Types of Malware Used by Threat Actors

Common malware types include Trojans, Backdoors, Worms, Viruses, Rootkits etc. and are widely used by many individual attackers to some of the largest hacker groups in the world. Countless types, forms and variants of these malware have been developed and released into the wild.

TROJANS

A Trojan is a malware which is designed to look like a completely legitimate application to the victim. Once the malicious application has been installed, the Trojan can inconspicuously install a backdoor on the victim machine and allow persistent access, log keystrokes, download more malware, encrypt critical data and steal private information. Since Trojans only work if the victim is enticed into installing the application which it is disguised as, elements of social engineering may be utilized to assist in this process.

An example of a notorious Trojan which targeted banking systems in Russia and conducted spying activities on the victim systems is Ibank. Ibank allows command and control through a backdoor, network traffic interception and modification, keylogging, blocking of antimalware and theft of access credentials. Ibank collects and saves critical data from the victim system before transferring it to the attacker's servers.

BACKDOORS

A backdoor is a general term to describe any software or application which grants external entities direct privileged access to the system, thus bypassing security measures. The 'external entity' may be a malicious threat actor or a manufacturer trying to reset a forgotten password. Backdoors can lead to persistent access on a victim machine, installation of other malware, remote command execution and even total compromise. Backdoors are very similar to trojans, however, trojans are the legitimate-looking programs that deliver malware which can install a backdoor, whereas backdoors include any intentional security exposure on a system. As mentioned, backdoors can come from malware, or be hard-coded/built into a machine within the supply chain.

Hupigon is a backdoor trojan which opens a backdoor server on the victim system to allow command and control and join a botnet. Hupigon can perform spying activities, such as stealing login credentials, keylogging and capturing video. Hupigon cannot spread on its own like a worm, so it is sent in an email or hosted on a website. Once installed, files and processes related to Hupigon are concealed through intercepting Windows API calls and it uses the registry to automatically start at boot.

WORMS

A worm is a malware that can self-replicate and spread to other systems, without needing user interaction. Worms can carry payloads which are able to perform actions on the victim systems, including installing backdoors and causing denial of service. Worms can spread through many vectors, including email, instant messaging, network services and removable storage. As worms manipulate components of the underlying OS, they are mostly inconspicuous to ordinary users and usually will not be recognized until performance issues occur. Worms are characterized by their insane infection speeds, as exemplified by the 15 minutes it took for the SQL Slammer worm to take over servers worldwide.

Stuxnet is arguably the most infamous worm ever, due to its usage to obstruct the development of nuclear weapons in Iran. Stuxnet was a highly complex and unique worm, which only targeted the computers used in the Iranian uranium enrichment facilities and was able to modify the programming of PLCs (programmable logic controllers) to make the centrifuges malfunction. Stuxnet utilized multiple Windows 0-days to infect computers, then checked if it used a specific type of PLC, and if it did, modified its programming to make the centrifuges spin too quickly.

VIRUSES

A virus is a malware that attaches itself to files on the victim system and causes abnormal behavior when run. Unlike worms, viruses require user interaction to run and infect other hosts. When executed, viruses can perform a wide range of activities, including corrupting data, flooding network traffic and gaining remote control over the target machine. There are numerous types of viruses, including macro viruses – where applications that allow "macros", or embedded code, such as Microsoft Word, have malicious code within them – and boot sector viruses – which infects the Master Boot Record and runs when the system is booted from the infected drive or when it accesses infected removable media.

The Melissa virus was an email-based macro virus that caused $80 million in damage in the US and infected hundreds of thousands of systems worldwide. The virus would be included in a Word document that has been sent in an email to the victim, and once the victim opened the document, the malicious macro would run and send the same malicious email to 50 addresses in Outlook. Although the virus itself did not cause direct damage on its victims, the fast infection rate slowed Internet speeds and led Microsoft to shut down its email service.

ROOTKITS

A rootkit is a type of malware which is designed to stay inconspicuous and covertly gather critical data and credentials, open a backdoor with which an attacker can remotely control the system, hide other malware, log keystrokes etc.. Rootkits can infect the system BIOS, the bootloader, memory or applications, and are very difficult to detect as they have OS-level security privileges and thus can undermine any antivirus software attempts to find them. Unlike viruses and worms, rootkits cannot self-replicate, so they typically infect other systems through direct attacks, phishing emails and malicious downloads. For example, an attacker would manually attack the system and escalate to administrator or root, then install a rootkit.

Sony's Extended Copy Protection (XCP), which aimed to provide DRM for CDs, was found to be secretly installing a hidden rootkit in 2005. The XCP rootkit disallowed any software from accessing music on the CDs other than the included media player, through intercepting calls to the CD and mixing returned read data with random bytes. The rootkit was installed without the user's consent and was not included in the EULA. The XCP rootkit constantly over-utilized system resources and hid itself by making all files and processes that start with sys invisible to the user. This led to unrelated malware manipulating this cloaking mechanism to conceal itself from the user. Overall, the XCP rootkit reminds us of the frightening fact that sometimes, the most trusted corporations can deceive its users.

RANSOMWARE

Ransomware is a form of malware which is becoming increasingly more common, and encrypts or blocks access to files on the target system and requests payment (usually through cryptocurrency) in order to decrypt them. Ransomware uses asymmetric ciphers (ciphers with two keys for encryption and decryption), such as RSA, to encrypt files with a public key and demand payment to decrypt them with a private key. Ransomware infections mostly occur through emails that utilize social engineering and malicious attachments, and drive-by downloads which allow files to be downloaded just by viewing a website. Some types of ransomware, such as "scareware", do not encrypt files, instead using popups to coerce the user into making a payment.

CryptoLocker was a ransomware that used trojans to infect its hundreds of thousands of victim Windows PCs. The trojan would be sent as a ZIP file attachment in a seemingly harmless email and disguised as a PDF file in the zipped file. When CryptoLocker is run, it generates an RSA key pair and encrypts certain types of local files, including Word documents and pictures. In order to decrypt the files, the victim must pay a ransom of around $400 within 72 hours to retrieve the RSA private key and decryption program. The attackers are believed to have gained a total of around $3 million from CryptoLocker victims.

ADVANCED: APT MALWARE

Advanced Persistent Threats are highly sophisticated and often state-sponsored groups of attackers and typically develop and utilize custom-built malware to penetrate its targets. An intimidating example of a custom malware is Flame, which is actually believed to be developed by the NSA, CIA and the Israeli military.

Flame is a highly complex, modular malware that was found in 2012 to be conducting intelligence gathering and cyber espionage on several Middle Eastern countries. Flame could record audio from the microphone, take screenshots and steal documents and send them back to the operators. Flame had an extremely large file size of 20MB and it took researchers several months to analyze its code, demonstrating the sheer complexity specially-crafted malware can have.

‹ Previous Topic

Mark Complete ✓

Next Topic ›

Back to Lesson