Malware

From Wikipedia, the free encyclopedia

Malware, short for **malicious software**, is any software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems.[1] Malware is defined by its malicious intent, acting against the requirements of the computer user, and does not include software that causes unintentional harm due to some deficiency. The term *badware* is sometimes used, and applied to both true (malicious) malware and unintentionally harmful software.[2]

Beast, a Windows-based backdoor Trojan horse.

Malware may be stealthy, intended to steal information or spy on computer users for an extended period without their knowledge, as for example Regin, or it may be designed to cause harm, often as sabotage (e.g., Stuxnet), or to extort payment (CryptoLocker). 'Malware' is an umbrella term used to refer to a variety of forms of hostile or intrusive software,[3] including computer viruses, worms, trojan horses, ransomware, spyware, adware, scareware, and other malicious programs. It can take the form of executable code, scripts, active content, and other software.[4] Malware is often disguised as, or embedded in, non-malicious files. As of 2011 the majority of active malware threats were worms or trojans rather than viruses.[5]

In law, malware is sometimes known as a **computer contaminant**, as in the legal codes of several U.S. states.[6][7]

Spyware or other malware is sometimes found embedded in programs supplied officially by companies, e.g., downloadable from websites, that appear useful or attractive, but may have, for example, additional hidden tracking functionality that gathers marketing statistics. An example of such software, which was described as illegitimate, is the Sony rootkit, a Trojan embedded into CDs sold by Sony, which silently installed and concealed itself on purchasers' computers with the intention of preventing illicit copying; it also reported on users' listening habits, and unintentionally created vulnerabilities that were exploited by unrelated malware.[8]

Software such as anti-virus, anti-malware, and firewalls are used to protect against activity identified as malicious, and to recover from attacks.[9]

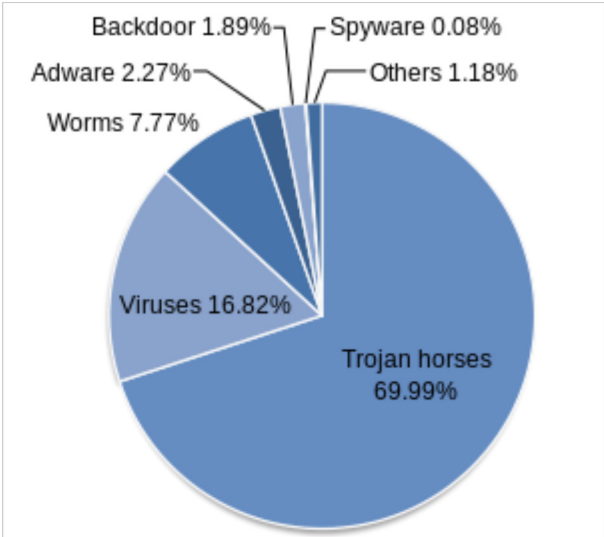
Contents

- 1 Purposes
- 2 Proliferation
- 3 Infectious malware: viruses and worms
- 4 Concealment: Viruses, trojan horses, rootkits, backdoors and evasion
  - 4.1 Viruses
  - 4.2 Trojan horses

- 4.3 Rootkits
- 4.4 Backdoors
- 4.5 Evasion
- 5 Vulnerability to malware
  - 5.1 Security defects in software
  - 5.2 Insecure design or user error
  - 5.3 Over-privileged users and over-privileged code
  - 5.4 Use of the same operating system
- 6 Anti-malware strategies
  - 6.1 Anti-virus and anti-malware software
  - 6.2 Website security scans
  - 6.3 "Air gap" isolation or "Parallel Network"
- 7 Grayware
- 8 History of viruses and worms
- 9 Academic research
- 10 See also
- 11 References
- 12 External links

Purposes

Many early infectious programs, including the first Internet Worm, were written as experiments or pranks. Today, malware is used by both black hat hackers and governments, to steal personal, financial, or business information.[10][11]



Malware by categories on 16 March 2011.

Malware is sometimes used broadly against government or corporate websites to gather guarded information,[12] or to disrupt their operation in general. However, malware is often used against individuals to gain information such as personal identification numbers or details, bank or credit card numbers, and passwords. Left unguarded, personal and networked computers can be at considerable risk against these threats. (These are most frequently defended against by various types of firewall, anti-virus software, and network hardware).[13]

Since the rise of widespread broadband Internet access, malicious software has more frequently been designed for profit. Since 2003, the majority of widespread viruses and worms have been designed to take control of users' computers for illicit purposes.[14] Infected "zombie computers" are used to send email spam, to host contraband data such as child pornography,[15] or to engage in distributed denial-of-service attacks as a form of extortion.[16]

Programs designed to monitor users' web browsing, display unsolicited advertisements,

or redirect affiliate marketing revenues are called spyware. Spyware programs do not spread like viruses; instead they are generally installed by exploiting security holes. They can also be packaged together with user-installed software, such as peer-to-peer applications.[17]

Ransomware affects an infected computer in some way, and demands payment to reverse the damage. For example, programs such as CryptoLocker encrypt files securely, and only decrypt them on payment of a substantial sum of money.

Some malware is used to generate money by click fraud, making it appear that the computer user has clicked an advertising link on a site, generating a payment from the advertiser. It was estimated in 2012 that about 60 to 70% of all active malware used some kind of click fraud, and 22% of all ad-clicks were fraudulent.[18]

Malware is usually used for criminal purposes, but can be used for sabotage, often without direct benefit to the perpetrators. One example of sabotage was Stuxnet, used to destroy very specific industrial equipment. There have been politically motivated attacks that have spread over and shut down large computer networks, including massive deletion of files and corruption of master boot records, described as "computer killing". Such attacks were made on Sony Pictures Entertainment (25 November 2014, using malware known as Shamoon or W32.Disttrack) and Saudi Aramco (August 2012).[19][20]

Proliferation

Preliminary results from Symantec published in 2008 suggested that "the release rate of malicious code and other unwanted programs may be exceeding that of legitimate software applications."[21] According to F-Secure, "As much malware [was] produced in 2007 as in the previous 20 years altogether."[22] Malware's most common pathway from criminals to users is through the Internet: primarily by e-mail and the World Wide Web.[23]

The prevalence of malware as a vehicle for Internet crime, along with the challenge of anti-malware software to keep up with the continuous stream of new malware, has seen the adoption of a new mindset for individuals and businesses using the Internet. With the amount of malware currently being distributed, some percentage of computers are currently assumed to be infected. For businesses, especially those that sell mainly over the Internet, this means they need to find a way to operate despite security concerns. The result is a greater emphasis on back-office protection designed to protect against advanced malware operating on customers' computers.[24] A 2013 Webroot study shows that 64% of companies allow remote access to servers for 25% to 100% of their workforce and that companies with more than 25% of their employees accessing servers remotely have higher rates of malware threats.[25]

On 29 March 2010, Symantec Corporation named Shaoxing, China, as the world's malware capital.[26] A 2011 study from the University of California, Berkeley, and the Madrid Institute for Advanced Studies published an article in *Software Development Technologies*, examining how entrepreneurial hackers are helping enable the spread of malware by offering access to computers for a price. Microsoft reported in May 2011 that one in every 14 downloads from the Internet may now contain malware code. Social media, and Facebook in particular, are seeing a rise in the number of tactics used to spread malware to computers.[27]

A 2014 study found that malware was increasingly aimed at the ever more popular mobile devices such as smartphones.[28]

Infectious malware: viruses and worms

The best-known types of malware, viruses and worms, are known for the manner in which they spread, rather than any specific types of behavior. The term *computer virus* is used for a program that embeds itself in some other executable software (including the operating system itself) on the target system without the user's consent and when that is run causes the virus to spread to other executables. On the other hand, a *worm* is a stand-alone malware program that *actively* transmits itself over a network to infect other computers. These definitions lead to the observation that a virus requires the user to run an infected program or operating system for the virus to spread, whereas a worm spreads itself.[29]

Concealment: Viruses, trojan horses, rootkits, backdoors and evasion

These categories are not mutually exclusive, so malware may use multiple techniques.[30] This section only applies to malware designed to operate undetected, not sabotage and ransomware.

Viruses

A computer program usually hidden within another seemingly innocuous program that produces copies of itself and inserts them into other programs or files, and that usually performs a malicious action (such as destroying data).[31]

Trojan horses

For a malicious program to accomplish its goals, it must be able to run without being detected, shut down, or deleted. When a malicious program is disguised as something normal or desirable, users may unwittingly install it. This is the technique of the *Trojan horse* or *trojan*. In broad terms, a Trojan horse is any program that invites the user to run it, concealing harmful or malicious executable code of any description. The code may take effect immediately and can lead to many undesirable effects, such as encrypting the user's files or downloading and implementing further malicious functionality.

In the case of some spyware, adware, etc. the supplier may require the user to acknowledge or accept its installation, describing its behavior in loose terms that may easily be misunderstood or ignored, with the intention of deceiving the user into installing it without the supplier technically in breach of the law.

Rootkits

Once a malicious program is installed on a system, it is essential that it stays concealed, to avoid detection. Software packages known as *rootkits* allow this concealment, by modifying the host's operating system so that the malware is hidden from the user. Rootkits can prevent a malicious process from being visible in the system's list of

processes, or keep its files from being read.[32]

Some malicious programs contain routines to defend against removal, not merely to hide themselves. An early example of this behavior is recorded in the Jargon File tale of a pair of programs infesting a Xerox CP-V time sharing system:

> Each ghost-job would detect the fact that the other had been killed, and would start a new copy of the recently stopped program within a few milliseconds. The only way to kill both ghosts was to kill them simultaneously (very difficult) or to deliberately crash the system.[33]

Backdoors

A backdoor is a method of bypassing normal authentication procedures, usually over a connection to a network such as the Internet. Once a system has been compromised, one or more backdoors may be installed in order to allow access in the future,[34] invisibly to the user.

The idea has often been suggested that computer manufacturers preinstall backdoors on their systems to provide technical support for customers, but this has never been reliably verified. It was reported in 2014 that US government agencies had been diverting computers purchased by those considered "targets" to secret workshops where software or hardware permitting remote access by the agency was installed, considered to be among the most productive operations to obtain access to networks around the world.[35] Backdoors may be installed by Trojan horses, worms, implants, or other methods.[36][37]

Evasion

Since the beginning of 2015, a sizable portion of malware utilizes a combination of many techniques designed to avoid detection and analysis.[38]

- The most common evasion technique is when the malware evades analysis and detection by fingerprinting the environment when executed.[39]
- The second most common evasion technique is confusing automated tools' detection methods. This allows malware to avoid detection by technologies such as signature-based antivirus software by changing the server used by the malware.[40]
- The third most common evasion technique is timing-based evasion. This is when malware runs at certain times or following certain actions taken by the user, so it executes during certain vulnerable periods, such as during the boot process, while remaining dormant the rest of the time.
- The fourth most common evasion technique is done by obfuscating internal data so that automated tools do not detect the malware.

Vulnerability to malware

- In this context, and throughout, what is called the "system" under attack may be

anything from a single application, through a complete computer and operating system, to a large network.
- Various factors make a system more vulnerable to malware:

Security defects in software

Malware exploits security defects (security bugs or vulnerabilities) in the design of the operating system, in applications (such as browsers, e.g. older versions of Microsoft Internet Explorer supported by Windows XP[41]), or in vulnerable versions of browser plugins such as Adobe Flash Player, Adobe Acrobat or Reader, or Java (http://www.java.com/en/download/testjava.jsp) (see Java SE critical security issues).[42][43] Sometimes even installing new versions of such plugins does not automatically uninstall old versions. Security advisories from plug-in providers announce security-related updates.[44] Common vulnerabilities are assigned CVE IDs and listed in the US National Vulnerability Database. Secunia PSI[45] is an example of software, free for personal use, that will check a PC for vulnerable out-of-date software, and attempt to update it.

Malware authors target bugs, or loopholes, to exploit. A common method is exploitation of a buffer overrun vulnerability, where software designed to store data in a specified region of memory does not prevent more data than the buffer can accommodate being supplied. Malware may provide data that overflows the buffer, with malicious executable code or data after the end; when this payload is accessed it does what the attacker, not the legitimate software, determines.

Insecure design or user error

Early PCs had to be booted from floppy disks; when built-in hard drives became common the operating system was normally started from them, but it was possible to boot from another boot device if available, such as a floppy disk, CD-ROM, DVD-ROM, or USB flash drive. It was common to configure the computer to boot from one of these devices when available. Normally none would be available; the user would intentionally insert, say, a CD into the optical drive to boot the computer in some special way, for example to install an operating system. Even without booting, computers can be configured to execute software on some media as soon as they become available, e.g. to autorun a CD or USB device when inserted.

Malicious software distributors would trick the user into booting or running from an infected device or medium; for example, a virus could make an infected computer add autorunnable code to any USB stick plugged into it; anyone who then attached the stick to another computer set to autorun from USB would in turn become infected, and also pass on the infection in the same way.[46] More generally, any device that plugs into a USB port-—"including gadgets like lights, fans, speakers, toys, even a digital microscope"—can be used to spread malware. Devices can be infected during manufacturing or supply if quality control is inadequate.[46]

This form of infection can largely be avoided by setting up computers by default to boot from the internal hard drive, if available, and not to autorun from devices.[46] Intentional booting from another device is always possible by pressing certain keys during boot.

Older email software would automatically open HTML email containing potentially

malicious JavaScript code; users may also execute disguised malicious email attachments and infected executable files supplied in other ways.

Over-privileged users and over-privileged code

In computing, privilege refers to how much a user or program is allowed to modify a system. In poorly designed computer systems, both users and programs can be assigned more privileges than they should be, and malware can take advantage of this. The two ways that malware does this is through overprivileged users and overprivileged code.

Some systems allow all users to modify their internal structures, and such users today would be considered over-privileged users. This was the standard operating procedure for early microcomputer and home computer systems, where there was no distinction between an *administrator* or *root*, and a regular user of the system. In some systems, non-administrator users are over-privileged by design, in the sense that they are allowed to modify internal structures of the system. In some environments, users are over-privileged because they have been inappropriately granted administrator or equivalent status.

Some systems allow code executed by a user to access all rights of that user, which is known as over-privileged code. This was also standard operating procedure for early microcomputer and home computer systems. Malware, running as over-privileged code, can use this privilege to subvert the system. Almost all currently popular operating systems, and also many scripting applications allow code too many privileges, usually in the sense that when a user executes code, the system allows that code all rights of that user. This makes users vulnerable to malware in the form of e-mail attachments, which may or may not be disguised.

Use of the same operating system

- Homogeneity: e.g. when all computers in a network run the same operating system; upon exploiting one, one worm can exploit them all:[47] For example, Microsoft Windows or Mac OS X have such a large share of the market that concentrating on either could enable an exploited vulnerability to subvert a large number of systems. Instead, introducing diversity, purely for the sake of robustness, could increase short-term costs for training and maintenance. However, having a few diverse nodes could deter total shutdown of the network as long as all the nodes are not part of the same directory service for authentication, and allow those nodes to help with recovery of the infected nodes. Such separate, functional redundancy could avoid the cost of a total shutdown, at the cost of increased complexity and reduced usability in terms of single sign-on authentication.

Anti-malware strategies

As malware attacks become more frequent, attention has begun to shift from viruses and spyware protection, to malware protection, and programs that have been specifically developed to combat malware. (Other preventive and recovery measures, such as backup and recovery methods, are mentioned in the computer virus article).

Anti-virus and anti-malware software

A specific component of anti-virus and anti-malware software, commonly referred to as an on-access or real-time scanner, hooks deep into the operating system's core or kernel and functions in a manner similar to how certain malware itself would attempt to operate, though with the user's informed permission for protecting the system. Any time the operating system accesses a file, the on-access scanner checks if the file is a 'legitimate' file or not. If the file is identified as malware by the scanner, the access operation will be stopped, the file will be dealt with by the scanner in a pre-defined way (how the anti-virus program was configured during/post installation), and the user will be notified. This may have a considerable performance impact on the operating system, though the degree of impact is dependent on how well the scanner was programmed. The goal is to stop any operations the malware may attempt on the system before they occur, including activities which might exploit bugs or trigger unexpected operating system behavior.

Anti-malware programs can combat malware in two ways:

1. They can provide real time protection against the installation of malware software on a computer. This type of malware protection works the same way as that of antivirus protection in that the anti-malware software scans all incoming network data for malware and blocks any threats it comes across.
2. Anti-malware software programs can be used solely for detection and removal of malware software that has already been installed onto a computer. This type of anti-malware software scans the contents of the Windows registry, operating system files, and installed programs on a computer and will provide a list of any threats found, allowing the user to choose which files to delete or keep, or to compare this list to a list of known malware components, removing files that match.

Real-time protection from malware works identically to real-time antivirus protection: the software scans disk files at download time, and blocks the activity of components known to represent malware. In some cases, it may also intercept attempts to install start-up items or to modify browser settings. Because many malware components are installed as a result of browser exploits or user error, using security software (some of which are anti-malware, though many are not) to "sandbox" browsers (essentially isolate the browser from the computer and hence any malware induced change) can also be effective in helping to restrict any damage done.

Examples of Microsoft Windows antivirus and anti-malware software include the optional Microsoft Security Essentials[48] (for Windows XP, Vista, and Windows 7) for real-time protection, the Windows Malicious Software Removal Tool[49] (now included with Windows (Security) Updates on "Patch Tuesday", the second Tuesday of each month), and Windows Defender (an optional download in the case of Windows XP, incorporating MSE functionality in the case of Windows 8 and later).[50] Additionally, several capable antivirus software programs are available for free download from the Internet (usually restricted to non-commercial use).[51] Tests found some free programs to be competitive with commercial ones.[51] Microsoft's System File Checker can be used to check for and repair corrupted system files.

Some viruses disable System Restore and other important Windows tools such as Task Manager and Command Prompt. Many such viruses can be removed by rebooting the computer, entering Windows safe mode with networking,[52] and then using system tools

or Microsoft Safety Scanner.[53]

Hardware implants can be of any type, so there can be no general way to detect them.

Website security scans

As malware also harms the compromised websites (by breaking reputation, blacklisting in search engines, etc.), some websites offer vulnerability scanning.[54][55][56][57] Such scans check the website, detect malware, may note outdated software, and may report known security issues.

"Air gap" isolation or "Parallel Network"

As a last resort, computers can be protected from malware, and infected computers can be prevented from disseminating trusted information, by imposing an "air gap" (i.e. completely disconnecting them from all other networks). However, information can be transmitted in unrecognized ways; in December 2013 researchers in Germany showed one way that an apparent air gap can be defeated.[58]

Later in 2015, "BitWhisper", a Covert Signaling Channel between Air-Gapped Computers using Thermal Manipulations was introduced. "BitWhisper" supports bidirectional communication and requires no additional dedicated peripheral hardware.[59][60]

Grayware

Grayware is a term applied to unwanted applications or files that are not classified as malware, but can worsen the performance of computers and may cause security risks.[61]

It describes applications that behave in an annoying or undesirable manner, and yet are less serious or troublesome than malware. Grayware encompasses spyware, adware, fraudulent dialers, joke programs, remote access tools and other unwanted programs that harm the performance of computers or cause inconvenience. The term came into use around 2004.[62]

Another term, PUP, which stands for *Potentially Unwanted Program* (or PUA *Potentially Unwanted Application*),[63] refers to applications that would be considered unwanted despite often having been downloaded by the user, possibly after failing to read a download agreement. PUPs include spyware, adware, fraudulent dialers. Many security products classify unauthorised key generators as grayware, although they frequently carry true malware in addition to their ostensible purpose.

Software maker Malwarebytes lists several criteria for classifying a program as a PUP.[64]

History of viruses and worms

Before Internet access became widespread, viruses spread on personal computers by infecting the executable boot sectors of floppy disks. By inserting a copy of itself into the machine code instructions in these executables, a virus causes itself to be run whenever a program is run or the disk is booted. Early computer viruses were written for the Apple

II and Macintosh, but they became more widespread with the dominance of the IBM PC and MS-DOS system. Executable-infecting viruses are dependent on users exchanging software or boot-able floppies and thumb drives so they spread rapidly in computer hobbyist circles.

The first worms, network-borne infectious programs, originated not on personal computers, but on multitasking Unix systems. The first well-known worm was the Internet Worm of 1988, which infected SunOS and VAX BSD systems. Unlike a virus, this worm did not insert itself into other programs. Instead, it exploited security holes (vulnerabilities) in network server programs and started itself running as a separate process.[65] This same behavior is used by today's worms as well.

With the rise of the Microsoft Windows platform in the 1990s, and the flexible macros of its applications, it became possible to write infectious code in the macro language of Microsoft Word and similar programs. These *macro viruses* infect documents and templates rather than applications (executables), but rely on the fact that macros in a Word document are a form of executable code.

Today, worms are most commonly written for the Windows OS, although a few like Mare-D[66] and the L10n worm[67] are also written for Linux and Unix systems. Worms today work in the same basic way as 1988's Internet Worm: they scan the network and use vulnerable computers to replicate. Because they need no human intervention, worms can spread with incredible speed. The SQL Slammer infected thousands of computers in a few minutes in 2003.[68]

Academic research

The notion of a self-reproducing computer program can be traced back to initial theories about the operation of complex automata.[69] John von Neumann showed that in theory a program could reproduce itself. This constituted a plausibility result in computability theory. Fred Cohen experimented with computer viruses and confirmed Neumann's postulate and investigated other properties of malware such as detectability and self-obfuscation using rudimentary encryption. His doctoral dissertation was on the subject of computer viruses.[70]

See also

- Browser hijacking
- Category:Web security exploits
- Comparison of antivirus software
- Computer insecurity
- Cyber spying
- Identity theft
- Industrial espionage
- Malvertising
- Riskware
- Security in Web applications
- Social engineering (security)
- Targeted threat
- Web server overload causes
- Phishing
- Typosquatting

References

1. "Malware definition" (http://www.studioprovider.com/terms/malware.html). techterms.com. Retrieved 26 August 2013.

2. "What is badware?" (https://www.stopbadware.org/badware). *StopBadware*. Retrieved 18 February 2015.
3. "Defining Malware: FAQ" (http://technet.microsoft.com/en-us/library/dd632948.aspx). technet.microsoft.com. Retrieved 10 September 2009.
4. "An Undirected Attack Against Critical Infrastructure" (https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/CaseStudy-002.pdf) (PDF). United States Computer Emergency Readiness Team(Us-cert.gov). Retrieved 28 September 2014.
5. "Evolution of Malware-Malware Trends" (http://www.microsoft.com/security/sir/story/default.aspx#!10year_malware). *Microsoft Security Intelligence Report-Featured Articles*. Microsoft.com. Retrieved 28 April 2013.
6. "Virus/Contaminant/Destructive Transmission Statutes by State" (http://www.ncsl.org/issues-research/telecom/state-virus-and-computer-contaminant-laws.aspx). National Conference of State Legislatures. 2012-02-14. Retrieved 26 August 2013.
7. "§ 18.2-152.4:1 Penalty for Computer Contamination" (http://jcots.state.va.us/2005%20Content/pdf/Computer%20Contamination%20Bill.pdf) (PDF). Joint Commission on Technology and Science. Retrieved 17 September 2010.
8. Russinovich, Mark (2005-10-31). "Sony, Rootkits and Digital Rights Management Gone Too Far" (http://blogs.technet.com/markrussinovich/archive/2005/10/31/sony-rootkits-and-digital-rights-management-gone-too-far.aspx). *Mark's Blog*. Microsoft MSDN. Retrieved 2009-07-29.
9. "Protect Your Computer from Malware" (http://www.onguardonline.gov/media/video-0056-protect-your-computer-malware). OnGuardOnline.gov. Retrieved 26 August 2013.
10. "Malware" (http://www.consumer.ftc.gov/articles/0011-malware). FEDERAL TRADE COMMISSION- CONSUMER INFORMATION. Retrieved 27 March 2014.
11. Hernandez, Pedro. "Microsoft Vows to Combat Government Cyber-Spying" (http://www.eweek.com/security/microsoft-vows-to-combat-government-cyber-spying.html). eWeek. Retrieved 15 December 2013.
12. Kovacs, Eduard. "MiniDuke Malware Used Against European Government Organizations" (http://news.softpedia.com/news/MiniDuke-Malware-Used-Against-European-Government-Organizations-333006.shtml). Softpedia. Retrieved 27 February 2013.
13. "South Korea network attack 'a computer virus' " (http://www.bbc.co.uk/news/world-asia-21855051). *BBC*. Retrieved 20 March 2013.
14. "Malware Revolution: A Change in Target" (http://technet.microsoft.com/en-us/library/cc512596.aspx). March 2007.
15. "Child Porn: Malware's Ultimate Evil" (http://www.itworld.com/security/84077/child-porn-malwares-ultimate-evil). November 2009.
16. PC World – Zombie PCs: Silent, Growing Threat (http://www.pcworld.com/article/id,116841-page,1/article.html).
17. "Peer To Peer Information" (http://oit.ncsu.edu/resnet/p2p). NORTH CAROLINA STATE UNIVERSITY. Retrieved 25 March 2011.
18. "Another way Microsoft is disrupting the malware ecosystem" (http://blogs.technet.com/b/mmpc/archive/2012/11/29/another-way-microsoft-is-disrupting-the-malware-ecosystem.aspx). Retrieved 18 February 2015.
19. "Shamoon is latest malware to target energy sector" (http://www.computerweekly.com/news/2240161674/Shamoon-is-latest-malware-to-target-energy-sector). Retrieved 18 February 2015.
20. "Computer-killing malware used in Sony attack a wake-up call" (http://www.computerweekly.com/news/2240235919/Computer-killing-malware-used-in-Sony-attack-a-wake-up-call-to-business?asrc=EM_MDN_37122786&utm_medium=EM&utm_source=MDN&utm_campaign=20141203_Computer-killing%20malware%20used%20in%20Sony%20attack%20a%20wake-up%20call_). Retrieved 18 February 2015.
21. "Symantec Internet Security Threat Report: Trends for July–December 2007 (Executive Summary)" (http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_exec_summary_internet_security_threat_report_xiii_04-2008.en-us.pdf) (PDF) **XIII**. Symantec Corp. April 2008. p. 29. Retrieved 11 May 2008.

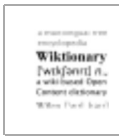
22. "F-Secure Reports Amount of Malware Grew by 100% during 2007" (http://www.f-secure.com/f-secure/pressroom/news/fs_news_20071204_1_eng.html) (Press release). F-Secure Corporation. 4 December 2007. Retrieved 11 December 2007.
23. "F-Secure Quarterly Security Wrap-up for the first quarter of 2008" (http://www.f-secure.com/f-secure/pressroom/news/fsnews_20080331_1_eng.html). F-Secure. 31 March 2008. Retrieved 25 April 2008.
24. "Continuing Business with Malware Infected Customers" (http://www.technicalinfo.net/papers/MalwareInfectedCustomers.html). Gunter Ollmann. October 2008.
25. "New Research Shows Remote Users Expose Companies to Cybercrime" (http://www.webroot.com/En_US/pr/web-security/ent/new-research-shows-remote-users-expose-companies-to-cybercrime-042313.html). Webroot. April 2013.
26. "Symantec names Shaoxing, China as world's malware capital" (http://www.engadget.com/2010/03/29/symantec-names-shaoxing-china-worlds-malware-capital). Engadget. Retrieved 15 April 2010.
27. Rooney, Ben (2011-05-23). "Malware Is Posing Increasing Danger" (http://online.wsj.com/article/SB10001424052748704904604576332812592346714.html). Wall Street Journal.
28. Suarez-Tangil, Guillermo; Juan E. Tapiador, Pedro Peris-Lopez, Arturo Ribagorda (2014). "Evolution, Detection and Analysis of Malware in Smart Devices" (http://www.seg.inf.uc3m.es/~guillermo-suarez-tangil/papers/2013cst-ieee.pdf) (PDF). *IEEE Communications Surveys & Tutorials*.
29. "computer virus – Encyclopedia Britannica" (http://www.britannica.com/EBchecked/topic/130688/computer-virus). Britannica.com. Retrieved 28 April 2013.
30. All about Malware and Information Privacy (http://techacute.com/malware-information-privacy/)
31. "What are viruses, worms, and Trojan horses?" (https://kb.iu.edu/d/aehm). *Indiana University*. The Trustees of Indiana University. Retrieved 23 February 2015.
32. McDowell, Mindi. "Understanding Hidden Threats: Rootkits and Botnets" (http://www.us-cert.gov/ncas/tips/ST06-001). US-CERT. Retrieved 6 February 2013.
33. "Catb.org" (http://catb.org/jargon/html/meaning-of-hack.html). Catb.org. Retrieved 15 April 2010.
34. Vincentas (11 July 2013). "Malware in SpyWareLoop.com" (http://www.spywareloop.com/news/malware). Spyware Loop. Retrieved 28 July 2013.
35. Staff, SPIEGEL. "Inside TAO: Documents Reveal Top NSA Hacking Unit" (http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969-3.html). SPIEGEL. Retrieved 23 January 2014.
36. Edwards, John. "Top Zombie, Trojan Horse and Bot Threats" (http://www.itsecurity.com/features/top-zombie-trojan-bots-092507). IT Security. Retrieved 25 September 2007.
37. Appelbaum, Jacob. "Shopping for Spy Gear:Catalog Advertises NSA Toolbox" (http://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html). SPIEGEL. Retrieved 29 December 2013.
38. Evasive malware (http://www.net-security.org/malware_news.php?id=3022)
39. Kirat, Dhilung; Vigna, Giovanni; Kruegel, Christopher (2014). *Barecloud: bare-metal analysis-based evasive malware detection*. ACM. pp. 287–301. ISBN 978-1-931971-15-7.
40. The Four Most Common Evasive Techniques Used by Malware (http://www.tripwire.com/state-of-security/security-data-protection/the-four-most-common-evasive-techniques-used-by-malware/). April 27, 2015.
41. "Global Web Browser... Security Trends" (http://www.kaspersky.com/images/Kaspersky_Report_Browser_Usage_ENG_Final.pdf) (PDF). Kaspersky lab. November 2012.
42. Rashid, Fahmida Y. (27 November 2012). "Updated Browsers Still Vulnerable to Attack if Plugins Are Outdated" (http://securitywatch.pcmag.com/none/305385-updated-browsers-still-vulnerable-to-attack-if-plugins-are-outdated). pcmag.com.
43. Danchev, Dancho (18 August 2011). "Kaspersky: 12 different vulnerabilities detected on every PC" (http://www.zdnet.com/blog/security/kaspersky-12-different-vulnerabilities-detected-on-every-pc/9283). pcmag.com.
44. "Adobe Security bulletins and advisories" (http://www.adobe.com/support/security/). Adobe.com. Retrieved 19 January 2013.

45. Rubenking, Neil J. "Secunia Personal Software Inspector 3.0 Review & Rating" (http://www.pcmag.com/article2/0,2817,2406767,00.asp). PCMag.com. Retrieved 19 January 2013.
46. "USB devices spreading viruses" (http://www.cnet.com/uk/news/usb-devices-spreading-viruses/). *CNET*. CBS Interactive. Retrieved 18 February 2015.
47. "LNCS 3786 – Key Factors Influencing Worm Infection", U. Kanlayasiri, 2006, web (PDF): SL40-PDF (http://www.springerlink.com/index/3x8582h43ww06440.pdf).
48. "Microsoft Security Essentials" (http://windows.microsoft.com/en-US/windows/products/security-essentials). Microsoft. Retrieved 21 June 2012.
49. "Malicious Software Removal Tool" (http://www.microsoft.com/security/pc-security/malware-removal.aspx). Microsoft. Retrieved 21 June 2012.
50. "Windows Defender" (http://www.microsoft.com/en-us/download/details.aspx?id=17). Microsoft. Retrieved 21 June 2012.
51. Rubenking, Neil J. (8 January 2014). "The Best Free Antivirus for 2014" (http://www.pcmag.com/article2/0,2817,2388652,00.asp). pcmag.com.
52. "How do I remove a computer virus?" (http://windows.microsoft.com/en-US/windows7/how-do-I-remove-a-computer-virus). Microsoft. Retrieved 26 August 2013.
53. "Microsoft Safety Scanner" (http://www.microsoft.com/security/scanner/en-us/default.aspx). Microsoft. Retrieved 26 August 2013.
54. "An example of a website vulnerability scanner" (http://www.unmaskparasites.com/). Unmaskparasites.com. Retrieved 19 January 2013.
55. "Redleg's File Viewer. Used to check a webpage for malicious redirects or malicious HTML coding" (http://aw-snap.info/file-viewer/). Aw-snap.info. Retrieved 19 January 2013.
56. "Example Google.com Safe Browsing Diagnostic page" (http://www.google.com/safebrowsing/diagnostic?site=http://google.com/). Google.com. Retrieved 19 January 2013.
57. "Safe Browsing (Google Online Security Blog)" (http://googleonlinesecurity.blogspot.jp/2012/06/safe-browsing-protecting-web-users-for.html). Retrieved 21 June 2012.
58. Hanspach, Michael; Goetz, Michael (November 2013). "On Covert Acoustical Mesh Networks in Air". *Journal of Communications*. doi:10.12720/jcm.8.11.758-767 (https://dx.doi.org/10.12720%2Fjcm.8.11.758-767).
59. Guri, Mordechai; Monitz, Matan; Mirski, Yisroel; Elovici, Yuval (April 2015). "BitWhisper: Covert Signaling Channel between Air-Gapped Computers using Thermal Manipulations" (http://arxiv.org/abs/1503.07919). *arXiv (C) IEEE*.
60. Guri, Mordechai; Monitz, Matan; Mirski, Yisroel; Elovici, Yuval (March 2015). "BitWhisper: The Heat is on the Air-Gap" (http://cyber.bgu.ac.il/blog/bitwhisper-heat-air-gap). *BGU Cyber Security Labs*.
61. Vincentas (11 July 2013). "Grayware in SpyWareLoop.com" (http://www.spywareloop.com/news/grayware). Spyware Loop. Retrieved 28 July 2013.
62. "Threat Encyclopedia – Generic Grayware" (http://about-threats.trendmicro.com/us/archive/grayware/GENERIC_GRAYWARE). Trend Micro. Retrieved 27 November 2012.
63. "Rating the best anti-malware solutions" (http://arstechnica.com/security/2009/12/av-comparatives-picks-eight-antipua-winners/). Arstechnica. Retrieved 28 January 2014.
64. "PUP Criteria". *https://www.malwarebytes.org/pup/*. Malwarebytes.
65. William A Hendric (4 September 2014). "Computer Virus history" (https://antivirus.comodo.com/blog/computer-safety/short-history-computer-viruses/). *The Register*. Retrieved 29 March 2015.
66. Nick Farrell (20 February 2006). "Linux worm targets PHP flaw" (http://www.theregister.co.uk/2006/02/20/linux_worm/). *The Register*. Retrieved 19 May 2010.
67. John Leyden (28 March 2001). "Highly destructive Linux worm mutating" (http://www.theregister.co.uk/2001/03/28/highly_destructive_linux_worm_mutating/). *The Register*. Retrieved 19 May 2010.
68. "Aggressive net bug makes history" (http://news.bbc.co.uk/2/hi/technology/2720337.stm). *BBC News*. 3 February 2003. Retrieved 19 May 2010.

69. John von Neumann, "Theory of Self-Reproducing Automata", Part 1: Transcripts of lectures given at the University of Illinois, December 1949, Editor: A. W. Burks, University of Illinois, USA, 1966.
70. Fred Cohen, "Computer Viruses", PhD Thesis, University of Southern California, ASP Press, 1988.

External links

- Malicious Software (https://www.dmoz.org/Computers/Security/Malicious_Software) at DMOZ
- Further Reading: Research Papers and Documents about Malware on IDMARCH (Int. Digital Media Archive) (http://www.idmarch.org/document/Malware)
- Advanced Malware Cleaning (http://technet.microsoft.com/en-us/sysinternals/Video/gg618529) – a Microsoft video



Look up ***malware*** in Wiktionary, the free dictionary.