, Susan. "Common Web Application Vulnerabilities," in *Computerworld,* 25 February 2005. Accessed 10 June 2008 at *http://www.computerworld.com/printthis/2005/0,4814,99981,00.html*

Kasslin, Kimmo, F-Secure Corporation. "Kernel Malware: The attack from within," 22 February 2007. Accessed 31 May 2009 at *http://www.f-secure.com/weblog/archives/kasslin_AVAR2006_KernelMalware_paper.pdf*

Kornakov, Konstantin. "Phishing emerged as a more common exploit than viruses and Trojans," 31 January 2007.

Kornakov, Konstantin. "Cybercrime losses amount to $14.2 billion," on Viruslist.com, 30 January 2006. Accessed 31 May 2009 at *http://www.viruslist.com/en/viruses/news?id=178820306*

Lackorzynski, Tim. "Future Trends of Malware." 19 June 2006. Accessed 28 June 2008 at *http://wwwse.inf.tu-dresden.de/wiki/images/f/f6/PRO-TimLackorzynski.pdf*

Lemos, Robert. "Stormy weather for malware defenses: Virus-writers go after anti-virus vulnerabilities," in *Anti-Virus* (reprinted in *The Register*), 7 March 2007. Accessed 31 May 2009 at *http://www.theregister.co.uk/2007/03/07/storm_malware_defenses/*

Leyden, John. "Drive-by download menace spreading fast," in *The Register,* 23 January 2008. Accessed 30 July 2008 at *http://www.theregister.co.uk/2008/01/23/booby_trapped_Web_botnet_menace/*

Linger, Richard, Stacy Prowell, and Kirk Sayre, Carnegie Mellon University Software Engineering Institute. Computing the Behavior of Malicious Code with Function Extraction Technology, in *Proceedings of the Cyber Security and Information Intelligence Research Workshop,* Oak Ridge and Knoxville, Tennessee, 13-15 April 2009. Accessed 31 May 2009 at *http://www.csiir.ornl.gov/csiirw/09/CSIIRW09-Proceedings/Abstracts/Linger-abstract.pdf—and—http://www.csiir.ornl.gov/csiirw/09/CSIIRW09-Proceedings/Slides/Linger-slides.pdf*

Linger, Richard C. Function Extraction Technology: Automated Calculation of Computer Program Behavior. Accessed 31 May 2009 at *http://www.cert.org/sse/fxmc.html—also* at *http://www.functionextraction.info/webpage/fxmc5.php*

Livingston, Brian. "IceSword Author Speaks Out On 'Rootkits'," in *Datamation,* 14 June 2005. Accessed 25 May 2009 at *http://itmanagement.earthweb.com/columns/executive_tech/article.php/3512621*

Marx, Andreas, AV-Test.org. "Outbreak Response Times: Putting AV to the Test," in *Virus Bulletin,* February 2004. Accessed 31 May 2009 at *http://www.av-test.org/down/papers/2004-02_vb_outbreak.pdf*

Mashevsky, Yury. "Watershed in malicious code evolution." 29 July 2005. Accessed 31 July 2008 at *http://www.viruslist.com/en/analysis?pubid=167798878*

Masud, Mehedy, Latifur Khan, and Bhavani Thuraisingham. "Detecting Malicious Executables," class lecture given in the University of Texas at Dallas Department of Computer Science, 10 September 2007. Accessed at *http://www.utdallas.edu/~bxt043000/cs4398_f7/Lecture7.ppt*

McMillan, Robert. "Microsoft stats show Web attacks taking off," in *PC World,* Volume 26 Issue 7, July 2008, pg. 56. Accessed 31 May 2009 at *http://pcworld.about.com/od/securit1/Microsoft-Data-Show-Web-Attack.htm*

Messmer, Ellen. "Top 5 security-menace predictions for 2008," in *Network World,* 13 November 2007. Accessed 31 May 2009 at *http://www.networkworld.com/news/2007/111307-top-security-menace-2008.html*

Moore, David, Vern Paxson, Stefan Savage, Colleen Shannon, Stuart Staniford, and Nicholas Weaver, The Cooperative Association for Internet Data Analysis (CAIDA). "The Spread of the Sapphire/Slammer Worm." CAIDA white paper, 2003. Accessed 25 May 2009 at *http://www.caida.org/publications/papers/2003/sapphire/sapphire.html*

Multi-State Information Sharing and Analysis Center and United States Computer Emergency Readiness Team (US-CERT). "Current Malware Threats and Mitigation Strategies." Informational Whitepaper, 16 May 2005. Accessed 31 May 2009 at *http://www.us-cert.gov/reading_room/malware-threats-mitigation.pdf*

Murphy, Edmond J. *Counterintelligence Through Malicious Code Analysis.* Naval Postgraduate School Master's Thesis, June 2007. Accessed 26 May 2009 at *http://oai.dtic.mil/oai/oai?&verb=getRecord&metadataPrefix=html&identifier=ADA471421*

Nachenberg, Carey. "Generic Exploit Blocking: Prevention, Not Cure." *ISACA Information Systems Control Journal,* Volume 2, 2005. Accessed 22 July 2005 at *http://www.isaca.org/Template.cfm?Section=Home&CONTENTID=34328&TEMPLATE=/ContentManagement/ContentDisplay.cfm*

NIST National Vulnerability Database. Accessed 26 June 2008 at *http://Web.nvd.nist.gov/view/vuln/search;jsessionid=8ecde241b67a5495fbca99cf826c?execution=e1s1*

NSA Malicious Code Tiger Team. *Guidance for Addressing Malicious Code Risk,* 10 September 2007. Accessed 25 May 2009 at *http:// www.nsa.gov/ia/_files/Guidance_For_Addressing_Malicious_Code_Risk.pdf*

Organisation for Economic Cooperation and Development (OECD). *Malicious Software (Malware): Security Threat to the Internet Economy.* Ministerial Background Report DSTI/ICCP/REG(2007)5/FINAL, 6 March 2008. Accessed 31 May 2009 at *http://www.oecd.org/dataoecd/53/34/40724457.pdf*

Osterman, Michael. "Malware is getting very serious." Network World 28 September 2006. Accessed 31 May 2009 at *http://www.networkworld.com/newsletters/gwm/2006/0925msg2.html*

PCWorld download page for IceSword. Accessed 25 May 2009 at *http://www.pcworld.com/downloads/file/fid,64212-order,1-page,1-c,moreantispywaretools/description.html?&page=11*

Peterson, Pat. "Malware Trends: The Attack of Blended Spyware Crime," in *the Web Security report,* September 2006. Accessed 31 May 2009 at *http://websecurityreports.messagingnews.com/9_06/*

Prince, Brian. "Malware Maelstrom Coming from Russia with Love," in *eWeek,* 2 August 2007. Accessed 25 May 2009 at *http://www.eweek.com/c/a/Security/Malware-Maelstrom-Coming-from-Russia-with-Love/*

Provos, Niels, Dean McNamee, Panayiotis Mavrommatis, Ke Wang and Nagendra Modadugu, Google, Inc. "The Ghost In The Browser: Analysis of Web-based Malware," in *Proceedings of HotBots'07,* Cambridge, MA, 10 April 2007. Accessed 1 August 2008 at *http://www.usenix.org/event/hotbots07/tech/full_papers/provos/provos.pdf*

Provos, Niels, Joe McLain, and Ke Wang. "Search Worms," in *Proceedings of the 4th ACM Workshop on Recurring Malcode (WORM 2006),* Fairfax, VA, 3 November 2006. Accessed 31 May 2009 at *http://doi.acm.org/10.1145/1179542.1179544*

Purser, Jimmy Ray. "Tool Shed—IceSword for Rootkit Detection," in *NetworkWorld,* 12 January 2009. Accessed 25 May 2009 at *http://www.networkworld.com/community/node/37148*

Reifer, Donald J., Pranjali Baxi, Fabio Hirata, Jonathan Schifman, and Ricky Tsao. "Addressing Malicious Code in COTS: A Protection Framework," in *COTS-Based Software Systems* (Lecture Notes in Computer Science, Volume 3412/2005; Berlin/Heidelberg, Germany: Springer Verlag, 2005), pp. 157-167. Accessed 31 May 2009 at *http://www.springerlink.com/content/lp7l4m3q2nmtncp1/fulltext.pdf*

Royal Canadian Mounted Police. "Future Trends in Malicious Code—2006 Report." Information Technology Security Report/Lead Agency Publication R2-002, August 2006. Accessed 29 June 2008 at *http://www.rcmp-grc.gc.ca/tsb/pubs/it_sec/r2-002_e.pdf*

Rubenking, Neil J. "Rooting out Rootkits," in *PC Magazine,* 30 April 2007. Accessed 21 May 2009 at *http://www.pcmag.com/article2/0,2817,2123981,00.asp*

Rutkowska, Joanna. "Introducing Stealth Malware Taxonomy, Version 1.01," November 2006. Accessed 31 May 2009 at *http://invisiblethings.org/papers/malware-taxonomy.pdf*

Rutkowska, Joanna. "System Virginity Verifier—Defining the Roadmap for Malware Detection on Windows System," presented at the Hack in the Box Security Conference, Kuala Lumpur, Malaysia, 28-29 September 2005. Accessed 21 May 2009 at *http://www.invisiblethings.org/papers/hitb05_virginity_verifier.ppt*

Seltzer, Larry. "Spyware Fades to a Dull Roar, but Targeted Attacks Loom." *eWeek,* 20 July 2006. Accessed 31 May 2009 at *http://www.eweek.com/c/a/Security/Spyware-Fades-to-a-Dull-Roar-But-Targeted-*Attacks-Loom/

Shannon, Colleen and David Moore. "The Spread of the Witty Worm." Presentation to the monthly meeting of the San Diego Regional Information Watch, 15 June 2004. Accessed 31 May 2009 at *http://www.caida.org/publications/presentations/2004/witty_worm/witty_worm_lisa.pdf*

Shannon, Colleen. "Current Network Security Threats: DoS, Viruses, Worms, Botnets." Presented at the Trans-European Research and Education Networking Association (TERENA) Networking Conference, 23 May 2007. Accessed 31 May 2009 at *http://tnc2007.terena.org/core/getfile.php?file_id=460*

Sherstobitoff, Ryan. "The Silent Epidemic—The rise of economically motivated malware and targeted attacks." Presented at the 2007 Boise Information Systems Security Association InfoSec Conference, 25 April 2007. Accessed 16 July 2008 at *http://www.boiseissa.org/conference/2007.sherstobitoff.ppt*

stopbadware.org. "May 2008 Badware Web sites Report." 24 June 2008. Accessed 31 May 2009 at: *http://www.stopbadware.org/pdfs/StopBadware_Infected_Sites_Report_062408.pdf*

SwatIt. "Bots, Drones, Zombies, Worms and other things that go bump in the night." Accessed 30 June 2008 at *http://www.swatit.org/bots/*

Symantec. *Internet Security Threat Report: Trends for July 1 2003 – December 31 2003,* Volume V, March 2004. Accessed 31 May 2009 at *http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_symantec_internet_security_threat_report_v.pdf*

Symantec. *Internet Security Threat Report: Trends for January 1 2004 – June 30 2004,* Volume VI, September 2004. Accessed 31 May 2009 at *http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_symantec_internet_security_threat_report_vi.pdf*

Symantec. *Internet Security Threat Report: Trends for July 04 – December 04,* Volume VII, March 2005. Accessed 31 May 2009 at *http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_symantec_internet_security_threat_report_vii.pdf*

Symantec. *Internet Security Threat Report: Trends for January 05 – June 05,* Volume VIII, September 2005. Accessed 31 May 2009 at *http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_symantec_internet_security_threat_report_viii.pdf*

Symantec. *Internet Security Threat Report: Trends for July 05 – December 05,* Volume IX, March 2006. Accessed 31 May 2009 at *http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_symantec_internet_security_threat_report_ix.pdf*

Symantec AntiVirus Research Center. "Understanding Virus Behavior in 32-bit Operating Environments." Accessed 20 July 2008 at *http://www.Symantec.com/avcenter/reference/virus.behavior.under.win.32.pdf*

Talbot, Bruce and Danny Lai (for Australian Department of Communications, Information Technology, and the Arts). "Spyware Discussion Paper," draft May-June 2005. Accessed 31 May 2009 at *http://www.dbcde.gov.au/__data/assets/pdf_file/0008/25973/Spyware_discussion_paper.pdf*

Telang, Rahul and Sunil Wattal: "Impact of Software Vulnerability Announcements on the Market Value of Software Vendors—an Empirical Investigation," in *Proceedings of the Fourth Workshop on the Economics of Information Security,* Cambridge, MA, 2-3 June 2005. Accessed 22 July 2008 at *http://infosecon.net/workshop/pdf/telang_wattal.pdf* and at *http://www.heinz.cmu.edu/~rtelang/event_study.pdf*

Telang, Rahul, Ashish Arora, Ramayya Krishnan and Yubao Yang. "An Empirical Analysis of Software Vendors' Patching Behavior," January 2006. Accessed 31 May 2009 at *http://www.heinz.cmu.edu/~rtelang/disclosure_jan_06.pdf*

Trend Micro. "The Trend of Malware Today: Annual Virus Round-up and 2004 Forecast." December 2003. Accessed 29 June 2008 at *http://us.trendmicro.com/imperia/md/content/us/pdf/threats/securitylibrary/virusroundup.pdf*

US-CERT Multi-State Information Sharing and Analysis Center and United States Computer Emergency Readiness Team. "Current Malware Threats and Mitigation Strategies." 16 May 2005. Accessed 10 June 2008 at *http://www.us-cert.gov/reading_room/malware-threats-mitigation.pdf*

Vaas, Lisa. "Malware Poisoning Results for Innocent Searches," in eWeek, 27 November 2007. Accessed 31 May 2009 at *http://www.eweek.com/c/a/Security/Malware-Poisoning-Results-for-Innocent-Searches/*

Virus Source Code Database. Accessed 10 June 2008 at *http://www.totallygeek.com/vscdb/*

Vogt, Tom. "Simulating and optimising worm propagation algorithms." 29 September 2003 (updated 16 February 2004). Accessed 25 May 2009 at *http://Web.lemuria.org/security/WormPropagation.pdf—and* at *http://www.rootsecure.net/content/downloads/pdf/worm_propogation.pdf*

Wait, Patience. "Malware's Tangled Roots." *Government Computer News,* 21 August 2006. Accessed 31 May 2009 at *http://gcn.com/Articles/2006/08/16/Malwares-tangled-roots.aspx?Page=4*

Watson, Brian P. "Bots, Smaller and Wilier, Deepen Their Threat to Networks," in *Baseline,* 17 September 2007. Accessed 25 May 2009 at *http://www.baselinemag.com/c/a/Intelligence/Bots-Smaller-and-Wilier-Deepen-Their-Threat-to-Networks/*

Wikipedia: "Timeline of notable computer viruses and worms." Accessed 25 May 2009 at *http://en.wikipedia.org/wiki/Timeline_of_notable_computer_viruses_and_worms*

Yachin, Dan. "Zero Hour Virus Protection: Defending Against the Unknown." IDC White Paper, August 2005. Accessed 30 June 2008 at *http://www.vbuster.hu/download/vb_docs/00_zh_esp/idc_def_against_unknown.pdf*

Yegulalp, Serdar. "Review—Six Rootkit Detectors Protect Your System," in *InformationWeek,* 16 January 2007. Accessed 21 May 2009 at *http://www.informationweek.com/news/software/reviews/showArticle.jhtml?articleID=196901062&pgno=1*

Young, Tom. "Malware enters new phase." *Computing,* 7 December 2006, pg. 11. Accessed 31 May 2009 at *http://www.computing.co.uk/computing/analysis/2170413/malware-enters-phase*

Zhang, Yu, Tao Li, Jia Sun, and Renchao Qin, Sichuan University (China). "An FSM-Based Approach for Malicious Code Detection Using the Self-Relocation Gene," in *Proceedings of the Fourth International Conference on Intelligent Computing: Advanced Intelligent Computing Theories and Applications,* Shanghai, China, 15-18 September 2008, pp. 364-371. Accessed 31 May 2009 at *http://dx.doi.org/10.1007/978-3-540-87442-3_46*

SECTION 7 ▶ Definitions of Acronyms and Key Terms

Acronym or Term	Definition
AES	Advanced Encryption Standard
AIX	Advanced Interactive eXecutive
AMD	Advanced Micro Devices
AMTSO	Anti-Malware Testing Standards Organization
API	Application Programming Interface
ASC	AntiSpyware Coalition
ASCII	American Standard Code for Information Interchange
AV	Anti-Virus
BGP	Border Gateway Protocol
BHO	Browser Helper Object
BSD	Berkeley Software Distribution
CA	*formerly an acronym for Computer Associates*
CAIDA	Cooperative Association for Internet Data Analysis
CD	Compact Disc
CERT/CC	Computer Emergency Response Team Coordination Center
CHM	Compiled HTML Help
CISSP	Certified Information System Security Professional
COTS	Commercial Off-The-Shelf
CPU	Central Processing Unit
CSI	Computer Security Institute
DDoS	Distributed Denial of Service
DLL	Dynamic Linked Library
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DNA	Deoxyribonucleic acid
DNS	Domain Name System
DoD	Department of Defense
DoS	Denial of Service
DOS	Disk Operating System
dpi	Dots Per Inch
DTIC	Defense Technical Information Center
DVD	Digital Versatile Disc
EICAR	European Institute for Antivirus Research

Acronym or Term	Definition
ESM	External Security Manager
FBI	Federal Bureau of Investigation
FTP	File Transfer Protocol
FX	Function Extraction
GB	Gigabyte
GHz	Gigahertz
GNU	GNU's Not UNIX
GPL	GNU Public License
GUI	Graphical User Interface
HIPS	Host Intrusion Prevention System
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
IA	Information Assurance
IAC	Information Analysis Center
IATAC	Information Assurance Technology Analysis Center
ID	Identifier
IE	Internet Explorer®
IEEE	Institute of Electrical and Electronics Engineers
IM	Instant Messenger
IMAP	Internet Message Access Protocol
IO	Information Operations
IP	Internet Protocol
IRC	Internet Relay Chat
ISP	Internet Service Provider
IT	Information Technology
LKM	Linux Kernel Module
LSP	Layered Service Provider
MB	Megabyte
MD5	Message Digest 5
MHz	MegaHertz
MIME	Multipurpose Internet Mail Extensions
MMS	Multimedia Messaging Service
MP3	MPEG Audio Layer Three
MPEG	Moving Picture Experts Group
NAS	Network Attached Storage

Acronym or Term	Definition
NATO	North Atlantic Treaty Organization
NAVSEA	Naval Sea Systems Command
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NFS	Network File System
NNTP	Network News Transfer Protocol
NSA	National Security Agency
OECD	Organisation for Economic Cooperation and Development
OEM	Original Equipment Manufacturer
OES	Open Enterprise Server
OLE	Object Linking and Embedding
OS	Operating System
P2P	Peer-to-Peer
PC	Personal Computer
PDA	Personal Digital Assistant
PDF	Portable Document Format
POP	Post Office Protocol
PUP	Potentially Unwanted Program
RAM	Random Access Memory
RFID	Radio Frequency Identification
ROM	Read-Only Memory
RTF	Rich Text Format
SaaS	Software-as-a-Service
SD	SecureDigital
SDK	Software Development Kit
SDLC	Software Development Life Cycle
SSL	Secure Sockets Layer
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SP	Special Publication
SVV	System Virginity Verifier
TCP	Transmission Control Protocol
TERENA	Trans-European Research and Education Networking Association
TPM	Trusted Platform Module
UDP	User Datagram Protocol

Acronym or Term	Definition
URL	Uniform Resource Locator
US-CERT	United States Computer Emergency Response Team
USB	Universal Serial Bus
VxMS	Veritas Mapping Service
XML	eXtensible Markup Language
XSS	Cross-Site Scripting

SECTION 8 ▶ Definitions

Demilitarized Zone
A separate network that hosts an organization's Internet-facing computers and services. By enforcing logical or physical separation, external-facing hosts and the organization's intranet, malware, and other compromises that occur in the demilitarized zone are prevented from spreading to systems on the internal network.

False negative
Refers to the result of an anti-malware detection scan that fails to indicate existing malware.

False positive
Refers to the result of an anti-malware detection scan that indicates the presence of malware that is not actually present.

Heuristic detection
A mechanism designed to detect new or unknown malware using a variety of scanning, including running the malware in a virtual sandbox. One of the primary drawbacks of heuristic detection is that it is more prone to false positives.

In the wild
Currently infecting operational systems and spreading over the Internet. This is by contrast with malicious code developed for observation in an isolated laboratory.

Malware
Software or firmware intended to perform an unauthorized process that will have adverse impact on one or more required properties of the targeted system, including (but not limited to)—confidentiality, privacy, integrity, availability, dependability, usability, and performance. Definitions of the numerous individual categories of malware are provided in Section 2.1, Table 2-1 "Malware Types." Malware is also referred to as malicious code. Sometimes the term virus is inaccurately used to designate all categories of malware that get installed on operational systems (rather than those types of malware that are embedded, *i.e.,* built, into systems during their development, distribution, or initial pre-operational installation).

Polymorphic virus
Traditionally, viruses infect files with identical copies of themselves. Through polymorphism, viruses use some form of mutation or obfuscation to slightly alter their own executable images before infecting other files. The mutated/obfuscated executable is functionally equivalent to the original virus, but produces a different signature, making it difficult for signature-based anti-malware scanners to recognize it. Virus-writers may specify the rate at which a virus mutates, with a longer mutation rate causing the virus to modify itself at the same rate (or faster) as anti-virus suppliers are typically able to add signatures generated from the older version(s) of the virus into their signature databases. In this way, the polymorphic virus always keeps "one step ahead" of the available signatures.

Propagation
The method through which certain categories of malware spread from one system to another. The malware types that most commonly propagate are viruses and worms. There are various propagation vectors, including—

- **Network-based propagation**, in which the malware identifies and migrates to another host on the same a computer network;
- **Execution-based propagation**, in which an infected file is opened or executed and the execution of opener application or the infected executable causes the malware to spread and infect additional files;

- **Disk-based propagation**, in which the malware infects a removable data storage medium (CD, thumb drive, external hard drive, *etc.*) and spreads to the next system on which that medium is connected/inserted;
- **Trojan-based propagation**, in which the malware is hidden within a seemingly legitimate software application and propagates when a person downloads that application then shares it with someone else.

Quarantine

A mechanism used by anti-malware tools to isolate and constrain malware so that it cannot propagate further or reach the operating system or any other software on the system. To achieve isolation and constraint, the anti-malware tool moves the files it suspects of being infected to a specific location in the file system that is inaccessible by any process on the system other than the anti-malware tool itself.

Scanning

The process by which anti-malware tools systematically review and observe the contents of the hard disk, memory, and other areas of a computing system to locate suspected malware.

Signature

A pattern of bytes that is unique to a specific piece of malware's binary code. When signature-based anti-malware tools scan for malware, they search files on the system for the presence of these specific patterns.

Virus

A type of malware that replicates itself by attaching its program instructions to an ordinary host program or document. When the host program is executed, the virus' instructions are also executed. As noted, the term virus is sometimes used less accurately to refer to any type of malware that is "delivered" to an operational system or to any type of self-propagating malware, including worms and some types of Trojans.

Zero-day

Zero-day malware is a previously unknown instance of malware for which specific anti-malware signatures are not yet available. Because signature-based anti-malware tools can only defend against malware for which samples have been obtained and signatures generated, signature-based tools are not effective against zero-day viruses.

SECTION 9 ▶ Additional Information

This section contains additional information that may be of interest to the reader. This information was referred to in the main part of this report.

9.1 Economic Rationale for Malware Attackers

The following have been determined to be the most prevalent economic motivators and enablers for attackers who disseminate or embed malware—

- Email costs virtually nothing to send.
- All the costs of dealing with spam and malware are passed on to the Internet provider and the "unwilling" recipients, who are charged for protective measures, bandwidth, and other connection costs, on top of the costs of repairing the computer or having lost money to scams.
- Criminals minimize their costs to the extreme: they pay no tax, escape the cost of running a genuine business, and pay commission only to others in criminal circles worldwide and at a comparatively low price. The cost to malicious actors continues to decrease as freely available email storage space increases.
- Use of botnets makes it easier and even cheaper to send malware through email.
- Criminals often have access to cheap techniques for harvesting email addresses as well as easy access to malware and outsourced spamming services.
- Anti-detection techniques are constantly evolving to make it cheaper to operate.
- Malicious actors can easily switch ISPs if their activity is detected and their service terminated.
- Malware itself and the compromised computers being used to further launch malware attacks are a low cost, readily available, and easily renewable resource.
- High-speed Internet connections and increased bandwidth allow for the mass creation of compromised hosts that comprise a self sustaining attack system.
- Malicious actors can replace hosts that have been disconnected or disinfected.

9.2 Objectives of Botnet Attackers

The following have been observed to be typical objectives of attackers who establish botnets—

- To locate and infect other information systems with bots and other malware, thereby maintaining and building their supply of new bots to achieve other objectives;
- To conduct distributed denial of service attacks (DDoS);
- To create a service that can be bought, sold or rented out;
- To rotate IP addresses under one or more domain names for the purpose of increasing the longevity of fraudulent Web sites (*e.g.,* phishing and/or malware sites);
- To send spam that distributes more malware;
- To steal sensitive information from each compromised computer that belongs to the botnet;
- To host a malicious phishing site (often in conjunction with other members of the botnet to provide redundancy);
- To run additional attack code.

9.3 Worms: How They Are Constructed, How They Operate

The typical worm has the following components—

- **Reconnaissance module**—Scans the network/Internet for vulnerable hosts. This may be done in real-time, or in advance (see description of worm propagation methods below);
- **Attack module**—May exploit from one to many known vulnerabilities in a potentially vulnerable host;
- **Communication module**—Enables the worm to communicate with other worms or to transfer information to a central command module that ensures the correct functioning of the communication module; the command module locates neighboring worms for communication.

Worms propagate *via* a variety of vectors that can be categorized either as scan-based or topology-based. Scan-based worms (*i.e.,* those using scan-based vectors) probe the network's entire IP address space or the routable address space while simultaneously scanning as many hosts as it can to find a vulnerable host. Usually this is accomplished by the attacker flooding the targeted hosts with requests from randomly spoofed source IP addresses. A vulnerable victim, believing the requests are legitimate, will respond to each spoofed address.

When it finds a vulnerable host, the worm sends out a probe to infect it, then transfers a copy of itself to the infected host. The infected host then runs the worm, which repeats the process to find and infect other victims. For example, Sapphire/Slammer (2003) used a single UDP packet to scan, infect, and replicate itself to victims.

Worm scanning techniques used include—

- **Random scanning**, which selects victim IP Version 4 addresses at random, was used by Code Red and Slammer. *DNS random scanning* uses the DNS infrastructure to locate likely victims by guessing DNS names instead of using IP addresses. Researchers have modeled a DNS random scanning worm that has propagated successfully on an IPv6 network.
- **Selective random scanning**, which reduces the potential scanning space by using additional information such as the Team Cymru Bogon list (see: *http://www.cymru.com/Documents/bogon-list.html)* and/or the IANA's IPv4 address allocation map (see: *http://www.iana.org/assignments/ipv4-address-space),* was used by the Slapper worm.
- **Routable scanning**, in which border gateway protocol (BGP) routing tables form the basis for building scan lists, is a special case of selective random scanning; at least two worms, The Class-A Routing Worm" and the "BGP Routing Worm" have been developed in labs to study the propagation of routable scanning worms.
- **Localized scanning**, which preferentially scans for hosts in the infected host's "local" address space, was used by Code Red II and Nimda worms.
- **Hitlist-scanning**, which requires the compilation of a list of vulnerable machines before the worm is released; these machines will be the first targeted when the worm is launched. A more sophisticated form of hitlist-scanning is *importance scanning.* The term "importance scanning" comes from the concept of *importance sampling* in statistics. Importance-scanning worms optimally exploit the non-uniform distribution of vulnerable hosts by probing the Internet according to the known or statistically likely distribution of vulnerable hosts, which focuses the scans on the most relevant parts of the address space. If a complete list of vulnerable hosts can be assembled, importance-scanning worms can reach the fastest rates of infection, thereby becoming flash worms. A flash worm spreads to every machine on its list of IP addresses of known-vulnerable machines; they spread extremely fast because they target only vulnerable hosts, so their success rate is extremely high. To date, importance-scanning has been modeled in research labs, but not reported "in the wild."

- **Search-based scanning**—Search-based worms are a variant of hitlist-scanning worms. These worms have emerged as random scanning and its variants have become increasingly detectable by anti-malware countermeasures. Search-based worms use Google and other search engines to automate submission of carefully crafted search queries to search engines such as Google, and build a list from the returned results of those queries of likely vulnerable Web servers to which they then copy themselves.
- **Topological-scanning**—In contrast to scan-based worms, topology-based or topological-scanning worms target the topological neighbors of their initial hosts, which they discover by a variety of means. For example, the Morris worm (1988) retrieved the neighbor list from a host's local UNIX */etc/hosts.equiv* and *.rhosts* files plus individual users' *.forward* and *.rhosts* files. An *email virus* is a variant of a topological-scanning worm. When an email user receives a message and opens the attachment containing the virus, the virus infects the user's machine then sends copies of itself to all addresses in the user's email address book.

9.4 Malicious Anti-malware Tools

"...be careful not to download a clean-up tool from a vendor you've never heard of before. Some criminals are promoting bogus...tools and have set up professional-looking Web sites to scam the unwary."
—Graham Cluley, Sophos [19]

A number of alleged freeware anti-malware tools have been discovered to contain malicious logic. The reader is encouraged to perform due diligence on *any* anti-malware tool before installing it, and to be particularly wary of freeware tools produced by developers that go to lengths to obfuscate their identities. Due diligence should begin with an investigation of the tool's reputation among known, reputable security organizations and malware experts. [20]

Google is a particularly useful tool for investigating anti-malware tools. It is very easy to turn up reports of suspected malicious tools by simply Googling the tools' names. The authors of this report entered the names of all tools on one of the many long lists of freeware anti-malware tools published on the Internet. Just a few of the names that turned up in reports from numerous reputable security publications, anti-malware vendors, and security experts: Internet Antivirus Pro (for which an antidote was issued by Microsoft's Malware Protection Center), Antivirus XP 08 (a password-stealing Trojan), Personal Antivirus (whose perpetrators cynically used iFrame Search Engine Optimization poisoning attacks to redirect Google searches for information on the Air France Flight 447 disaster as their mechanism for installing the rogue anti-malware Trojan on Google users' PCs). The reader will discover that organizations like Spyware-assistance.org routinely publish lists of tools that have been discovered to be malicious and/or to install spyware.

Some freeware tools have clear indicators of their possible maliciousness. For example, there is a very impressive-sounding anti-malware tool offered by a software company that has a Web site that bears all the earmarks of a textbook malicious Web site. In another case, one tool appears to be a legitimate anti-spyware tool until one reads the developer's tool description, in which he admits to (read: brags about) also having produced a rogue anti-malware scanner that was expressly designed to generate false positives in order to scare users. Such a tool could at best be useful to a legitimate anti-malware tool vendor that wished to attract customers by running free over-the-Internet scans (as described in Section 4.3.5), which would always find that the scanned computer was infected. The vendor would, of course, only provide remediation to users who paid for full tool licenses (this is the standard business model even of the legitimate tool vendors who offer free over-the-Internet scans).

The value of this false-positive-generating rogue anti-malware scanner is left to the reader. The potential use by hackers or cybercriminals who operate as Graham Cluley describes in his quotation above—encourage users to visit their Web sites for a free scan that will detect and "clean up" malware; in some cases, the free scanner appears in a pop-up window on the user's screen and he/she doesn't need to navigate anywhere. If the user takes advantage of the free scan, the result is a background download of spyware, Trojans, bots, or other malware to the users' systems, or the offer of a free download of an anti-malware tool that in fact contains or constitutes malicious code.

For further information on the problem of rogue antimalware tools, see—

- Nichols, Shaun. Fake antivirus attacks on the rise, on vnunet.com, 17 September 2008. Accessed 31 May 2009 at *http://www.vnu.co.uk/vnunet/news/2226211/fake-antivirus-attacks-balloon*
- Early, Erin. "The Rise and Rise of Rogue Security Software," on Help Net Security, 22 December 2008. Accessed 31 May 2009 at *http://www.net-security.org/article.php?id=1193*
- Rogue security software, on WikiPedia. Accessed 31 May 2009 at *http://en.wikipedia.org/wiki/Rogue_software*
- Krebs, Brian. "Massive Profits Fueling Rogue Antivirus Market," in *The Washington Post,* 16 March 2009. Accessed 31 May 2009 at *http://voices.washingtonpost.com/securityfix/2009/03/obscene_profits_fuel_rogue_ant.html*
- Krebs, Brian. "Rogue Antivirus Distribution Network Dismantled," in *The Washington Post,* 20 March 2009. Accessed 31 May 2009 at *http://voices.washingtonpost.com/securityfix/2009/03/sunlight_disinfects_rogue_anti.html*
- SASIs-Securityspot. Accessed 31 May 2009 at *http://sasis-securityspot.blogspot.com/*

References

19 Graham Cluley, Sophos. "Conficker's impact on Google Search," on his blog, 31 March 2009. Accessed 31 May 2009 at *http://www.sophos.com/blogs/gc/g/2009/03/31/confickers-impact-google-search*

20 Names to look for include Mikko Hypponen, Steve Trilling, Ernst Leiss, Graham Cluley, Paul Ducklin, Péter Ször, Roger Thompson, Matt Fearnow, David Chess, Nick Fitzgerald, and Joe Wells.