What is Malware?

Malware is short for ***mal***icious soft***ware***, 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. Following are explained several of the most common types of malware; adware, bots, bugs, rootkits, spyware, Trojan horses, viruses, and worms.

Adware

Adware (short for advertising-supported software) is a type of malware that automatically delivers advertisements. Common examples of adware include pop-up ads on websites and advertisements that are displayed by software. Often times software and applications offer “free” versions that come bundled with adware. Most adware is sponsored or authored by advertisers and serves as a revenue generating tool. While some adware is solely designed to deliver advertisements, it is not uncommon for adware to come bundled with spyware (see below) that is capable of tracking user activity and stealing information. Due to the added capabilities of spyware, adware/spyware bundles are significantly more dangerous than adware on its own.

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.

Ransomware

Ransomware is a form of malware that essentially holds a computer system captive while demanding a ransom. The malware restricts user access to the computer either by encrypting files on the hard drive or locking down the system and displaying messages that are intended to force the user to pay the malware creator to remove the restrictions and regain access to their computer. Ransomware typically spreads like a normal computer worm (see below) ending up on a computer via a downloaded file or through some other vulnerability in a network service.

Rootkit

A rootkit is a type of malicious software designed to remotely access or control a computer without being detected by users or security programs. Once a rootkit has been installed it is possible for the malicious party behind the rootkit to remotely execute files, access/steal information, modify system configurations, alter software (especially any security software that could detect the rootkit), install concealed malware, or control the computer as part of a botnet. Rootkit prevention, detection, and removal can be difficult due to their stealthy operation. Because a rootkit continually hides its presence, typical security products are not effective in detecting and removing rootkits. As a result, rootkit detection relies on manual methods such as monitoring computer behavior for irregular activity, signature scanning, and storage dump analysis. Organizations and users can protect themselves from rootkits by regularly patching vulnerabilities in software, applications, and operating systems, updating virus definitions, avoiding suspicious downloads, and performing static analysis scans.

Spyware

Spyware is a type of malware that functions by spying on user activity without their knowledge. These spying capabilities can include activity monitoring, collecting keystrokes, data harvesting (account information, logins, financial data), and more. Spyware often has additional capabilities as well, ranging from modifying security settings of software or browsers to interfering with network connections. Spyware spreads by exploiting software vulnerabilities, bundling itself with legitimate software, or in Trojans.

Trojan Horse

A Trojan horse, commonly known as a “Trojan,” is a type of malware that disguises itself as a normal file or program to trick users into downloading and installing malware. A Trojan can give a malicious party remote access to an infected computer. Once an attacker has access to an infected computer, it is possible for the attacker to steal data (logins, financial data, even electronic money), install more malware, modify files, monitor user activity (screen watching, keylogging, etc), use the computer in botnets, and anonymize internet activity by the attacker.

Virus

A virus is a form of malware that is capable of copying itself and spreading to other computers. Viruses often spread to other computers by attaching themselves to various programs and executing code when a user launches one of those infected programs. Viruses can also spread through script files, documents, and cross-site scripting vulnerabilities in web apps. Viruses can be used to steal information, harm host computers and networks, create botnets, steal money, render advertisements, and more.

Worm

Computer worms are among the most common types of malware. They spread over computer networks by exploiting operating system vulnerabilities. Worms typically cause harm to their host networks by consuming bandwidth and overloading web servers. Computer worms can also contain “payloads” that damage host computers. Payloads are pieces of code written to perform actions on affected computers beyond simply spreading the worm. Payloads are commonly designed to steal data, delete files, or create botnets. Computer worms can be classified as a type of computer virus, but there are several characteristics that distinguish computer worms from regular viruses. A major difference is that computer worms have the ability to self-replicate and spread independently while viruses rely on human activity to spread (running a program, opening a file, etc). Worms often spread by sending mass emails with infected attachments to users' contacts.

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 speeds
- 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)

Malware Prevention and Removal

There are several general best practices that organizations and individual users should follow to prevent malware infections. Some malware cases require special prevention and treatment methods, but following these recommendations will greatly increase a user's protection from a wide range of malware:

- Install and run anti-malware and firewall software. When selecting software, choose a program that offers tools for detecting, quarantining, and removing multiple types of malware. At the minimum, anti-malware software should protect against viruses, spyware, adware, Trojans, and worms. The combination of anti-malware software and a firewall will ensure that all incoming and existing data gets scanned for malware and that malware can be safely removed once detected.
- Keep software and operating systems up to date with current vulnerability patches. These patches are often released to patch bugs or other security flaws that could be exploited by attackers.
- Be vigilant when downloading files, programs, attachments, etc. Downloads that seem strange or are from an unfamiliar source often contain malware.

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.