Malware: Keeping Your Company Safe Inside

Author: eFraudPrevention

BankUnited

Threats are continuously evolving but your firewall protection may not. Now is the time to look beyond traditional network security and incorporate protection against malware and exploits that pass-through PCs and mobile devices when users browse the Internet, send or receive an email, and download applications.

The software which enables these crimes is categorized as malware. As worrisome as malware is—and it continues to get worse—there are straightforward and extremely effective ways to address it. But first, know your enemy. Typical malware consists of six main types—viruses, worms, Trojans, spyware, adware, and rootkits.

Viruses

Probably the best-known type of malware is the virus. Computer viruses have been around for decades, however, the basic premise has remained constant. Typically designed to inflict damage against the end user, computer viruses can purge an entire hard disk, rendering data useless in a matter of moments.

Just as biological viruses replicate themselves when infecting a host cell, computer viruses will often replicate and spread themselves through an infected system. Other types of viruses are used for ‘seek and destroy’ where specific file types or portions of the hard disk are targeted. Criminals conducting cyber-thefts will often unleash a virus on penetrated systems after extracting the desired information as a means of destroying forensic evidence.

Computer viruses were originally spread through the sharing of infected floppy disks. As the technology evolved so too did the distribution method. Today, viruses are commonly spread through file sharing, web downloads, and email attachments. In order to infect a system, the virus must be executed on the target system; dormant computer viruses which have not been executed do not pose an immediate threat. Viruses typically do not possess any legitimate purposes and in some countries are illegal to possess.

Worms

Computer worms have existed since the late 1980s but were not prevalent until networking infrastructures within organizations became common. Unlike computer viruses, worms have the capability of spreading themselves through networks without any human interaction.

Once infected by a worm, the compromised system will begin scanning the local network in an attempt locates additional victims. After locating a target, the worm will exploit software vulnerabilities in a remote system, injecting it with malicious code in order to complete the compromise. Due to their means of attack, worms are only successful at infecting systems on the network which are running specific operating systems. Worms are often viewed more as a nuisance than a real threat. However, they may be used to spread other malware or inflict damage against target systems.

Trojans

Like viruses, Trojans typically require some type of user interaction in order to infect a system. However, unlike most worms and viruses, Trojans often try to remain undetected on the compromised host. Trojans are small pieces of executable code embedded into another application. Typically the infected file is an application the victim would use regularly (such as Microsoft Word or Calculator). The goal is for the victim to unknowingly execute the malicious code when launching an otherwise innocent program.

This often results in Trojans infecting a system without triggering any type of notification. There are several types of Trojans, each fulfilling a different purpose. Some Trojans are designed specifically to extract sensitive data from the infected system; these types of Trojans typically install keyloggers or take screenshots of the victim's computer and automatically transmit the information back to the attacker. Other, more dangerous "remote access Trojans" (RATs), will take control of the infected system, opening up a back door for an attacker to later access. Remote access Trojans are typically used in the creation of botnets.

Spyware/Adware

Like some types of Trojans, spyware is used to collect and relay sensitive information back to its distributor. Spyware typically is not malicious in nature. However, it is a major nuisance, typically infecting web browsers, and making them nearly inoperable. Spyware is often used for deceitful marketing purposes, such as monitoring user activity without their knowledge. At times, spyware may be disguised as a legitimate application, providing the user with some benefit while secretly recording behavior and usage patterns.

Like spyware, adware is a major nuisance for users. But it is usually not malicious in nature. Adware, as the name implies, is typically used to spread advertisements providing some type of financial benefit to the attacker. After becoming infected by adware, the victim becomes bombarded by pop-ups, toolbars, and other types of advertisements when attempting to access the Internet. Adware usually does not cause permanent damage to a computer. However, it can render the system inoperable if not removed properly.

Rootkits

Arguably the most dangerous type of malware is the rootkit. Like remote access Trojans, rootkits provide the attacker with control over an infected system. However, unlike Trojans, rootkits are exceptionally difficult to detect or remove. Rootkits are typically installed into low-level system resources (below the operating system). Because of this, rootkits often go undetected by conventional anti-virus software. Once infected with a rootkit, the target system may be accessible by an attacker providing unrestricted access to the rest of the network.

Knowing when you've got one Malware in network traffic or on a computer makes its presence known one of three ways:

- Signature" is a fingerprint or pattern in the file that can be recognized by a network security system like a firewall even before it gets to a computer. If such a file actually gets to a computer, the anti-virus/anti-malware software on the machine should catch it.
- A suspect file type appearing out of context, like an executable (.exe) or registry value hidden in a compressed file like a .zip.
- Behavior; even a rootkit may reveal itself when it "phones home" to the operator who controls it. If this behavior is abnormal—for instance, in volume or time of day—this can be an indicator of a compromised system.

All content is for informational purposes only and does not constitute legal, tax, or accounting advice. You should consult your legal and tax or accounting advisors before making any financial decisions.