Enrique Hower

COM 327 CA01

Malware Writing Project

Malware

Malicious software, or malware, is any software intentionally designed to cause damage to a computer, server, client, or computer network. A wide variety of types of malware exist, common categories include: computer viruses, worms, Trojan horses, ransomware, spyware, adware, and scareware. Each type of malware has its own unique way of causing havoc, and most rely on user action of some kind. Some strains are delivered over email via a link or executable file. Others are delivered via instant messaging or social media. Even mobile phones are vulnerable to attack.

Types of Malware

Worms

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, such as running a file or opening a program to spread. Worms often spread by sending mass emails with infected attachments to users' contacts.

Adware

Adware, or advertising 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 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.

Bots

Bots are software programs created to automatically perform specific operations. While some bots are created for relatively harmless purposes such as video gaming, internet auctions and online contests, it is becoming increasingly common to see bots being used maliciously. Bots can be used in a collection of computers to be controlled by third parties called botnets 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.

Trojan Horse

A Trojan horse 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 such as login information, financial data, even electronic

money. An attacker also has the ability to install more malware, modify files, monitor user activity, 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.

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 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.

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 attacker to remotely execute files, access and steal information, modify system configurations, alter software, 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.

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 ending up on a computer via a downloaded file or through some other vulnerability in a network service.

Bug

In the context of software, a bug is a flaw that 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.

Preventative Measures

Keep Software Up to Date

Software makers like Microsoft and Oracle routinely update their software to fix bugs that could potentially be exploited by hackers.

Don't Click on Links Within Emails

A good rule of thumb is if you don't recognize a sender of an email, don't click on any links within it. 44.8 percent of Windows virus infections happen because the computer user clicked on something.

Use Free Antivirus Software

Using free antivirus software is an inexpensive way to protect a computer and safeguard against various forms of malware.

Use a Strong Password

A strong password is one that is complex, with a mix of letters, numbers, and symbols. Avoid using the same password for multiple programs.

Minimize Downloads

Make sure your Web browser's security settings are high enough to detect unauthorized downloads. For Internet Explorer, the medium security setting is the minimum level to use.

Use a Pop-Up Blocker

Web browsers have the ability to stop pop-up windows and allow you to set the security for accepting pop-ups. Because pop-ups are regularly infected with malware, it is recommended to never clicking on links within pop-up screens.

References

Grimes, R. A. (2019, May 1). *9 types of malware and how to recognize them*. Retrieved from csoonline.com: https://www.csoonline.com/article/2615925/security-your-quick-guide-to-malware-types.html

Love, J. (2018, March 28). *Malware Types and Classifications*. Retrieved from lastline.com: https://www.lastline.com/blog/malware-types-and-classifications/

Regan, J. (2019, July 11). *What is Malware? How Malware*. Retrieved from avg.com: https://www.avg.com/en/signal/what-is-malware

Sowells, J. (n.d.). *Understanding the Threat*. Retrieved from uscybersecurity.net: https://www.uscybersecurity.net/malware/

What is Malware and How to Defend Against It? (n.d.). Retrieved from kaspersky.com: https://usa.kaspersky.com/resource-center/preemptive-safety/what-is-malware-and-how-to-protect-against-it

What is Malware? (n.d.). Retrieved from forcepoint.com: https://www.forcepoint.com/cyber-edu/malware