CM2025 Computer Security: Midterm Coursework

SOH YI JIE GABRIEL – (220516695)

UNIVERSITY
OF LONDON

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

1.

The Black Basta malware is ransomware, first reported in April 2022. In such an attack, the perpetrators encrypt the victim's data, delete backup files, and then demand money in exchange for the decryption key [1]. This extortion method leaves victims without access to their critical data unless they pay the ransom, hence the name "ransomware." Affiliates of Black Basta have breached over 500 organizations globally, targeting critical infrastructure sectors including healthcare [2]. These attacks disrupt operations and jeopardize sensitive information, underlining the importance of the mitigations recommended by federal agencies to defend against such sophisticated threats [3].

Individuals and organizations can take security precautions such as regularly updating operating systems, software, and firmware to fix any vulnerabilities, minimizing the risk of exploitation [4]. Utilizing phishing-resistant Multi-Factor Authentication (MFA) for various services adds an extra layer of protection against unauthorized access attempts. Educating users to identify and report phishing attempts can help prevent initial ransomware infiltration [5]. Employing CISA-recommended security measures for remote access software strengthens defenses against common ransomware entry points. Regularly backing up critical system data offline or in secure cloud storage can mitigate the impact of an attack.

If your system is infected with Black Basta ransomware, take immediate action by disconnecting affected systems from the network to halt the malware's spread. Contact relevant authorities like the FBI or CISA and seek help from cybersecurity professionals. Refrain from paying the ransom, as this doesn't guarantee data retrieval and may incentivize further criminal activity. Instead, if you have backups, use them to restore data after thoroughly cleaning the system before reconnecting to the network. If backups aren't available, consult with cybersecurity experts to explore decryption tools or alternative recovery options. Additionally, conduct a comprehensive investigation to identify the attack's method and bolster security measures to prevent future incidents.

2.

The CatDDoS malware is a botnet, first reported in August 2023. A botnet is a network of infected computers, or "bots," controlled by an attacker without the users' knowledge. The term "bot" comes from "robot," referring to the compromised machine, while "net" represents the interconnected devices forming a zombie army [6]. In the article, the CatDDoS botnet exploits over 80 vulnerabilities to enlist devices into its network. Compromised devices take commands from a central Command and Control (CNC) server, directing various malicious activities, including distributed denial-of-service (DDoS) attacks. In a DDoS attack, the targeted website or service is flooded with excessive traffic, overwhelming its servers and rendering it inaccessible to legitimate users. DNSBomb, mentioned in the article, enhances such attacks by exploiting DNS queries and responses, highlighting the destructive potential of botnets in the digital realm [7].

To protect against the CatDDoS malware and similar threats, updating software regularly is vital. This includes routers, networking gear, and devices from vendors mentioned in the article to minimize vulnerability exploitation [8]. Employing reputable antivirus software, enabling firewalls, and practicing strong cybersecurity measures, like using unique passwords and multi-factor authentication, can further enhance defense against malware infiltration [9]. Caution is also advised when interacting with unfamiliar links or downloads to prevent malware installation.

If infected, swift action is crucial. Disconnecting the affected device from the internet can halt its participation in malicious activities. Conducting a comprehensive antivirus scan is essential to detect and remove the malware, with some software offering specialized tools for botnet-related threats. Restoring the device to a previous backup point may effectively eliminate the malware. If backups are unavailable or the infection persists, seeking assistance from cybersecurity professionals or support forums is recommended for tailored solutions and guidance.

3.

A worm is the P2PInfect malware. The incident, first reported on July 11, 2023, spreads via networks on its own and doesn't require attachment to software that already exists because of special capacity for self-replication [10]. In contrast to viruses, worms function autonomously, taking advantage of weaknesses in systems or protocols within networks to infiltrate and spread. The durability and flexibility of contemporary worms, such as P2PInfect, demonstrate their sophistication. They were created in Rust and leverage techniques like SSH abuse and Redis vulnerabilities to spread throughout other platforms [11]. Their progression, observed in strains aimed at novel architectures such as ARM, illustrates the continuous ingenuity of malevolent entities. These worms are very difficult to detect because they use self-defense mechanisms including process protection and particular packer versions [12].

Use a proactive protection strategy to protect your system against P2PInfect. To block possible virus entry points, keep all software updated [13]. Use multi-factor authentication or strong passwords to improve authentication, particularly with SSH. Install the most recent version of antivirus software to find and eliminate P2PInfect, and use intrusion detection systems to watch network traffic for indications of worm activity [14]. Disabling unused services and ports and configuring firewalls to regulate traffic flow can help reduce attack surfaces.

In order to reduce the effects of a P2PInfect infection, quick action is essential. Quarantine impacted devices to contain the infection and isolate compromised systems to stop its spread. Utilize antivirus software to find and remove the harmful code, making sure to follow the right protocols for removal or quarantine. To recover data and restore system integrity, restore affected systems from clean backups made before the infection. To stop infections in the future, strengthen security measures by installing the required patches and updates. Pay attention for indications of persistence or re-infection in affected systems.

4.

First discovered in June 2023, the trojan known as GoldDigger targets users' devices by pretending to be reputable organizations such as local businesses or government websites. It spreads by luring users into downloading malicious Android applications through phony websites that impersonate reliable sources like Google Play pages or corporate websites in Vietnam [15]. GoldDigger requires users to enable Accessibility Service after installation in order to fully monitor user activity, capture private data such as banking credentials, and exfiltrate information to command-and-control servers. With increased rights, GoldDigger can operate invisibly and carry out its fraudulent schemes—intercepting SMS messages, collecting credentials, and mimicking user interactions—effectively [16].

In order to defend against the GoldDigger malware, users must download apps only from reputable stores, such as the official Google Play Store, and not use their devices' "Install from Unknown Sources" feature. This preventive measure helps prevent the installation of malicious apps that pose as legitimate ones. It is recommended that users update their devices and applications on a regular basis to fix any security flaws that could be exploited by malicious malware like GoldDigger. Using a reliable mobile security solution or antivirus software improves the capacity to recognize and remove viruses from devices [17].

In order to stop data from being sent to distant command-and-control servers, owners of a compromised device infected with the GoldDigger malware must disconnect it from the internet. Use reliable antivirus or anti-malware software to get rid of the malware. To stop unwanted access, must reset compromised passwords and accounts, especially those linked to sensitive or bank information. The infection will be completely eliminated if the device is returned to its original factory settings. Users should also be alert for any strange activity on their accounts. Contact cybersecurity experts for help or by reporting the occurrence to the appropriate authorities.

5.

Spyware is what the CloudMensis malware is. The first occurrence, which was originally documented in April 2022, operates by surreptitiously obtaining private data from the target device or user. This involves secretly gathered data such as papers, keystrokes, and screen shots from victims without their knowledge. After being taken, the data is sent back to the virus developers, who frequently communicate with one another over open cloud storage facilities [18]. The information benefits the assailants by maybe aiding in business espionage, identity theft, and other criminal endeavors. Such information might also end up on dark web orunderground marketplaces, where it might be sold to other purchasers for criminal uses [19].

Initially, ensure that the operating system and all installed applications are updated with the most recent security patches regularly. Frequently, these updates include fixes for well-known flaws that malware takes advantage of. Malware infestations can be avoided by using caution when internet browsing, avoiding clicking on dubious links, and not downloading anything from unreliable sources. The system's defenses can be further strengthened by turning on built-in security features like firewalls and anti-phishing measures and installing reliable antivirus software [20]. Protect against unwanted access by creating strong, unique passwords for each account and, use two-factor authentication.

In order to stop the propagation of malware like CloudMensis, disconnect compromised PC from internet and other devices when you notice any symptoms. Use most recent version of your antivirus program to do a complete system scan in order to find and remove malicious files. Use specialized eradication tools or consult cybersecurity professionals if the malware continues to persist. Eliminating leftover malware traces can be achieved by restoring system from a clean backup made before to the infection. Finally, strengthen system security and maintain vigilance against potential threats by regularly monitoring and educating yourself on cybersecurity best practices.

References

1. Gatlan, S. (2024). CISA: Black Basta ransomware breached over 500 orgs worldwide. [online] Bleeping Computer. Available at: https://www.bleepingcomputer.com/news/security/cisa-black-basta-ransomware-breached-over-500-orgs-worldwide/ (Accessed: 2 July 2024).
2. Arghire, I. (2024). Black Basta Ransomware Hit Over 500 Organizations. [online] SecurityWeek. Available at: https://www.securityweek.com/black-basta-ransomware-hit-over-500-organizations/ (Accessed: 2 July 2024).
3. HHS (2023). Black Basta Threat Profile. [online] HHS.gov. Available at: https://www.hhs.gov/sites/default/files/black-basta-threat-profile.pdf (Accessed: 2 July 2024).
4. Toulas, B. (2024). Black Basta ransomware gang linked to Windows zero-day attacks. [online] Bleeping Computer. Available at: https://www.bleepingcomputer.com/news/security/black-basta-ransomware-gang-linked-to-windows-zero-day-attacks/ (Accessed: 2 July 2024).
5. Fox, A. (2024). Ascension confirms data breached in Black Basta ransomware attack. [online] Healthcare IT News. Available at: https://www.healthcareitnews.com/news/ascension-confirms-data-breached-black-basta-ransomware-attack (Accessed: 2 July 2024).
6. CyberMaterial (2024). CatDDoS Botnet Exploits 80+ Security Flaws. [online] CyberMaterial. Available at: https://cybermaterial.com/catddos-botnet-exploits-80-security-flaws/ (Accessed: 2 July 2024).
7. Wainwright, H. (2024). What Are CatDDoS Botnet and DNSBomb DDoS Attacks? [online] hide.me. Available at: https://hide.me/en/blog/what-are-catddos-botnet-and-dnsbomb-ddos-attacks/ (Accessed: 2 July 2024).
8. SC Media (2024). CatDDoS botnet attacks surge, DNSBomb DDoS attack technique emerges. [online] SC Media. Available at: https://www.scmagazine.com/brief/catddos-botnet-attacks-surge-dnsbomb-ddos-attack-technique-emerges (Accessed: 2 July 2024).
9. The Hacker News (2024). Researchers Warn of CatDDoS Botnet and DNSBomb DDoS Attack. [online] The Hacker News. Available at: https://thehackernews.com/2024/05/researchers-warn-of-catddos-botnet-and.html (Accessed: 2 July 2024).
10. Toulas, B. (2023). P2PInfect botnet activity surges 600x with stealthier malware variants. [online] BleepingComputer. Available at: https://www.bleepingcomputer.com/news/security/p2pinfect-botnet-

activity-surges-600x-with-stealthier-malware-variants/ (Accessed: 2 July 2024).

11. Arghire, I. (2024). P2Pinfect Worm Now Dropping Ransomware on Redis Servers. [online] SecurityWeek. Available at: https://www.securityweek.com/p2pinfect-worm-now-dropping-ransomware-on-redis-servers/ (Accessed: 2 July 2024).
12. Pell, A. (2023). P2PInfect Botnet Activity Surges 600x with Stealthier Malware Variants. [online] LinuxSecurity. Available at: https://www.linuxsecurity.com/news/hackscracks/p2pinfect-botnet-activity-surges-600x-with-stealthier-malware-variants (Accessed: 2 July 2024).
13. SC Media (2024). P2PInfect botnet attacks surge, DNSBomb DDoS attack technique emerges. [online] SC Media. Available at: https://www.scmagazine.com/brief/catddos-botnet-attacks-surge-dnsbomb-ddos-attack-technique-emerges (Accessed: 2 July 2024).
14. Nozomi Networks (2024). P2PInfect Worm Evolves to Target a New Platform. [online] Nozomi Networks. Available at: https://www.nozominetworks.com/blog/p2pinfect-worm-evolves-to-target-a-new-platform (Accessed: 2 July 2024).
15. Muncaster, P. (2023). GoldDigger Android Trojan Drains Victim Bank Accounts. [online] Infosecurity Magazine. Available at: https://www.infosecurity-magazine.com/news/golddigger-android-trojan-drains/ (Accessed: 2 July 2024).
16. Cyber Affairs (2023). GoldDigger Android Trojan Targets Banking Apps in Asia Pacific Countries. [online] Cyber Affairs. Available at: https://www.cyberaffairs.com/2023/10/golddigger-android-trojan-targets-banking-apps/ (Accessed: 2 July 2024).
17. Group-IB (2023). GoldDigger Trojan targets Vietnamese users with fake Google Play Store pages. [online] Group-IB. Available at: https://www.group-ib.com/media-center/press-releases/golddigger-trojan-vietnam/ (Accessed: 2 July 2024).
18. M.Léveillé, M.-E. (2022). I see what you did there: A look at the CloudMensis macOS spyware. [online] WeLiveSecurity. Available at: https://www.welivesecurity.com/2022/07/19/i-see-what-you-did-there-look-cloudmensis-macos-spyware/ (Accessed: 2 July 2024).
19. Gatlin, S. (2022). New CloudMensis malware backdoors Macs to steal victims' data. [online] Bleeping Computer. Available at: https://www.bleepingcomputer.com/news/security/new-cloudmensis-malware-backdoors-macs-to-steal-victims-data (Accessed: 2 July 2024).
20. Hive Pro Threat Advisory (2022). CloudMensis Spyware Actively Targets Apple macOS Users. [online] Hive Pro. Available at:

https://www.hivepro.com/threat-advisory/cloudmensis-spyware-actively-targets-apple-macos-users/ (Accessed: 2 July 2024).