Malware and its types

Malware, short for *malicious software*, consists of programming (code, scripts, active content, and other software) designed to disrupt or deny operation, gather information that leads to loss of privacy or exploitation, gain unauthorized access to system resources, and other abusive behavior. The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code. Malware is not the same as defective software — software that has a legitimate purpose but contains harmful bugs (programming errors).

Purpose

Categorizing malware by its purpose – the intent of the author – can be difficult or impossible. The following categories give us some way to think about malware. Note, however, that some malware might reasonably fit into more than one category.

Pranks

Many early infectious programs, including a number of MS-DOS *viruses*, were written as experiments or pranks. They were generally intended to be harmless or merely annoying, rather than to cause serious damage to computer systems. In some cases, the perpetrator did not realize how much harm his or her creations would do. Young programmers learning about viruses and their techniques wrote them simply for practice, or to see how far they could spread. As late as 1999, widespread viruses such as the Melissa virus appear to have been written chiefly as a prank. Many believe the infamous Morris Worm, that shut down a large part of the Internet in 1988 and started a new era in network security, was a prank. Others are not so sure it belongs in this category.

Smartphone malware is increasing

Cabir is the name of a computer worm developed in 2004 that is designed to infect mobile phones running Symbian OS. It is believed to be the first computer worm that can infect mobile phones. When a phone is infected with Cabir, the message "Caribe" is displayed on the phone's display, and is displayed every time the phone is turned on. The worm then attempts to spread to other phones in the area using wireless Bluetooth signals.

Never released "in the wild", Caribe was sent to anti-virus firms apparently by white hat hackers as a proof of concept.[src]

Intentionally Harmful

Hostile intent related to vandalism can be found in programs designed to cause harm or data loss. Many DOS viruses, and the Windows Explore Zip worm, were designed to destroy files on a hard disk, or to corrupt the file system by writing invalid data to them. Network-born worms, such as the 2001 Code Red worm, fall into the same category. Sometimes designed to vandalize web pages, worms may seem like the online equivalent to graffiti tagging, with the author's alias or affinity group appearing everywhere the worm goes Code Red.

Profit

Since the rise of widespread broadband Internet access, some malicious software has been designed for a profit, like forced advertising, for example. (Some forced advertising causes your browser to redirect you to an advertising page or displays pop-ups.) Since 2003, the majority of widespread viruses and worms have been designed to take control of users' computers for black-market exploitation. Infected "zombie computers" are used to send email spam, to host contraband data such as child pornography, or to engage in distributed denial-of-service attacks as a form of extortion.

Indirect Profit

Another strictly for-profit category of malware has emerged in *spyware* – programs designed to monitor users' web browsing or other activity, display unsolicited advertisements, or redirect affiliate marketing revenues to the spyware creator. Spyware programs do not generally spread like viruses; they are, in general, installed by exploiting security holes or are packaged with*user-installed software*, such as peer-to-peer music sharing applications. Sometimes, the spyware is loaded unknowingly by the user in response to a web page pop-up. The sidebar explaining steps taken to kill a process appeared in the last module.

Windows ActiveX warning

Hacktivism

Hacktivism is the use of (illegal) hacking techniques for an activist cause. Hacktivism could be further defined as "the non-violent use of illegal or legally ambiguous digital tools in pursuit of political ends". These tools include web site defacements, redirects, denial-of-service attacks, information theft, virtual sit-ins, and virtual sabotage.

Like any form of activism, doing something for (what you consider to be) a good cause does not make it legal.

Does hacking imply illegal?

Some argue that in the original use of the term (50 years ago), hacking meant something different. Of course, in that era*cool* had been subverted to mean something that was good, not something at a temperature less than *hot*. A word which has also taken on an oddly similar meaning. *Phat*wasn't a word at all. Times change.

Outside the computing community, the generally understood meaning of "hacker" is one who gains access to computers illegally.

Viruses & Worms

The best-known types of malware, *viruses* and *worms*, are known for the manner in which they spread, rather than any other particular behavior. The term computer virus is used for a program that has infected some executable software and, when run, causes the virus to spread to other executables. Viruses may also perform other actions, like creating a backdoor for later use, damaging files, or even damaging equipment. On the other hand, a worm is a program that actively transmits itself over a network to infect other computers. Worms may also take malicious actions.

These definitions lead to the observation that a virus requires *user intervention* to spread, whereas a worm spreads itself automatically. Using this distinction, infections transmitted by email or Microsoft Word documents, which rely on the recipient opening a file or email to infect the system, would be classified as viruses rather than worms.

Spread of Conficker worm

By Gppande (Own work) [CC-BY-SA-3.0 or GFDL], via Wikimedia Commons

Trojans

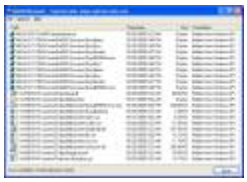
In broad terms, a *Trojan horse* is any program that invites the user to run it, concealing a harmful or malicious payload. The payload may take effect immediately and can lead to many undesirable effects, such as deleting the user's files or further installing malicious or undesirable software. Trojan horses known as *droppers* are used to start off a worm outbreak, by "injecting" the worm into users' local networks.

One of the most common ways that *spyware* is distributed is as a Trojan horse, bundled with a piece of desirable software that the user downloads from the Internet. When the user installs the software, the spyware is installed alongside. Spyware authors who attempt to act in a legal fashion may include an end-user license agreement that states the behavior of the spyware in loose terms, which the users are unlikely to read or understand.

Rootkits

Originally, a *rootkit* was a set of tools installed by a human attacker on a Unix system, allowing the attacker to gain administrator (root) access. Today, the term rootkit is used more generally for concealment routines in a malicious program.

Once a malicious program is installed on a system, it is essential that it stays concealed, to avoid detection and disinfection. The same is true when a human attacker breaks into a computer directly. Techniques 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.



RootkitRevealer showing the files hidden by the Sony DRM rootkit

In an attempt to keep the user from stopping a malicious process, another is sometimes installed to monitor it. When the process is stopped (killed), another is immediately created. Modern malware starts a number of processes that monitor and restore one another as needed. In the event that a user running Microsoft Windows is infected with such malware (if they wish to manually stop it), they could use Task Manager's 'processes' tab to find the main process (the one that spawned the "resurrector process(es)"), and use the 'end process tree' function, which would kill not only the main process, but the "resurrector(s)" as well, since they were started by the main process. Some malware programs use other techniques, such as naming the infected file similar to a legitimate or trustworthy file (expl0rer.exe VS explorer.exe) to avoid detection in the process list.

Backdoors

A *backdoor* is a method of bypassing normal authentication procedures. Once a system has been compromised (by one of the above methods, or in some other way), one or more backdoors may be installed in order to allow easier access in the future. Backdoors may also be installed prior to malicious software, to allow attackers entry.

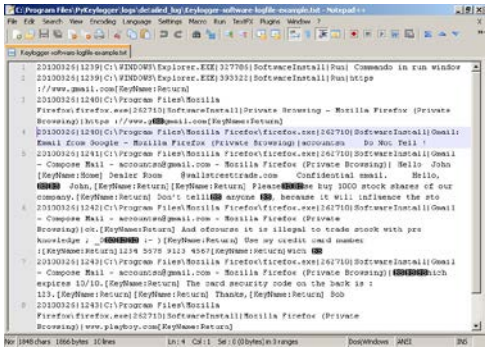
Beast, a Windows-based backdoor Trojan horse –

Spyware

Spyware is a type of malicious software that can be installed on computers, and which collects small pieces of information about users without their knowledge. The presence of spyware is typically hidden from the user, and can be difficult to detect. Typically, spyware is secretly installed on the user's personal computer.

While the term spyware suggests software that secretly monitors the user's computing, the functions of spyware extend well beyond simple monitoring. Spyware programs can collect various types of personal information, such as Internet surfing habits and sites that have been visited, but can also interfere with user control of the computer in other ways, such as installing additional software and redirecting Web browser activity. Spyware is known to change computer settings, resulting in slow connection speeds, different home pages, and/or loss of Internet connection or functionality of other programs. In an attempt to increase the understanding of spyware, a more formal classification of its included software types is provided by the term *privacy-invasive software*.

Classification of code as spyware (or sometimes browser cookies as "tracking" cookies) can be controversial. Often the software is installed by the user knowing that some amount of monitoring will take place. (Users generally agree to this activity to get free software and it is often associated with music and video sharing.) Some such software allows the user to turn off the monitoring, assuming they are aware of it and can find instructions for disabling it. Anti-spyware is usually part of anti-virus programs; scan using at least two different AV packages. Spybot Search and Destroy is a good freeware program for looking for spyware (but it is not an AV program).



A logfile from a software-basedkeylogger.
By Own work [GPL or Attribution], via Wikimedia Commons

Loggers

Keystroke logging (often called keylogging) is the action of tracking (or logging) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that their actions are being monitored. There are numerous keylogging methods, ranging from hardware and software-based approaches to electromagnetic and acoustic analysis.

Key logging is often used by law enforcement, parents, and jealous or suspicious spouses (lovers). The most common use, however, is in the workplace, where your employer is monitoring your use of the computer. Unfortunately, all of these activities are legal.

Adware

Adware, or advertising-supported software, is any software package which automatically plays, displays, or downloads advertisements to a computer. These advertisements can be in the form of a pop-up. The object of the Adware is to generate revenue for its author. Adware, by itself, is harmless; however, some adware may come with integrated spyware such as keyloggers and other privacy-invasive software.

Advertising functions are integrated into or bundled with the software, which is often designed to note what Internet sites the user visits and to present advertising pertinent to the types of goods or services featured there. Adware is usually seen by the developer as a way to recover development costs, and in some cases it may allow the software to be provided to the user free of charge or at a reduced price. The income derived from presenting advertisements to the user may allow or motivate the developer to continue to develop, maintain and upgrade the software product. Conversely, the advertisements may be seen by the user as interruptions or annoyances, or as distractions from the task at hand.

Some adware is also shareware, and so the word may be used as a term of distinction to differentiate between types of shareware software. What differentiates adware from other shareware is that it is primarily advertising-supported, like many free smartphone apps. Users may also be given the option to pay for a "registered" or "licensed" copy to do away with the advertisements. Pandora Radio offers both a free version (with ads) and a paid subscription (without ads).

There is a group of software (Alexa toolbar, Google toolbar, Eclipse data usage collector, etc.) that send data to a central server about which pages have been visited or which features of the software have been used. However differently from "classic" malware these tools document activities and only send data with the user's approval. The user may opt in to share the data in exchange to the additional features and services, or (in case of Eclipse) as the form of voluntary support for the project. Some security tools report such loggers as malware while others do not. The status of the group is questionable. Some tools like PDF Creator are more on the boundary than others because opting out has been made more complex than it could be (during the installation, the user needs to uncheck two check boxes rather than one). However, PDF Creator is only sometimes mentioned as malware and is still subject of discussions.

Source: http://cs.sru.edu/~mullins/cpsc100book/module05_SoftwareAndAdmin/module05-04_softwareAndAdmin.html