Computer Security Midterms Coursework Part A:

The first malware that I researched on is a ransomware called BlackSuit Ransomware. It is an evolved version of a previously known ransomware called Royal ransomware, which was active from September 2022 to June 2023 (CISA, 2024). BlackSuit ransomware conducts data exfiltration and extortion prior to the encryption process, and if the ransom is not paid, the victims' data will be published on a leaked site.

The attackers start by gaining initial access to the victim's networks through means such as phishing or Remote Desktop Protocol (CISA, 2024). Afterwards, they utilise programs like SoftPerfectNetworx to map out the victim's network (CISA, 2024). They then employ tools like Mimikatz, Nirsoft's password stealing software, and GMER to disable specific system processes such as the antivirus software (CISA, 2024). Legitimate cybersecurity tools and malware like Cobalt Strike and Ursnif/Gozi are used to steal victims' data (CISA, 2024).

Moving on to the encryption process. Firstly, they use windows restart manager to check whether the targeted files are currently in use or blocked before deleting all backup copies with the Windows Volume Shadow Copy service (CISA, 2024). Next, they send out .bat files in encrypted 7zip files to execute their attack (CISA, 2024). These files will proceed to create a new admin user to gain full control, force system updates to group policies while allowing the ransomware to run, and delete system settings, event logs and the files once the encryption is done.

The FBI and CISA have provided a list of mitigation strategies against this threat (CISA, 2024). This involves ensuring that all operating systems, software, and firmware are up-to-date, and that administrator accounts have multifactor authentication that are phishing resistant. If your device is infected with BlackSuit, they advise against paying the ransom and to instead report the issue to the appropriate authorities, such as the FBI's Internet Crime Complain Centre.

The second malware I looked up is another ransomware called BianLian ransomware. Named after its developer who is part of a data extortion cybercriminal group, they started in June 2022 and focuses on encrypting the victims' systems and stealing financial, customer, corporate, technical and personal files for leverage (CISA, 2024).

They start by utilizing compromised Remote Desktop Protocol(RDP) credentials that were likely obtained through phishing or initial access brokers to obtain initial access to the victims' networks (CISA, 2024). They disabled the antivirus protections and modified security settings using PowerShell and Windows command shell, added in custom backdoors and installed remote management and access software for control and persistence purposes, created and altered administrators accounts, concealed their traffic using either Ngrok or Rsocks, and exploited vulnerabilities like CVE-2022-37969 to gain more privileges (CISA, 2024). BianLian actors have also employed various means for learning about the victims' environment such as using tools like Advanced Port Scanner and Ping Castle to map out networks, discover user accounts and identify accessible devices (CISA, 2024). The victim's credentials are harvested from local machines, LSASS memory and Active Directory databases using programs like Impacket and Session Gopher (CISA, 2024). They utilized methods such as PsExec to connect to the other network accessible devices, created admin accounts to modify firewall rules, and installed Webshells, giving them remote system control and network access (CISA, 2024). Lastly, malware and scripts are used to collect registry values, files, clipboard data and encrypt the stolen data (CISA, 2024).

In terms of prevention, the FBI, CISA, and ASD'S ACSC have provided a list of mitigations (CISA, 2024). Some suggestions include auditing the network's remote access to identify currently using or authorized software and granting just specific users with access to the PowerShell. Upon infection, they have advised against paying the ransom and to instead report it to the local authorities.

The third malware I will be discussing is a variant of a Trojan called “Remcos remote access Trojan (RAT). Despite being around since 2016, recently in the third quarter of 2024, two distinct variants of Remcos Rat have been identified (Mascellino, 2024).

I will be focusing on its second variant which centres around spreading through spam emails with malicious Microsoft Office Open XML (DOCX) attachments (Jaiswal and M, 2024). These files exploit a remote code execution vulnerability called “CVE-2017-11882” to run hidden scripts that downloads more malware, eventually deploying the Remcos RAT (Jaiswal and M, 2024).

Once installed, it connects to a Command-and-Control server and gives instructions to the malware (Mascellino, 2024). These instructions involve collecting various sensitive information such as capturing keystrokes and are encrypted even when sent back to the attackers (Mascellino, 2024). Once active, Remcos uses a process called “process hollowing” where it hijacks a legitimate program like dllhost.exe and replace its code with malicious instructions (Mascellino, 2024). It hides itself using various anti-analysis techniques such as having vectored exception handlers consisting of special code paths which are designed to confuse security tools (Mascellino, 2024). These various tactics allows it to blend in seamlessly with the system while hiding its tools. Remcos also adds itself to the windows registry so that it automatically runs whenever the device restarts (Mascellino, 2024).

McAfee Labs has provided some indicators of compromise for handling these variants. This includes having up-to-date systems, patching known vulnerabilities and employing intrusion prevention system and content disarm tools (Mascellino, 2024). In the case of an infected device, it is recommended to use a reputable anti-malware software such as Combo Cleaner to detect and remove the Remcos RAT (Meskauskas, 2024).

The fourth malware I looked at is a type of infostealer known as “Lumma Information Stealer”. It primarily targets cryptocurrency wallets and browser extensions with aims of stealing information such as their wallet data, browser cookies, credit card details, connection history and two-factor authentication information (CSA Singapore, 2023). It is also capable of a technique known as cryptojacking where attackers hijack a victim’s computer to mine cryptocurrency for themselves (Lin, 2024).

Despite being active since August 2022, the first prominent case that I could uncover comes from 2023 when FortiGuard Labs researchers discovered a malicious YouTube campaign conducted by cybercriminals (Lin, 2024). They were using popular YouTube channels to advertise pirated software and tricking viewers into clicking on a link that will download a hidden malware loader which installs the Lumma Stealer malware (Lin, 2024). It also likes to spread through other means such as phishing (CSA Singapore, 2023).

An example of how Lumma Stealer steals data comes from this particular case. Here, it has an accomplice malware called “Clipper” which is designed to modify the clipboard such that when attempting to copy a wallet address, it is replaced with the attacker’s address instead (Mohanasundaram and Neil Tyagi, 2024). The Lumma Stealer then extracts and exfiltrates important data such as the copied wallet address to a command-and-control server where it communicates with the attacker’s server using obfuscated methods (Mohanasundaram and Neil Tyagi, 2024).

In terms of defence, the Cyber Security Agency of Singapore (CSA) have provided a list of suggestions to individuals and organisations. This includes disabling all ports and protocols that are inessential for business operations and employing an EDR Solution at end-users’ devices for continuous monitoring, detecting and responding of cyber threats (CSA Singapore, 2023). When infected, it is also recommended to a reliable and strong antivirus software to locate and remove the malware (Meskauskas, 2024).

The final malware I looked up on is a type of botnet called “BADBOX Botnet”. It was first discovered by researcher Daniel Milisic in April 2023 who noticed that the Android TV box he bought was engaging in unusual communications with unidentified websites (Falé, 2024).

BADBOX is a cybercriminal operation that involves selling off-brand Androd electronics with preinstalled malware with a recent discovery of over 192,000 infected devices (Falé, 2024). These devices are tampered with either during the supply chain or sold by manufacturers capable of installing APKs without the users’ authorisation (Falé, 2024). They are then sold through reputable retailers, such as Amazon making it difficult for consumers to detect the danger (Falé, 2024). BADBOX uses devices for purposes such as remote code installation, account abuse, ad fraud, and residential proxy (Falé, 2024).

Moving on to how BADBOX operates. The infected device’s firmware has been compromised such that when it starts up, the malware’s process begins (Falé, 2024). It immediately connects to a hidden backdoor, allowing it to install additional malicious programs without the user’s consent (Falé, 2024). It then runs a maliciously modified vital system library called “libanroid_runtime”. A malicious application called “Stager APK” is then decrypted and activated by BADBOX to start working (Falé, 2024). It connects to a Command-and-Control server to receive instructions and transmits the device’s data to endpoints like “/aplinfo” (Falé, 2024). After downloading all available malicious payloads from a designated site, they are converted into executable files through decryption (Falé, 2024). They are then loaded into the system launcher, enabling them to carry out harmful tasks such as running the attacker’s additional commands (Falé, 2024). As the malware comes preinstalled, only a few precautions can be taken such as choosing your trusted vendors wisely (Falé, 2024). Look out for indicators such as overheating, and performance issues due to excessive CPU consumption (Toulas, 2024). Make sure that their firmware security is to up-to-date, separate smart devices from more critical systems and disconnect them from the internet when not in use (Toulas, 2024). The latter is especially crucial for when your device lacks firmware or security updates.

References

Cyber Security Agency of Singapore. (2023, October 13). *Defending Against Lumma Information Stealer Malware*. CSA. https://www.csa.gov.sg/alerts-advisories/Advisories/2023/ad-2023-017

Cybersecurity and Infrastructure Security Agency. (2024, August 27). *#StopRansomware: Blacksuit (Royal) Ransomware.* CISA. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-061a

Cybersecurity and Infrastructure Security Agency. (2024, November 20). *#StopRansomware: Bianlian Ransomware Group.* CISA. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-136a

Falé, P. (2024, December 17). *BADBOX Botnet is back*. Bitsight. https://www.bitsight.com/blog/badbox-botnet-back

Jaiswal, S., & M, A. (2024, December 11). *The stealthy stalker: Remcos RAT*. McAfee. https://www.mcafee.com/blogs/other-blogs/mcafee-labs/the-stealthy-stalker-remcos-rat/

Lin, C. (2024, January 8). *Deceptive cracked software spreads LUMMA variant on YouTube: FortiGuard Labs*. Fortinet. https://www.fortinet.com/blog/threat-research/lumma-variant-on-youtube

Mascellino, A. (2024, November 11). *New Remcos RAT variant targets windows users Via Phishing*. Infosecurity Magazine. https://www.infosecurity-magazine.com/news/remcos-rat-variant-targets-windows/

Mascellino, A. (2024, December 12). *Remcos RAT malware evolves with new techniques*. Infosecurity Magazine. https://www.infosecurity-magazine.com/news/remcos-rat-malware-evolves-new/

Meskauskas, T. (2024, November 18). *How to remove Remcos RAT from the operating system*. PCrisk. https://www.pcrisk.com/removal-guides/14048-remcos-rat-virus

Meskauskas, T. (2024, December 17). *Removal instructions for the Lumma stealer-type malware*. PCrisk. https://www.pcrisk.com/removal-guides/24616-lumma-stealer

Mohanasundaram, M., & Tyagi, N. (2024, November 20). *Lumma Stealer on the rise: How telegram channels are fueling malware proliferation*. McAfee. https://www.mcafee.com/blogs/other-blogs/mcafee-labs/lumma-stealer-on-the-rise-how-telegram-channels-are-fueling-malware-proliferation/

Toulas, B. (2024, December 19). *BadBox malware botnet infects 192,000 Android devices despite disruption*. BleepingComputer. https://www.bleepingcomputer.com/news/security/badbox-malware-botnet-infects-192-000-android-devices-despite-disruption/