Computer Security Midterm

Part A: Malware Research

Contents

Malwares

Malware 1: TicTacToe Dropper

TicTacToe Dropper is a trojan dropper, a malicious program designed to install other malware to a victim's device. TicTacToe Dropper was first discovered around 15 February 2024, it injects final stage payloads into users' devices. It operates through deception, exploiting phishing emails with attached .ISO files. Files with .ISO extension are designed to bypass initial antivirus checks. When unsuspecting users install and run these files, the dropper initiates a multi-stage infection chain.

This infection chain involves multiple stages, where nested .DLL payload files are executed one after another into the device memory. This allows them to evade file-based detection from antivirus software. When executed, depending on the attackers' intent, they can steal sensitive data, install additional malware, and more.

To mitigate the risks posed by TicTacToe Dropper and similar trojan attacks, users should be alert to phishing attacks. When handling emails from unknown sources, users should avoid installing or opening suspicious attachments. Additionally, users should also use unique and complex passwords for each application and website and enable Multi-Factor Authentication (MFA) wherever possible. MFA adds an extra layer of security by requiring further verification even with a password.

If a device is confirmed to be infected, users should disconnect the infected device from the internet to prevent data being transferred to the attackers. Running a thorough antivirus scan using reputable antivirus software can also help detect and remove the dropper and the additional malware installed. Furthermore, users should back up their important data as soon as possible before the virus crash the system to prevent further data loss.

(258 words)

Malware 2: Hermetic Wiper

Hermetic Wiper is a destructive trojan that aims to wipe or erase the contents of the infected system and render systems inoperable. Unlike ransomware that encrypts data for ransom, wiper malware aims for complete destruction.

Hermetic Wiper is first discovered around 23 February 2022, it is known for its use in cyberattacks against Ukraine, deleting data permanently from their system where it is almost impossible to recover the deleted data. It is normally spread through phishing emails. When executed, it corrupts the Master Boot Record (MBR), a data that tells the system where the operating system files are stored, and essentially wipes the data storage structure of the infected system. It is also designed to bypass detections from security software by disguising as a legitimate program that interact with storage components.

To prevent a system from being infected by similar wiper malwares, users should regularly back up important data to a separate hardware device or a cloud storage. In a case of an attack, having backups allows user to recover the lost data to minimize impact. Additionally, having a latest version of a reputable antivirus software can help detect and remove malicious programs.

If a device is confirmed to be infected, victim should immediately shut down the running processes in their task manager and disconnect the device from the network. This may prevent further spread of the malware. Although data recovery from Hermetic Wiper is almost impossible, victim should still hire cybersecurity professionals for assistance in system or data recovery.

(250 words)

Malware 3: ESXiArg

ESXiArg is a ransomware, a type of malicious program designed to encrypt a victim's important data so they cannot access them until a price is paid. It was first discovered in January 2023, known for its attacks on VNware ESXi servers.

ESXiArg encrypts files that were stored in the VMware ESXi servers, demanding a ransom payment in cryptocurrency from the victim before decrypting the files. It targets organizations that are running unpatched versions of ESXi by exploiting the vulnerabilities in the outdated servers. ESXiArg scans for ESXi servers on a network and exploits the vulnerabilities to gain access to the whole server. Once it gets access to the server, it encrypts all the critical server files including the disk files, configuration files and more. The ransomware then leaves a ransom note, demanding payment in Bitcoin, and threatens to leak parts of the file and permanently delete the rest if the ransom is not paid within a specified time frame.

To prevent a server from being infected by ESXiArg or similar malwares, administrators of the virtual servers should always ensure that their servers are up to date with the latest security updates, which may have patched the existing vulnerabilities to prevent possible attacks. Additionally, users should conduct regular vulnerability and malware scanning to identify and fix the vulnerability before it is too late.

If a victim's server is infected by ESXiArg or similar malwares, victims are not recommended to pay the ransom as it does not guarantee the return of data, and it may also fuel further attacks. Victim should disconnect the infected server from the network to prevent the ransomware from spreading to the servers in the network. Furthermore, victims should consult with cybersecurity professionals and law enforcement for guidance on the way to respond and data recovery.

(298 words)

Malware 4: Dracarys

Dracarys is an Android trojan spyware, a malicious program that monitors the activity and steal sensitive information from a device. It was first discovered in July 2022, known for targeting unsuspected users as a pirated premium application.

Dracarys is usually distributed in fake pirating websites. It often disguises as a popular and trending apps to trick users into installing it, after which it operates in the background, sending the victim's data to the attackers without the victim noticing. When installed, the app usually asks user for the permission to access their folders and contacts. Once allowed, the spyware can gain access to different sensitive information, including contacts, location, browsing history, gallery, and more. Additionally, it can also record audio, video, as well as taking screenshots and images.

To prevent the risks posed by Dracarys and similar malwares, users should only download apps from trusted sources such as the official app store, Google Play Store. Users should also enable Google Play Protect security service or their respective app store built in security service to help notify users of the potential threat posed by an application. Additionally, staying vigilant when allowing permission requested by an application and limiting them to what is necessary would also help to data leak.

If a device is infected by a spyware, the victim should immediately disconnect the infected device from the internet, this helps to prevent the spyware from sending out more of the victim's data. After that, running a thorough scan with a reputable anti-virus software may help identify and remove the root of the spyware program. Once the spyware is removed, it is recommended to change the passwords for all the accounts stored in the infected device in case the previous password was already compromised.

(291 words)

Malware 5: Laplas Clipper

Laplas Clipper is a type of information stealing malware mainly targeting cryptocurrency users. It is a Malware-as-a-Service (Maas), available for purchase and use by cybercriminals. It was first discovered in 2022, known for monitoring and modifying clipboard data on an infected system.

Laplas Clipper usually spreads through malicious software downloads or a trojan loader that install additional malwares. Once installed, it monitors the users who copy and paste cryptocurrency wallet addresses during transactions. When it detects a copied cryptocurrency wallet address, it replaces them with the attacker's wallet address. Wallet addresses are complex and difficult to memorise, Bitcoin addresses for example, are usually 34 characters long, consisting of random digits and case-sensitive letters, making it difficult for users to notice the substituted wallet address before completing the transaction. As a result, the cryptocurrency would be redirected to the attacker's wallet.

To mitigate the risks posed by Laplas Clipper or similar malwares, users should always double-check wallet addresses before proceeding with any cryptocurrency transactions. Additionally, relevant cryptocurrency trading platforms should educate users about the existence and the dangers of clipboard hijacking, which can reduce the risk of users falling victim to similar information stealing malware. Furthermore, users could use hardware wallets instead, they store keys and addresses offline, making them immune to malware on the device.

If a device is confirmed to be infected, users should immediately conduct a thorough anti-virus scan using a reputable anti-virus software to detect and remove the root of the clipper. Once removed, users should review their recent cryptocurrency transactions to check if there are any redirected transactions and notify the relevant trading platform.

(268 words)

References:

TicTacToe Dropper

1. Eric Ford, Sr. Threat Intelligence Analyst (2024). Cyber Intel Brief: February 15 - 21, 2024. [Online] Deep Watch [Accessed: 21 June 2024]. Available at: https://www.deepwatch.com/labs/cyber-intel-brief-february-15-21-2024/
2. Threatcop (2024). TicTacToe Dropper: New Malware Distribution Tactics Revealed. [Online] LinkedIn [Accessed: 21 June 2024]. Available at: https://www.linkedin.com/pulse/tictactoe-dropper-new-malware-distribution-tactics-revealed-avuyf
3. CyberThreat (2024). TicTacToe Dropper Unleashes Data Theft and Multi-Threat Spread on Windows Systems. [Online] InfoShare Systems [Accessed: 21 June 2024]. Available at: https://varutra.com/ctp/threatpost/postDetails/TicTacToe-Dropper-Unleashes-Data-Theft-and-Multi-Threat-Spread-on-Windows-Systems/R0hkYUFtVlEvcDR0a2ZDbmVVOUZiUT09

Hermetic Wiper

1. Cybersecurity Advisory (2022). Update: Destructive Malware Targeting Organizations in Ukraine. [Online] Cybersecurity and Infrastructure Security Agency CISA [Accessed: 22 June 2024]. Available at: https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-057a
2. Malwarebytes (2022). What is HermeticWiper? [Online] ThreatDown by Malwarebytes. [Accessed: 22 June 2024]. Available at: https://www.threatdown.com/glossary/what-is-hermeticwiper/

ESXiArg

1. Bob Plankers (2023). ESXiArgs: Questions & Answers [Online] VMware by Broadcom. [Accessed: 22 June 2024]. Available at: https://core.vmware.com/esxiargs-questions-answers#introduction
2. Stop Ransomware (2023). #StopRansomware Guide [Online] Cybersecurity and Infrastructure Security Agency CISA [Accessed: 22 June 2024]. Available at: https://www.cisa.gov/stopransomware/ransomware-guide

Dracarys

1. Tomas Meskauskas (2023). Dracarys Malware (Android). Malware Removal Instructions (Updated). [Online] PCrisk [Accessed: 22 June 2024]. Available at: https://www.pcrisk.com/removal-guides/24569-dracarys-malware-android

2. Monika Grigutytė (2023). 11 signs you have malware and what to do about it. [Online] NordVPN. [Accessed: 22 June 2024] Available at: https://nordvpn.com/blog/signs-of-malware/

Laplas Clipper

1. Anna Gilbertson and Hanah Darley (2023). Defending Against Crypto Thieves with DETECT + RESPOND. [Online] DarkTrace [Accessed: 22 June 2024] Available at: https://darktrace.com/blog/laplas-clipper-defending-against-crypto-currency-thieves-with-detect-respond
2. NordVPN (2024). Laplas Clipper malware threat description. [Online] NordVPN [Accessed: 22 June 2024] Available at: https://nordvpn.com/cybersecurity/threat-center/laplas-clipper/
3. Tom Blackstone and Gabe Turner (2024). 2024 Guide: Everything You Should Know to Invest in Crypto Safely [Online] Security [Accessed: 22 June 2024] Available at: https://www.security.org/digital-security/crypto/