Cyberattack Techniques and Types – Malware and Ransomware

Attackers use a variety of techniques and attack types to achieve their objectives. *Malware* and *exploits* are integral to the modern cyberattack strategy. Spamming and phishing are commonly employed techniques to deliver malware and exploits to an endpoint via an email executable or a web link to a malicious website. After an endpoint is compromised, an attacker typically installs backdoors, remote access Trojans, and other malware to ensure persistence. Compromised endpoints ("bots") under the control of an attacker are often used to perpetrate much larger-scale attacks against other organizations or networks as part of a botnet. This section describes different types of malware, vulnerabilities, and exploits; business email compromise (BEC), and how bots and botnets function, along with different types of botnets.

Key Terms

Malware is malicious software or code that typically takes control of, collects information from, or damages an infected endpoint. Malware broadly includes viruses, worms, Trojan horses (including remote access Trojans, or RATs), ransomware, anti-AV, logic bombs, backdoors, rootkits, bootkits, spyware, and (to a lesser extent) adware.

An *exploit* is a small piece of software code, part of a malformed data file, or a sequence (string) of commands that leverages a vulnerability in a system or software, causing unintended or unanticipated behavior in the system or software.

A *vulnerability* is a bug or flaw that exists in a system or software and creates a security risk.

Malware

Malware is malicious software or code that typically takes control of, collects information from, or damages an infected endpoint. Malware broadly includes:

Viruses. A virus is malware that is self-replicating but must first infect a host program and be executed by a user or process.

Worms. A worm is malware that typically targets a computer network by replicating itself to spread rapidly. Unlike viruses, worms do not need to infect other programs and do not need to be executed by a user or process.

Trojan horses. A Trojan horse is malware that is disguised as a harmless program but actually gives an attacker full control and elevated privileges of an endpoint when installed. Unlike other types of malware, Trojan horses are typically not self-replicating.

Ransomware. Ransomware is malware that locks a computer or device (Locker ransomware) or encrypts data (Crypto ransomware) on an infected endpoint with an encryption key that only the attacker knows, thereby making the data unusable until the victim pays a ransom (usually cryptocurrency, such as Bitcoin). Reveton and LockeR are two examples of Locker ransomware. Locky, TeslaCrypt/EccKrypt, Cryptolocker, and Cryptowall are examples of Crypto ransomware.

Anti-AV. Anti-AV is malware that disables legitimately installed antivirus software on the compromised endpoint, thereby preventing automatic detection and removal of other malware.

Logic bombs. A logic bomb is malware that is triggered by a specified condition, such as a given date or a particular user account being disabled.

Backdoors. A backdoor is malware that allows an attacker to bypass authentication to gain access to a compromised system.

Rootkits. A rootkit is malware that provides privileged (root-level) access to a computer. Rootkits are installed in the BIOS of a machine, which means operating system-level security tools cannot detect them.

Bootkits. A bootkit is malware that is a kernel-mode variant of a rootkit, commonly used to attack computers that are protected by full-disk encryption.

Spyware and adware. Spyware and adware are types of malware that collect information, such as internet surfing behavior, login credentials, and financial account information on an infected endpoint. Spyware often changes browser and other software settings, and slows computer and internet speeds on an infected endpoint. Adware is spyware that displays annoying advertisements on an infected endpoint, often as pop-up banners.

Key Terms

A *boot sector virus* targets the boot sector or *master boot record* (MBR) of an endpoint's storage drive or other removable storage media.

A *boot sector* contains machine code that is loaded into an endpoint's memory by firmware during the startup process, before the operating system is loaded.

A *master boot record* (MBR) contains information about how the logical partitions (or file systems) are organized on the storage media and an executable boot loader that starts up the installed operating system.

A *floppy disk* is a removable magnetic storage medium commonly used from the mid-1970s until about 2007, when it was largely replaced by compact discs and removable USB storage devices. Floppy disks were typically available in 8-inch, 5¼-inch, and 3½-inch sizes with capacities from 90 kilobytes to 200 megabytes.

Early malware typically consisted of viruses that displayed annoying – but relatively benign – errors, messages, or graphics.

The first computer virus was Elk Cloner, written in 1982 by a ninth-grade high school student near Pittsburgh, Pennsylvania. Elk Cloner was a relatively benign *boot sector* virus that displayed a poem on the fiftieth time that an infected *floppy disk* was inserted into an Apple II computer.

The first PC virus was a boot sector virus, written in 1986, called Brain. Brain was also relatively benign and displayed a message with the actual contact information for the creators of the virus. Brain was written by two Pakistani brothers who created the virus so that they could track piracy of their medical software.

One of the first computer worms to gain widespread notoriety was the Morris worm, written by a Harvard and Cornell University graduate student, Robert Tappan Morris, in 1988. The worm exploited weak passwords and known vulnerabilities in several Unix programs and spread rapidly across the early internet (the worm infected up to an estimated 10 percent of all Unix machines connected to the internet at that time – about 6,000 computers), sometimes infecting a computer numerous times to the point that it was rendered useless – an example of an early DoS attack. The U.S. Government Accountability Office (GAO) estimated the damage caused by the Morris worm between US$100,000 and US$10 million.

Unfortunately, more than 35 years since these early examples of malware, modern malware has evolved and is used for far more sinister purposes. Examples of modern malware include:

WannaCry. In a period of just 24 hours in May 2017, the WannaCry ransomware attack infected more than 230,000 vulnerable Windows computers in more than 150 countries worldwide. Although the attack was quickly halted after the discovery of a "kill switch," the total economic damage is estimated between hundreds of millions to as much as US$4 billion, despite the perpetrators collecting only 327 ransom payments totaling about US$130,000.

HenBox. HenBox typically masquerades as legitimate Android system and VPN apps, and sometimes drops and installs legitimate versions of other apps as a decoy. The primary goal of the HenBox apps appears to be to spy on those who install them. By using traits similar to legitimate apps, for example, copycat iconography and app or package names, HenBox lures victims into downloading and installing the malicious apps from third-party, non-Google Play app stores that often have fewer security and vetting procedures for the apps they host. As with other Android malware, some apps may also be available on forums or file-sharing sites, or even may be sent to victims as email attachments.

TeleRAT. Telegram Bots are special accounts that do not require an additional phone number to set up and are generally used to enrich Telegram chats with content from external services or to get customized notifications and news. TeleRAT abuses Telegram's Bot API for C2 and data exfiltration.

Rarog. Rarog is a cryptocurrency-mining Trojan that has been sold on various underground forums since June 2017 and has been used by countless criminals since then. Rarog has been primarily used to mine the Monero cryptocurrency. However, it can mine others. It comes equipped with several features, including providing mining statistics to users, configuring various processor loads for the running miner, the ability to infect USB devices, and the ability to load additional *dynamic-link libraries* (DLLs) on the victim device. Rarog provides an affordable way for new criminals to gain entry using this particular type of malware. Other examples of cryptocurrency miners include Coinhive, JSE-Coin, Crypto-Loot, and CoinImp.

Key Terms

A *dynamic-link library* (DLL) is a type of file used in Microsoft operating systems that enables multiple programs to simultaneously share programming instructions contained in a single file to perform specific functions.

Modern malware is typically stealthy and evasive, and now plays a central role in a coordinated attack against a target.

Advanced malware leverages networks to gain power and resilience, and can be updated – just like any other software application – so that an attacker can change course and dig deeper into the network or make changes and enact countermeasures.

This is a fundamental shift compared to earlier types of malware, which were generally independent agents that simply infected and replicated themselves. Advanced malware increasingly has become a centrally coordinated, networked application in a very real sense. In much the same way that the internet changed what was possible in personal computing, ubiquitous network access is changing what is possible in the world of malware. Now all malware of the same type can work together toward a common goal, with each infected endpoint expanding the attack foothold and increasing the potential damage to the organization.

Important characteristics and capabilities of advanced malware include:

Distributed, fault-tolerant architecture. Advanced malware takes full advantage of the resiliency built into the internet itself. Advanced malware can have multiple control servers distributed all over the world with multiple fallback options, and can also leverage other infected endpoints as communication channels, thus providing a near infinite number of communication paths to adapt to changing conditions or update code as needed.

Multifunctionality. Updates from C2 servers can also completely change the functionality of advanced malware. This multifunctional capability enables an attacker to use various endpoints strategically to accomplish specific desired tasks, such as stealing credit card numbers, sending spam containing other malware payloads (such as spyware), or installing ransomware for the purpose of extortion.

Polymorphism and metamorphism. Some advanced malware has entire sections of code that serve no purpose other than to change the signature of the malware, thus producing an infinite number of unique signature hashes for even the smallest of malware programs. Techniques such as *polymorphism* and *metamorphism* are used to avoid detection by traditional signature-based anti-malware tools and software. For example, a change of just a single character or bit of the file or source code completely changes the *hash signature* of the malware.

Obfuscation. Advanced malware often uses common *obfuscation* techniques to hide certain binary strings that are characteristically used in malware and therefore are easily detected by anti-malware signatures, or to hide an entire malware program.

Key Terms

Polymorphism alters part of the malware code with every iteration, such as the encryption key or decryption routine, but the malware payload remains unchanged.

Metamorphism uses more advanced techniques than polymorphism to alter malware code with each iteration. Although the malware payload changes with each iteration – for example, by using a different code structure or sequence or by inserting garbage code to change the file size – the fundamental behavior of the malware payload remains unchanged.

A *hash signature* is a cryptographic representation of an entire file or program's source code.

Obfuscation is a programming technique used to render code unreadable. It can be implemented by using a simple substitution cipher, such as an *exclusive or* (XOR) operation – in which the output is true only when the inputs are different (for example, TRUE and TRUE equals FALSE, but TRUE and FALSE equals TRUE) – or by using more sophisticated encryption algorithms, such as the *Advanced Encryption Standard* (AES). Alternatively, a *packer* can be used to compress a malware program for delivery and then decompress it in memory at runtime.

Ransomware

Although ransomware is technically classified as malware, the surge in ransomware attacks over the past five years warrants additional consideration. Ransomware is a criminal business model that uses malware to hold something of value for ransom. Victims of a ransomware attack may have their operations severely degraded or shut down entirely. Although cryptographic ransomware is the most common and successful type of ransomware, it is not the only one. It's important to remember that ransomware is not a single family of malware but is a criminal business model in which malware is used to hold something of value for ransom.

While holding something of value for ransom is not a new concept, ransomware has become a multibillion-dollar criminal business targeting both individuals and corporations. Due to its low barriers to entry and effectiveness in generating revenue, it has quickly displaced other cybercrime business models and become the largest threat facing organizations today. It is also important to note that although threat actors generally do decrypt your data after the ransom is paid (the ransomware business model depends on a reasonable expectation that paying a ransom will restore access to your data), there are no guarantees that this will be the case. Additionally, many threat actors are now exfiltrating a copy of their victims' data – particularly PII and credit card numbers – before encrypting it, then selling the data on the dark web after the ransom is paid.

For a ransomware attack to be successful, attackers must execute the following five steps:

1. **Compromise and control a system or device.** Ransomware attacks typically begin by using social engineering to trick users into opening an attachment or viewing a malicious link in their web browser. This allows attackers to install malware onto a system and take control. However, another increasingly common tactic is for attackers to gain access to the network, perform reconnaissance on the network to identify potential targets and establish C2, install other malware and create backdoor accounts for persistence, and potentially exfiltrate data.

2. **Prevent access to the system.** Attackers will either identify and encrypt certain file types or deny access to the entire system.

3. **Notify victim.** Though seemingly obvious, attackers and victims often speak different languages and have varying levels of technical capabilities. Attackers must alert the victim about the compromise, state the demanded ransom amount, and explain the steps for regaining access.

4. **Accept ransom payment.** To receive payment while evading law enforcement, attackers utilize cryptocurrencies such as Bitcoin for the transaction.

5. **Return full access.** Attackers must return access to the device(s). Failure to restore the compromised systems destroys the effectiveness of the scheme as no one would be willing to pay a ransom if they didn't believe their valuables would be returned.

If the attacker fails in any of these steps, the scheme will be unsuccessful. Although the concept of ransomware has existed for decades, the technology and techniques, such as reliable encrypting and decrypting, required to complete all five of these steps on a wide scale were not available until just a few years ago.

Though the malware deployed in the current generation of cryptographic ransomware attacks is not especially sophisticated, it has proven very effective at not only generating revenue for the criminal operators but also preventing impacted organizations from continuing their normal operations. New headlines each week demonstrate that organizations large and small are vulnerable to these threats, enticing new attackers to jump onto the bandwagon and begin launching their own ransomware campaigns.