Malware Attacks

-Trojans and Ransomware focused

Author: Hangbo Zhang, Clement Chow

Abastrc

The purpose of this paper is to specifically focus on two types of malware: trojans and ransomware. To discuss what they are, how it works, method of spread, possible damage caused by them, common types of them and some famous examples, and also to show the ways to detect, prevent and recover from them.

Introduction

Malware (a portmanteau for malicious software) is any software intentionally designed to cause disruption to a computer, server, client, or computer network, leak private information, gain unauthorized access to information or systems, deprive users access to information or which unknowingly interferes with the user's computer security and privacy. By contrast, software that causes harm due to some deficiency is typically described as a software bug. Malware poses serious problems to individuals and businesses on the Internet. According to Symantec's 2018 Internet Security Threat Report (ISTR), malware variants number has increased to 669,947,865 in 2017, which is twice as many malware variants as in 2016. Cybercrime, which includes malware attacks as well as other crimes committed by computer, was predicted to cost the world economy 6 trillion dollars in 2021, and is increasing at a rate of 15% per year.

There are many types of malware that exist and are still active nowadays.

- Virus: A computer virus can replicate itself by modifying other programs and inserting its malicious code once it is executed. It is the only malware that can "infect" other files, and is one of the most difficult malware to remove.
- Worms: Worms replicate themselves without end-user involvement and can be transferred from one machine to another, spreading rapidly throughout the network
- Trojan horses: Trojan horse malware is one of the most difficult types of malware to detect because it masquerades as a legitimate program. This type of malware contains malicious code and instructions that once executed by the victim can be used to do whatever they want without being detected. It is often used to let other types of malware into the system.
- Hybrid malware: Modern malware is usually a "hybrid" or combination of multiple malware. For example, a "bot program" first appears as a Trojan horse and then acts as a worm once it is executed. They are often used to target individual users in larger network-wide attacks.
- Adware: Adware delivers unwanted and unauthorized advertisements (e.g., pop-ups) to end users.
- Malvertising: Malvertising uses legitimate advertisements to deliver malicious software to end-user computers.
- Spyware: Spyware secretly spies on unsuspecting end-users, collecting credentials and passwords, browsing history, etc.

The defense strategies against malware differs according to the type of malware but most can be thwarted by installing antivirus software, firewalls, applying regular patches to reduce zero-day attacks, securing networks from intrusion, having regular backups and isolating infected systems. Malware is now being designed to evade antivirus software detection algorithms.

Following are two detailed discovery and analysis of the two types of the malware: Trojan and Ransomware.

Trojan

I. Background

A. What is it

In computing, a Trojan is any malware that misleads users of its true intent. The term is derived from the Ancient Greek story of the deceptive Trojan horse that led to the fall of the city of Troy.

B. How it works

A Trojan will hide any malicious codes/activities inside a normal looking application. So it can be easily downloaded and opened by the user to achieve the purpose of the distributor, normally acting as a backdoor to contact a controller who can then have unauthorized access to the affected computer.

II. Types

A. Method to spread

Trojans generally spread by some form of social engineering such as phishing email where a user is duped into executing an email attachment disguised to appear not suspicious, or by clicking on some fake advertisement link. Unlike computer viruses, and worms, trojans generally do not attempt to inject themselves into other files or otherwise propagate themselves.

B. Damage

When a Trojan horse becomes active, it puts sensitive user data at risk and can negatively impact performance. Once a Trojan has been transferred, it can:

- give the attacker backdoor control over the computing device;
- record keyboard strokes to steal the user's account data and browsing history;
- download and install a virus or worm to exploit a vulnerability in another program;
- install ransomware to encrypt the user's data and extort money for the decryption key;
- activate the computing device's camera and recording capabilities;

- turn the computer into a zombie computer that can be used to carry out click fraud schemes or illegal actions;
- legally capture information relevant to a criminal investigation for law enforcement.

C. Famous Event(Example)

- Bitfrost, a remote access Trojan that infected Windows clients by changing, creating and altering components
- Tiny Banker, which allowed attackers to steal sensitive financial information. Researchers in the Center for Strategic and International Studies Security Group identified 'Tinba' in 2012 after two dozen major U.S. banks were infected.
- FakeAV Trojan, which embedded itself in the Windows system tray and continuously delivered an official-looking pop-up window, alerting the user to a problem with the computer. When users followed directions to fix the problem, they actually downloaded more malware.
- Magic Lantern, a government Trojan that uses keystroke logging, created by the FBI around the turn of the century to assist with criminal surveillance.
- Zeus, a financial services crimeware toolkit that allows a hacker to build their own Trojan horse. First detected in 2007, the Trojans built with Zeus still remain the most dangerous banking Trojans in the world, using form grabbing, keylogging and polymorphic variants of the Trojan that use drive-by downloads to capture victim credentials.

D. Common types of Trojan

- Downloader Trojan, which is a Trojan that targets a computer that is already affected by downloading and installing new versions of malicious programs.
- Backdoor Trojan, which creates a backdoor on the computer, enabling an attacker's access and control of the computer. Backdoor Trojans can allow data to be downloaded by third parties or stolen as well as additional malware to be uploaded.
- Distributed Denial of Service (DDoS) attack Trojan, which performs a DDoS attack on the computer and attempts to take down a network by flooding it with traffic that comes from the target infected computer and others.
- Game-thief Trojan, which targets online gamers and attempts to steal their account information.
- Mailfinder Trojan, which attempts to steal email addresses stored on a targeted device.
- SMS Trojan, which is a Trojan that infects mobile devices and has the ability to send or intercept text messages.
- Trojan banker, which attempts to steal financial accounts. This Trojan is designed to take the account information for all online activities, including credit card, banking and bill pay data.

III. Counter Measure

A. Detection

Since Trojan horses frequently appear disguised as legitimate system files, they are often very hard to find and destroy with conventional virus and malware scanners. Specialized software tools are often necessary for the identification and removal of discrete Trojan horses.

However, it's possible to identify the presence of a Trojan horse through unusual behaviors displayed by a computer. The quirks could include:

1. A change in the computer's screen, including changing color and resolution or an unnecessary flip upside down.
2. Excessive amounts of pop-up ads will appear, offering solutions to various errors which might prompt the end user to click on the ad.
3. The computer mouse may start moving by itself or freezing up completely and the functions of the mouse buttons may reverse.
4. The browser's home page may change or the browser will consistently redirect the user to a different website than the one they are requesting. This redirected website will often contain an offer that users can click on or download which will, in turn, install more malware.
5. The computer's antivirus and antimalware programs will be disabled and the necessary steps to remove malware will be inaccessible.
6. Mysterious messages and abnormal graphic displays may start appearing.
7. Unrecognized programs will be running in the task manager.
8. The taskbar will either change in appearance or completely disappear.
9. The computer's desktop wallpaper may change as well as the format of desktop icons and applications.
10. The user's personal email service may start sending spam messages to all or some of the addresses in the contact list that frequently contain malware and a persuasive tactic to get recipients to open and download the attack, thus spreading the Trojan horse to other computers.

B. Prevention

1. Computer security must start with Internet security software. Use your software to run diagnostic scans regularly. You can set the program to run scans automatically at regular intervals.

2. Update your operating system as soon as the software company releases updates. These types of Trojans tend to exploit security vulnerabilities in outdated software programs. In addition to updating your operating system, you should also check for updates to any other software you use on your computer.

3. Don't visit unsafe websites. Most Internet security packages include a component that warns you that the site you are about to visit is not secure.

4. Do not download attachments or click on links in unfamiliar emails.

5. Protect your account with a complex and unique password.

6. You should always use a firewall to maintain the security of your personal information.

C. Recover

If a Trojan horse is identified on a computer, the system should immediately be disconnected from the Internet and the questionable files should be removed using an antivirus or antimalware program or by reinstalling the operating system.

The hardest part of the removal process is recognizing which files are infected. Once the Trojan has been identified, the rest of the process becomes simpler. Users can sometimes find the infected files using the dynamic link library (DLL) error which is frequently presented by the computer to signify the presence of a Trojan horse. This error can be copied and searched online to find information about the affected exe file.

Once the files are identified, the System Restore function must be disabled. If this function is not disabled, then all the malicious files that are deleted will be restored and will infect the computer once again.

Next, users must restart their computer. While restarting, users should press the F8 key and select safe mode. Once the computer has successfully started up, users should access Add or Remove programs in the control panel. From here, the infected programs can be removed and deleted. In order to ensure all extensions associated with the Trojan application are removed, all of the program files should be deleted from the system.

Once this is complete, the system should be restarted once again, but this time in the normal start-up mode. This should complete the Trojan horse removal process.

Ransomware

I. Background

A. What is it

Ransomware is a computer virus that takes control of a user's computer or encrypts data and then demands a ransom in order to resume normal operations. The most notorious examples of ransomware are Reveton, CryptoLocker and WannaCry. Ransomware is usually spread through phishing attacks or clickjacking. Once a virus

is installed, users lose the ability to access their computer data or use their computer. Many ransomware attacks require ransom to be paid via cryptocurrency such as Bitcoin.

B. How it works

Ransomware is a type of malware from cryptovirology that threatens to publish the victim's personal data or perpetually block access to it unless a ransom is paid. While some simple ransomware may lock the system without damaging any files, more advanced malware uses a technique called cryptoviral extortion. It encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them. In a properly implemented cryptoviral extortion attack, recovering the files without the decryption key is an intractable problem – and difficult to trace digital currencies such as pay-safecard or Bitcoin and other cryptocurrencies are used for the ransoms, making tracing and prosecuting the perpetrators difficult.

Ransomware is spread through virus files that must be installed by the user as an .exe. Once the virus enters the network, it may spread laterally between devices. In this case, ransomware is also known as a worm. A network user may install a file on the local computer by mistake due to a phishing attack or a clickjacking attack. If antivirus software is installed on the network, it must have the signature of the ransomware attack file or be detectable by suspicious activity. Otherwise, the file may escape detection.

II. Types

A. Method to spread

Ransomware attacks are typically carried out using a Trojan disguised as a legitimate file that the user is tricked into downloading or opening when it arrives as an email attachment. However, one high-profile example, the WannaCry worm, traveled automatically between computers without user interaction

B. Targeted

The target's "geographic location" and "revenue number" are determining factors in the attacker's ideal target. At the same time, ransomware participants are also cautious about some "disallowed industries" and "disallowed countries.

Geographic location: Nearly half (47 percent) of ransomware attackers cited the United States as their most desirable location. This is followed closely by Canada, Australia and European countries.

Revenue number: On average, ransomware attackers expect to extort at least $100 million per attack, which requires that the annual revenue size of purchased access control targets be high enough. However, attackers sometimes specify different ransom amounts for different

locations; for example, ransom attacks targeting developing countries will result in substantially lower ransom amounts than in the United States.

Disallowed Industries: Almost half (47%) of ransomware attackers say they are unlikely to attack companies involved in healthcare and schooling. Slightly fewer (37 percent) refuse to target government departments, and in addition, about a quarter of ransomware participants claim they would not attack those nonprofit organizations.

Disallowed countries/regions: There are some attackers who refuse to target businesses or institutions in Russian-speaking countries. The rationale is that if they do not attack the region, local law enforcement will not bother them. There are also some who refuse to target South America as well as developing countries, where they believe they will not get enough money from their attack operations.

C. Damage

The damage of a ransomware attack is much more than the financial loss; more seriously, it can cause additional complications to businesses and organizations, resulting in multiple losses such as data destruction or loss, productivity disruption, normal business interruption, and corporate reputation damage.

D. Famous Event(Example)

- CryptoLocker: generated a 2048-bit RSA key pair and uploaded in turn to a command-and-control server, and used to encrypt files using a whitelist of specific file extensions. The malware threatened to delete the private key if a payment of Bitcoin or a pre-paid cash voucher was not made within 3 days of the infection. Due to the extremely large key size it uses, analysts and those affected by the Trojan considered CryptoLocker extremely difficult to repair.
- Reveton: In 2012, a major ransomware Trojan known as Reveton began to spread. Based on the Citadel Trojan (which, itself, is based on the Zeus Trojan), its payload displays a warning purportedly from a law enforcement agency claiming that the computer has been used for illegal activities, such as downloading unlicensed software or child pornography. Due to this behavior, it is commonly referred to as the "Police Trojan". The warning informs the user that to unlock their system, they would have to pay a fine using a voucher from an anonymous prepaid cash service such as Ukash or pay-safecard. To increase the illusion that the computer is being tracked by law enforcement, the screen also displays the computer's IP address, while some versions display footage from a victim's webcam to give the illusion that the user is being recorded.

- Fusob: Like a typical mobile ransomware, it employs scare tactics to extort people to pay a ransom.[94] The program pretends to be an accusatory authority, demanding the victim to pay a fine from $100 to $200 USD or otherwise face a fictitious charge. Rather surprisingly, Fusob suggests using iTunes gift cards for payment. Also, a timer clicking down on the screen adds to the users' anxiety as well.
- Petya: It was first discovered in March 2016; unlike other forms of encrypting ransomware, the malware aimed to infect the master boot record, installing a payload which encrypts the file tables of the NTFS file system the next time that the infected system boots, blocking the system from booting into Windows at all until the ransom is paid. Check Point reported that despite what it believed to be an innovative evolution in ransomware design, it had resulted in relatively-fewer infections than other ransomware active around the same time frame.

E. Common Types

Three main types of ransomware include scareware, screen lockers, and encrypting ransomware:

- Scareware: Scareware, as it turns out, is not that scary. It includes rogue security software and tech support scams. You might receive a pop-up message claiming that malware was discovered and the only way to get rid of it is to pay up. If you do nothing, you'll likely continue to be bombarded with pop-ups, but your files are essentially safe. A legitimate cybersecurity software program would not solicit customers in this way. If you don't already have this company's software on your computer, then they would not be monitoring you for ransomware infection. If you do have security software, you wouldn't need to pay to have the infection removed—you've already paid for the software to do that very job.
- Screen lockers: Upgrade to terror alert orange for these guys. When lock-screen ransomware gets on your computer, it means you're frozen out of your PC entirely. Upon starting up your computer, a full-size window will appear, often accompanied by an official-looking FBI or US Department of Justice seal saying illegal activity has been detected on your computer and you must pay a fine. However, the FBI would not freeze you out of your computer or demand payment for illegal activity. If they suspected you of piracy, child pornography, or other cybercrimes, they would go through the appropriate legal channels.
- Encrypting ransomware: This is the truly nasty stuff. These are the guys who snatch up your files and encrypt them, demanding payment in order to decrypt and redeliver. The reason why this type of ransomware is so dangerous is because once cybercriminals get ahold of your files, no security software or system restore can return them to you. Unless you pay the ransom—for the most part, they're gone. And even if you do pay

up, there’s no guarantee the cybercriminals will give you those files back.

III. Counter Measure

A. Detection & Prevention

They say an ounce of prevention is worth a pound of cure. This is certainly true when it comes to ransomware. If an attacker encrypts your device and demands a ransom, there’s no guarantee they will unencrypt it whether or not you pay up.

Ransomware is scary because you can lose important personal and business data in the process, and even if you pay the ransom, there may be other short- and long-term effects. However, there are a number of anti-ransomware strategies you can use to protect yourself and your business.

1. Back up your data
Do not store all your data in one location. Back up your data regularly so that you can restore lost data after ransomware attacks and other disasters. Note that CryptoLocker will also find and encrypt data on mapped drives. Therefore, you should schedule regular backup schedules to back up data to an external backup service or drive that is not assigned a drive number or disconnected when no backup is performed.

2. Show hidden file extensions
CryptoLocker files often have the extension ".PDF.EXE" because attackers understand that the default behavior of Windows is to hide known file extensions. Therefore, you can easily find suspicious files by enabling your computer to view full file extensions.

3.Disable running files from the Local AppData or AppData folder
One of the most famous behaviors of CryptoLocker is running executable files from Local AppData and AppData folders. Therefore, you can create rules on your system through Windows or intrusion prevention software to disable this behavior. You can also always exclude legitimate program files that run from the AppData area.

4.Filtering EXEs in email
If your gateway email scanner can filter incoming files by extension, it is recommended that emails with ".exe" file extensions or files with multiple file extensions (one of which is an executable file extension) be rejected.

If, after rejecting emails with .exe extensions, you do need to receive or send executable files in your environment, you can choose to receive emails using password-protected ZIP files or through cloud services.

5. Disable RDP

Cryptolocker/Filecoder accesses the target computer via Remote Desktop Protocol (RDP). This is a Windows utility that allows other users to access your desktop remotely. Disabling DRP will protect your computer from remote attacks.

6.Train your employees
Security is always a shared responsibility between you and your employees. Therefore, it is important to always provide timely and routine training to your employees on resisting cybercrime, so that they understand the system, network security, threat assessment, and their respective roles and responsibilities.

7. Patch or update your software
Malware authors often count on people to run outdated software with known vulnerabilities so that they can exploit them for personal or financial gain. Therefore, updating your software regularly can significantly reduce your chances of being attacked, and some vendors issue regular security updates and emergency updates.

You can enable automatic updates or manually visit the vendor's website to get updates. Note that criminals also like to disguise their software as update notifications.

8. Use an effective security suite
Deploying both a software firewall and anti-malware software helps you identify potential threats or suspicious behavior. One of these two layers of defense is indispensable, as malware authors often issue new variants to evade detection.

Most malware types rely on remote commands to initiate execution. If you happen to find a new ransomware variant that bypasses your security software, there is little chance that it will bypass the firewall because it will attempt to connect remotely to the bot command server.

9. Prevent Unauthorized Access
There are a number of precautions you can take to avoid unauthorized access. These security practices can greatly improve your defenses from all kinds of cyber attacks. For example,Never install any software or grant administrator privileges unless the software comes from a trusted source and you know what it does.Install anti-virus software to help your system detect any malicious programs.Install whitelisting software to prevent any unauthorized applications from executing.

10. Use reasonable restrictions
You should impose certain restrictions on the following contractors or employees.Use devices that contain company records, files, or programsUse devices that are connected to the Company's network and that may be inadequately protectedAre third parties or temporary workers

11. use appropriate credential tracking
Anyone, employee or contractor with access to your systems could create a potential point of vulnerability for an attacker. Mistakes, inappropriate restrictions and failure to update passwords can all lead to an increased probability of being attacked.

B. Recover

If you do find yourself with a ransomware infection, the number one rule is to never pay the ransom.

One potential option for removing ransomware is that you may be able to retrieve some encrypted files by using free decryptors. To be clear: Not all ransomware families have had decryptors created for them, in many cases because the ransomware is utilizing advanced and sophisticated encryption algorithms. And even if there is a decryptor, it's not always clear if it's for the right version of the malware. You don't want to further encrypt your files by using the wrong decryption script. Therefore, you'll need to pay close attention to the ransom message itself, or perhaps ask the advice of a security/IT specialist before trying anything.

Other ways to deal with a ransomware infection include downloading a security product known for remediation and running a scan to remove the threat. You may not get your files back, but you can rest assured the infection will be cleaned up. For screen locking ransomware, a full system restore might be in order. If that doesn't work, you can try running a scan from a bootable CD or USB drive.

Conclusion

As we can conclude from the two types of malware above: the most common way of spreading malware is social engineering, the most common damage caused by the malware is financial lost (either the direct lost as ransom or indirect lost as the cost to recover the system), the most easy and common ways to detect and prevent the attack are to install a good anti-malware software and self-awareness (not click or download suspicious link or software). And also having a good backup routine can help reduce the damage of the attack and cost of recovery.

References

Introduction to malware definition attacks types and analysis. Introduction To Malware Definition Attacks Types And Analysis. (n.d.). Retrieved May 3, 2022, from https://www.greycampus.com/blog/information-security/introduction-to-malware-definition-attacks-types-and-analysis

8 most common types of malware attacks. Arctic Wolf. (2021, October 21). Retrieved May 3, 2022, from https://arcticwolf.com/resources/blog/8-types-of-malware

Wikimedia Foundation. (2022, April 12). *Trojan horse (computing)*. Wikipedia. Retrieved May 3, 2022, from https://en.wikipedia.org/wiki/Trojan_horse_(computing)

Kaspersky. (2021, October 5). *What is a trojan horse and what damage can it do?* www.kaspersky.com. Retrieved May 3, 2022, from https://www.kaspersky.com/resource-center/threats/trojans

Gatefy. (2021, June 4). 11 real and famous cases of malware attacks. Gatefy. Retrieved May 3, 2022, from https://gatefy.com/blog/real-and-famous-cases-malware-attacks/

What is ransomware? Information Security Office. (n.d.). Retrieved May 3, 2022, from https://security.berkeley.edu/faq/ransomware/

Kaspersky. (2022, February 9). Ransomware attacks and types – how encryption trojans differ. www.kaspersky.com. Retrieved May 3, 2022, from https://www.kaspersky.com/resource-center/threats/ransomware-attacks-and-types

Kaspersky. (2022, February 17). Ransomware protection: How to keep your data safe in 2022. www.kaspersky.com. Retrieved May 3, 2022, from https://www.kaspersky.com/resource-center/threats/how-to-prevent-ransomware

7 steps to help prevent & limit the impact of Ransomware. CIS. (2021, July 15). Retrieved May 3, 2022, from https://www.cisecurity.org/insights/blog/7-steps-to-help-prevent-limit-the-impact-of-ransomware

Boehm, J., Hall, F., Isenberg, R., & Michel, M. (2022, March 3). Ransomware prevention: How organizations can fight back. McKinsey & Company. Retrieved May 3, 2022, from https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/ransomware-prevention-how-organizations-can-fight-back

Ransomware data recovery: 5 ways to save your data. Cloudian. (2022, January 31). Retrieved May 3, 2022, from https://cloudian.com/guides/ransomware-backup/ransomware-data-recovery-5-ways-to-save-your-data/