CM2025 Computer Security: Midterm Coursework June 2024

student #: 230668566

Table of Contents

PART A: Carry out research to list 5 recently published new malware

Here are the five recently emerged malwares:

1) “SUBMARINE” Backdoor

Overview of Malware

Submarine is a variant of backdoor that first emerged in October 2022, where it exploits the zero-day bug in ESG devices, which allows for remote command injection. *(TheHackerNews, Jul 29, 2023)*

This backdoor operates with root privileges and is designed to maintain persistence by embedding itself within the system's SQL database, using a combination of SQL triggers, shell scripts, and a loaded library for a Linux daemon that together enable execution with root privileges, persistence, command and control, and cleanup. *(CISA, September 07, 2023)*

This backdoor obtained associated Multipurpose Internet Mail Extensions (MIME) attachment files from the victim. These files contained the contents of the compromised SQL database, which included sensitive information.

Prevention & Mitigation

There are various methods to prevent one’s system from being compromised by this form of malware:

Keeping Softwares and OS up-to-date

Firstly, **to keep all softwares up-to-date** – particularly the OS, updating as frequently as possible to avail the system and making for hackers or threat actors harder to exploit known vulnerabilities.

Conduct Regular Audits

Secondly, **conduct regular security audits and vulnerability assessments** to identify and mitigate potential security risks. Continuous monitoring of network traffic and system logs can help in early detection of backdoor activities.

Install Security Applications

Lastly, **Install enterprise-level security applications** – firewalls, active and passive system scanning and other anti-malware tools.

There are also several ways to mitigate and cope with such infection:

Isolate Compromised Systems

Firstly, we could do so by isolating the infected system from the rest of the local or home network to prevent further spread of the backdoor and limit damage. *(CISA)*

Use Reputable Anti-Malware Tools

Secondly, use reputable anti-malware tools to scan and remove the backdoor from the infected system.

2) Agenda Ransomware

Overview of Malware

Agenda was first detected in July 2022, targeting large enterprises and high-value targets.

Agenda ransomware targets its victims through phishing and spear phishing emails. They are also known to leverage exposed applications and interfaces such as Citrix and remote desktop protocol (RDP).

Agenda also able to scan or exclude certain file paths, propagating to remote machines via PsExec, precisely timing out when the payload is executed and changes the root password on all ESXi hosts, thereby locking out their owners, then uses Secure Shell (SSH) to upload the malicious payload.

Prevention & Mitigation

Enable multi-factor authentication

Organisations should enable multi-factor authentication (MFA) for all user accounts, to provide an additional layer of security. This can be done through the use of mobile apps, such as Google Authenticator or Microsoft Authenticator, or the use of physical tokens or smart cards.

Patch and Update Management

Maintain a disciplined process for applying security patches and updates to all systems and ensure all softwares is up-to-date.

Access Control and Privilege Management

Implement the principle of least privilege, only granting users the minimum access required.

User Awareness and Training

Educate employees on ransomware threats and proper security practices and train users to identify phishing attempts and other social engineering tactics used to deliver ransomware.

Implement backup and disaster recovery

Organisations should implement regular backup and disaster recovery (BDR) processes, to ensure that they can recover from ransomware attacks or other disasters. This includes creating regular backups of all data and systems and storing these backups in a secure, offsite location. The backups should be tested regularly to ensure that they are working and that they can be restored quickly and easily.

Prevent Payment of Ransom

Do not pay the ransom, as this does not guarantee the return of encrypted files and may encourage further attacks.

3) Atomic Stealer Trojan

Overview of Malware

This malware first emerged during mid of 2023, targeting the macOS users.

The malware takes the form of an unsigned disk image file (Setup.dmg) that, when executed, urges the victim to enter their system password on a bogus prompt to escalate privileges and carry out its malicious activities.

Atomic Stealer targets and collects various types of sensitive information from infected systems. This can include login credentials, banking information, cryptocurrency wallets, and other personal data.

The malware is distributed via software cracks and game cheats, targeting users who may be looking to circumvent licensing or copy protection, and may bypass antivirus and anti-malware solutions. (Proofpoint)

Prevention & Mitigation

Firewall Configuration:

Deploy and properly configure firewalls to block malicious traffic and unauthorised access attempts.

Strong Password Policies

Enforce the use of complex, unique passwords for all accounts.

Multi-Factor Authentication

Require multi-factor authentication to add an extra layer of security, particularly for sensitive accounts.

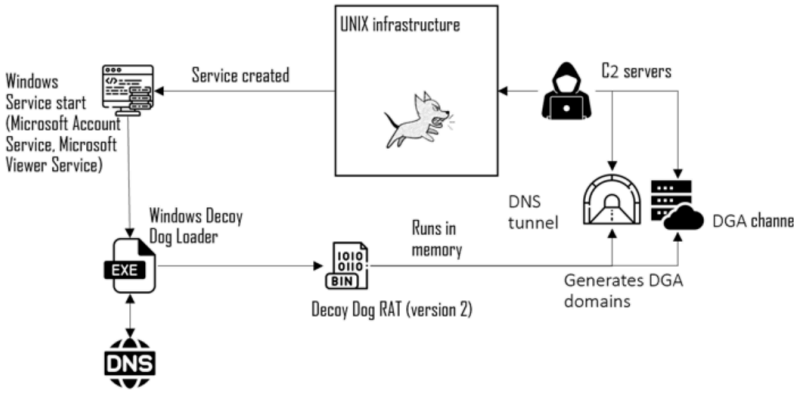
Stay vigilant against social engineering

Be cautious of unexpected requests for system passwords or personal information, especially from unverified sources. Cybercriminals often employ social engineering techniques to trick users into divulging sensitive data.

Avoid Downloading Untrusted Software

Only download software and files from trusted sources. Be wary of unofficial websites, suspicious email attachments, and peer-to-peer networks.

4) “Decoy Dog” Windows Trojan



Overview of Malware

Decoy Dog is a type of Trojan that first **emerged in early April 2022**, targeting enterprise networks. *(The Hacker News, July 2023)*

Decoy Dog makes use of the domain name system (DNS) to perform command-and-control (C2). An endpoint that's compromised by the malware communicates with, and receives instructions from, a controller (i.e., a server) via DNS queries and IP address responses to perform a variety of malicious activities, such as, exfiltrating sensitive data from the infected system, downloading and executing additional payloads, establishing remote access and control over the compromised endpoint and spreading the malware to other systems within the network. It is delivered via a Microsoft Office document that contains a malicious macro.

Decoy Dog's use of DNS for C2 communications makes it challenging to detect and can bypass certain security controls that may be focused on monitoring more traditional network traffic patterns.

This usage of DNS allows the threat actors to issue instructions, maintain communication with compromised machines, and perpetuate their presence undetected over extended periods.

Prevention & Mitigation

Firewall Configuration:

Deploy and properly configure firewalls to block malicious traffic and unauthorised access attempts.

User Awareness and Training

Educate employees on ransomware threats and proper security practices and train users to identify phishing attempts and other social engineering tactics used to deliver ransomware.

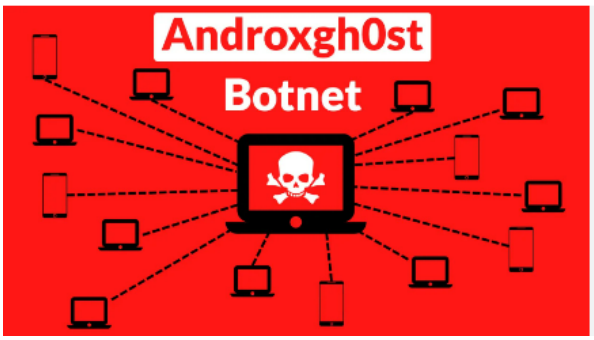
Quarantine Infected Devices

Quarantine affected devices, preventing the spread to other systems by using security softwares.

Run Anti-Virus Software

Running a full system scan with up-to-date antivirus software to detect and remove the malware.

5) Androxgh0st BotNet



Overview of Malware

Androxgh0st is a botnet that emerged during December 2022 which targets mainly Laravel applications and exploits known security flaws in Apache HTTP Server, Laravel Framework, and PHPUnit to gain initial access and for privilege escalation and persistence.

It is designed to exfiltrate sensitive data from various sources, including .env files, databases, and cloud credentials for use in spam or crypto-mining.

Androxgh0st malware also supports numerous functions capable of abusing the Simple Mail Transfer Protocol (SMTP), such as scanning and exploiting exposed credentials and application programming interfaces (APIs), and web shell deployment.

Androxgh0st also has the ability to self-replicate by using compromised AWS credentials to create new users and instances. Unusual web requests to specific server locations may be indicative of an Androxgh0st infection.

Prevention & Mitigation

There is several ways of prevention & Mitigation measures to prevent the malware:

- Verify that the **default configuration for all URIs** is to deny access unless there is a specific need for it to be accessible from the internet.

- Ensure Laravel applications **are not configured to run in debug or testing mode** because it might allow attackers to exploit weaknesses more easily.

- **Review outgoing GET requests** to file hosting platforms (e.g., GitHub and Pastebin), particularly when the request accesses a .php file.

- Keep all operating systems, software and firmware up to date.

Works Cited for Part A

Wikipedia, Ransomware. Accessed on 4th June 2024.

https://en.wikipedia.org/wiki/Ransomware

CISA: New Submarine malware found on hacked Barracuda ESG appliances. Sergiu Gatlan,July 28, 2023.

https://www.bleepingcomputer.com/news/security/cisa-new-submarine-malware-found-on-hacked-barracuda-esg-appliances/#:~:text=A%20suspected%20pro%2DChina%20hacker,since%20at%20least%20October%202022.

CISA Releases Malware Analysis Reports on Barracuda Backdoors, Sep. 07.2023

https://www.cisa.gov/news-events/alerts/2023/07/28/cisa-releases-malware-analysis-reports-barracuda-backdoors

Veeam Ransomware Protection Guide, August 2022

https://www.veeam.com/wp-ransomware-protection-guide.html

CISA Guidance on Patching for Prevention of Ransomware Attacks

https://www.cisa.gov/uscert/ncas/tips/ST15-002

CIS Critical Security Controls

https://www.cisecurity.org/controls/cis-controls-list

Decoy Dog: New Breed of Malware Posing Serious Threats to Enterprise Networks (Jul 26, 2023)

https://thehackernews.com/2023/07/decoy-dog-new-breed-of-malware-posing.html

Agenda (Qilin) Ransomware: In-Depth Analysis, Detection, and Mitigation (Accessed June 9, 2024)

https://www.sentinelone.com/anthology/agenda-qilin/

Breaking down Atomic MacOS Stealer (AMOS), Mar 5, 2024

https://medium.com/@dineshdevadoss04/breaking-down-atomic-macos-stealer-amos-8cd5eea56024#:~:text=The%20Atomic%20MacOS%20Stealer%20(AMOS,in%20the%20below%20malware's%20advertisement.

How to Get Rid of Atomic Stealer Mac Malware (July 18, 2023)

https://news.trendmicro.com/2023/07/18/get-rid-of-atomic-stealer-mac-malware/

Worldwide Agenda Ransomware Wave Targets VMware ESXi Servers

https://www.darkreading.com/cloud-security/agenda-ransomware-vmware-esxi-servers

Androxgh0st, The PolySwarm Blog by The Hivemind

https://blog.polyswarm.io/androxgh0st