An introduction to malware

Previously, you learned that **malware** is software designed to harm devices or networks. Since its first appearance on personal computers decades ago, malware has developed into a variety of strains. Being able to identify different types of malware and understand the ways in which they are spread will help you stay alert and be informed as a security professional.

Icônes représentant différents types de logiciels malveillants

Virus

A **virus** is malicious code written to interfere with computer operations and cause damage to data and software. This type of malware must be installed by the target user before it can spread itself and cause damage. One of the many ways that viruses are spread is through phishing campaigns where malicious links are hidden within links or attachments.

Worm

A **worm** is malware that can duplicate and spread itself across systems on its own. Similar to a virus, a worm must be installed by the target user and can also be spread with tactics like malicious email. Given a worm's ability to spread on its own, attackers sometimes target devices, drives, or files that have shared access over a network.

A well known example is the Blaster worm, also known as Lovesan, Lovsan, or MSBlast. In the early 2000s, this worm spread itself on computers running Windows XP and Windows 2000 operating systems. It would force devices into a continuous loop of shutting down and restarting. Although it did not damage the infected devices, it was able to spread itself to hundreds of thousands of users around the world. Many variants of the Blaster worm have been deployed since the original and can infect modern computers.

Note: Worms were very popular attacks in the mid 2000s but are less frequently used in recent years.

Trojan

A trojan, also called a **Trojan horse**, is malware that looks like a legitimate file or program. This characteristic relates to how trojans are spread. Similar to viruses, attackers deliver this type of malware hidden in file and application downloads. Attackers rely on tricking unsuspecting users into believing they’re downloading a harmless file, when they’re actually infecting their own device with malware that can be used to spy on them, grant access to other devices, and more.

Adware

Advertising-supported software, or **adware**, is a type of legitimate software that is sometimes used to display digital advertisements in applications. Software developers often use adware as a way to lower their production costs or to make their products free to the public—also known as freeware or shareware. In these instances, developers monetize their product through ad revenue rather than at the expense of their users.

Malicious adware falls into a sub-category of malware known as a **potentially unwanted application (PUA)**. A PUA is a type of unwanted software that is bundled in with legitimate programs which might display ads, cause device slowdown, or install other software. Attackers sometimes hide this type of malware in freeware with insecure design to monetize ads for themselves instead of the developer. This works even when the user has declined to receive ads.

Spyware

Spyware is malware that's used to gather and sell information without consent. It's also considered a PUA. Spyware is commonly hidden in *bundleware*, additional software that is sometimes packaged with other applications. PUAs like spyware have become a serious challenge in the open-source software development ecosystem. That’s because developers tend to overlook how their software could be misused or abused by others.

Scareware

Another type of PUA is **scareware**. This type of malware employs tactics to frighten users into infecting their own device. Scareware tricks users by displaying fake warnings that appear to come from legitimate companies. Email and pop-ups are just a couple of ways scareware is spread. Both can be used to deliver phony warnings with false claims about the user's files or data being at risk.

Fileless malware

Fileless malware does not need to be installed by the user because it uses legitimate programs that are already installed to infect a computer. This type of infection resides in memory where the

malware never touches the hard drive. This is unlike the other types of malware, which are stored within a file on disk. Instead, these stealthy infections get into the operating system or hide within trusted applications.

Pro tip: Fileless malware is detected by performing memory analysis, which requires experience with operating systems.

Rootkits

A **rootkit** is malware that provides remote, administrative access to a computer. Most attackers use rootkits to open a backdoor to systems, allowing them to install other forms of malware or to conduct network security attacks.

This kind of malware is often spread by a combination of two components: a dropper and a loader. A **dropper** is a type of malware that comes packed with malicious code which is delivered and installed onto a target system. For example, a dropper is often disguised as a legitimate file, such as a document, an image, or an executable to deceive its target into opening, or dropping it, onto their device. If the user opens the dropper program, its malicious code is executed and it hides itself on the target system.

Multi-staged malware attacks, where multiple packets of malicious code are deployed, commonly use a variation called a loader. A **loader** is a type of malware that downloads strains of malicious code from an external source and installs them onto a target system. Attackers might use loaders for different purposes, such as to set up another type of malware---a botnet.

Botnet

A **botnet**, short for “robot network,” is a collection of computers infected by malware that are under the control of a single threat actor, known as the “bot-herder.” Viruses, worms, and trojans are often used to spread the initial infection and turn the devices into a bot for the bot-herder. The attacker then uses file sharing, email, or social media application protocols to create new bots and grow the botnet. When a target unknowingly opens the malicious file, the computer, or bot, reports the information back to the bot-herder, who can execute commands on the infected computer.

Ransomware

Ransomware describes a malicious attack where threat actors encrypt an organization's data and demand payment to restore access. According to the Cybersecurity and Infrastructure Security Agency (CISA), ransomware crimes are on the rise and becoming increasingly sophisticated. Ransomware infections can cause significant damage to an organization and its customers. An example is the

WannaCry attack that encrypts a victim's computer until a ransom payment of cryptocurrency is paid.

Key takeaways

The variety of malware is astounding. The number of ways that it’s spread is even more staggering. Malware is a complex threat that can require its own specialization in cybersecurity.

One place to learn more about malware analysis is INFOSEC's introductory course on malware analysis. Even without specializing in malware analysis, recognizing the types of malware and how they’re spread is an important part of defending against these attacks as a security analyst.

Revision #1
Created 2023-08-27 13:22:04 UTC by naruzkurai
Updated 2023-08-27 13:22:51 UTC by naruzkurai