UNIT-2 Malware and its types

Learning Outcomes
By the end of this unit the learner will be able to:
✓ Understand the different types of malware ✓ Discuss the risks posed by malware ✓ Identify the sources of malware and implement safeguards

Unit 2

Malware and its types

What is Malware?

Malware is short for malicious software, meaning software that can be used to compromise computer functions, steal data, bypass access controls, or otherwise cause harm to the host computer. Malware is a broad term that refers to a variety of malicious programs. This post will define several of the most common types of malware; adware, bots, bugs, rootkits, spyware, Trojan horses, viruses, and worms.

Bot

Bots are software programs created to automatically perform specific operations. While some bots are created for relatively harmless purposes (video gaming, internet auctions, online contests, etc), it is becoming increasingly common to see bots being used maliciously. Bots can be used in botnets (collections of computers to be controlled by third parties) for DDoS attacks, as spambots that render advertisements on websites, as web spiders that scrape server data, and for distributing malware disguised as popular search items on download sites. Websites can guard against bots with CAPTCHA tests that verify users as human.

Bug

In the context of software, a bug is a flaw produces an undesired outcome. These flaws are usually the result of human error and typically exist in the source code or compilers of a program. Minor bugs only slightly affect a program's behavior and as a result can go for long periods of time before being discovered. More significant bugs can cause crashing or freezing. Security bugs are the most severe type of bugs and can allow attackers to bypass user authentication, override access privileges, or steal data. Bugs can be prevented with developer education, quality control, and code analysis tools.

The following categories give us some way to think about malware. Note, however, that some malware might reasonably fit into more than one category.

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.

Fig. 2.1 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.

Fig. 2.2

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.

Fig. 2.3

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).

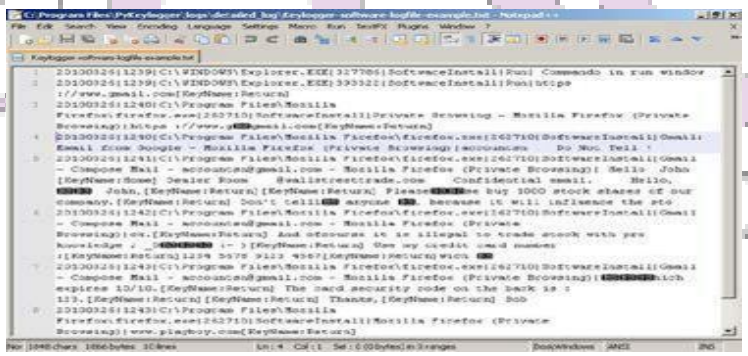

Fig. 2.4 A logfile from a software-basedkeylogger.

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.

Malware Symptoms

While these types of malware differ greatly in how they spread and infect computers, they all can produce similar symptoms. Computers that are infected with malware can exhibit any of the following symptoms:

- Increased CPU usage
- Slow computer or web browser speed

- Problems connecting to networks
- Freezing or crashing
- Modified or deleted files
- Appearance of strange files, programs, or desktop icons
- Programs running, turning off, or reconfiguring themselves (malware will often reconfigure or turn off antivirus and firewall programs)
- Strange computer behavior
- Emails/messages being sent automatically and without user's knowledge (a friend receives a strange email from you that you did not send)

Spam

Spam is the electronic sending of mass unsolicited messages. The most common medium for spam is email, but it is not uncommon for spammers to use instant messages, texting, blogs, web forums, search engines, and social media. While spam is not actually a type of malware, it is very common for malware to spread through spamming. This happens when computers that are infected with viruses, worms, or other malware are used to distribute spam messages containing more malware. Users can prevent getting spammed by avoiding unfamiliar emails and keeping their email addresses as private as possible.

Vandals

Web sites have come alive through the development of such software applications as ActiveX and Java Applets. These devices enable animation and other special effects to run, making Web sites more attractive and interactive.

However, the ease with which these applications can be downloaded and run has provided a new vehicle for inflicting damage. A vandal is a software application or applet that causes destruction of varying degrees. A vandal can destroy just a single file or a major portion of a computer system.

Attacks

Innumerable types of network attacks have been documented, and they are commonly classified in three general categories: reconnaissance attacks, access attacks, and denial of service (DoS) attacks.

Reconnaissance Attacks

Active reconnaissance is a type of computer attack in which an intruder engages with the targeted system to gather information about vulnerabilities. Both active and passive reconnaissance are also used for ethical hacking, in which white hat hackers use attack methods to determine system vulnerabilities so that problems can be taken care of before the system falls prey to a real attack.

Access Attacks

There are four types of access attacks: password attacks, trust exploitation, port redirection and man-in-the middle attacks.

A Network attacker uses packet sniffer tools to obtain user accounts and passwords information. Normally we log in and out of a system using authentication passwords to shared resources in a router or server, an attacker also repeatedly attempts to log in to a shared resource or to gain unauthorised access to an organisation's network; this can also be referred to as dictionary or brute force attacks.

Trust exploitation attacker is to compromise a trusted host, using it to stage attacks on other hosts in a network. If a host in a network of a company is protected by a firewall (inside host), but is accessible to a trusted host outside the firewall (outside host), the inside host can be attacked through the trusted outside host.

A port redirection attack is another type of attack based on trust exploitation. The attacker uses a compromised host to gain access through a firewall that would otherwise be blocked.

Data Interception

Data transmitted via any type of network can be subject to interception by unauthorized parties. The perpetrators might eavesdrop on communications or even alter the data packets being transmitted. Perpetrators can use various methods to intercept the data. IP spoofing, for example, entails posing as an authorized party in the data transmission by using the Internet Protocol (IP) address of one of the data recipients.

Social Engineering

Social engineering is the increasingly prevalent act of obtaining confidential network security information through non-technical means. For example, a social engineer might pose as a technical support representative and make calls to employees to gather password information. Other examples of social engineering include bribing an associate to gain access to a server or searching a colleague's office to find a password that has been written in a hidden spot.

Further Reading:

- ✓ ***Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software (Paperback), 2011 by Michael Sikorski***
- ✓ ***Windows Malware Analysis Essentials, 2015 by Victor Marak***