CM2025: Computer Security

Midterm Assignment Part 1

Arjun Muralidharan

4th July 2021

Contents

1 Airport Security **3**

1.1 Distributed Denial of Service Attack (DDoS) . . . 3

1.1.1 Threat Assessment . . . 3

1.1.2 Mitigation Strategy . . . 3

1.2 Tampering with Self-Service Check-In Terminals . . . 3

1.2.1 Threat Assessment . . . 3

1.2.2 Mitigation Strategy . . . 4

1.3 REvil Targeted Ransomware . . . 4

1.3.1 Threat Assessment . . . 4

1.3.2 Mitigation Strategy . . . 5

1 Airport Security

1.1 Distributed Denial of Service Attack (DDoS)

1.1.1 Threat Assessment

Airports are becoming more reliant on the Internet of Things (IoT) to connect devices and provide data to services. These devices include biometric screening, scanners and printers as well as cellphones. Bad actors have a large attack surface because these devices depend on the airport's internet network. Security cameras and other devices are visible to the public, making them vulnerable to attackers.

There are many ways that this vast attack surface could be exploited. One possible way is to attack a network hub, reducing its operational capability, by using the huge number of devices connected, also known as a DoS attack, done by overwhelming a target with traffic and forcing it to crash.

Mirai is an example of such a famous botnet [1]. It scans IoT devices for potential weaknesses, and then issues commands from a host to further flood systems with requests. This could cause airport security problems such as delays, cancellations or interruptions to flights, a lack of communication, or air traffic control. For example, in 2015, 1400 passengers were affected by DDoS attacks on a Polish airport [2].

1.1.2 Mitigation Strategy

Hardening the entry points to our connected devices is the first step in protecting against DDoS attacks. For the best protection against DDoS attacks, it is important to close all ports and keep firmware current. Additionally, it is crucial that all devices are wired securely and use wireless protocols like WPA whenever possible. Also, it is important to keep services on different networks as possible. A VPN could be used to connect security cameras to the appropriate endpoint [3].

The best defense against a DDoS is not only to secure entry points but also to configure an Intrusion Detection System to detect unusual activity. This is in accordance with a set of rules. Wood & Stankovic [4] identify several kinds of attacks in a DDoS scenario in sensor networks and suggest mitigation strategies.

Afify et al. [5] highlight the importance IDS and also recommend creating redundant networks, splitting devices into various tiers demanding different security, and, in the event of a DDoS, can switch networks. These strategies combined can prevent malicious actors from gaining access to devices.

1.2 Tampering with Self-Service Check-In Terminals

1.2.1 Threat Assessment

Many airports use self-service terminals to check in and perform other services. It reduces wait times and airport staff requirements. But it can also pose a security threat. An attacker might tamper or

steal identity information. They could also be used to deny service to customers or create arbitrary boarding pass codes. In May 2018, a hacker gained access to one of these terminals in Iran. [6] The arrival and departure displays were modified to show messages criticizing the government. However, any message could be displayed including misinformation or instruction to further a criminal goal.

1.2.2 Mitigation Strategy

This is where security at an airport begins, as the airport has full control over the kiosk system. These services can be operates by airlines, but different airlines might implement different products with varying security. To ensure that only one system needs to be audited and secured, it's better to use an vendor-based product that can be used by all airlines. Additionally, each airport can manage their vendors according to their respective threat vectors and certification standards. It is important to restrict WiFi access and the usage of external disks and drives. To protect sensitive information from being compromised, all data should be encrypted, including customer details. You can monitor the machine's activity to spot irregular patterns using an Intrusion Detection System. We should keep this system separate from any other services in order to prevent attacks such as the Iran attack, where attackers could broadcast messages across the airport.

A further strategy includes ensuring that there is always a presence of physical security personnel observing the people who are checking in with the kiosks. They could be positioned close to the machines, providing assistance for passengers and escalating any dangers.

1.3 REvil Targeted Ransomware

1.3.1 Threat Assessment

According to the Kapersky [7], there is an increase in targeted ransomware attacks, which include "Spear Phishing", emails that contain files and links to illicit sites in an attempt to convince the user to download malicious software. They could also be embedded in sites used by employees. This malware blocks the access to sensitive data and allows attackers to demand ransom payment from victims. Bulletin states that targeted attacks are designed to target victims based upon their financial capability, dependence on encrypted data, and the greater the impact they will have. Ransomware gangs promise not to target hospitals, but no sector is out of reach.

Airports have all these factors: they have valuable data, deep pockets (or their insurances), so any disruption would have a massive impact. This malware has been used to attack airports, as we have seen it. In December 2019, the REvil malware infected Albany County Airport Authority. To recover their data, they paid a ransom. REvil also infected a currency exchange operator that runs several counters at British airports in 2019. To recover their data, they paid more than 2 million Bitcoin [8] [9].

Companies could lose their data, and be at risk of data leaks. The REvil's group already sold the

victim's data to dark web. It is possible that the ransom was not paid and they may continue to sell the victim's data after payment. REvil ransomware allows users to download ZIP files via phishing email. These archives contain a JavaScript file that will launch a shell application that gives itself enhances access rights. The payload will be delivered once all Windows backups are deleted. It will then iterate through each folder, encrypt them, and leave a ransom note in each. To communicate the attack and provide instructions, the desktop background is also altered [10].

1.3.2 Mitigation Strategy

Based on the MITRE ATT&CK [11] framework we can identify aspects of the ransom attack:

1. Initial Access: Spear-phising emails sent out
2. Execution: JavaScript file with obfuscation
3. Privilege Escalation: Scripts executed via Shell
4. Defensive Evasion: Removing any on-system backups
5. Impact: Local disk encryption

These are the areas where we need to improve and harden. It is possible to prevent the first access by blocking certain file types in the email system and upskilling staff on security threats at regular intervals. This will also help build awareness within the organisation. Compressed archives enable attackers to hide contents and evade viruses scanners. Such files can be shared by employees. They can either unpack the contents before sending, or they could use shared network drives which is less accessible to hackers. Training should explain attackers use social engineering, and instruct staff to discard unknown attachments and verifying any hyperlinks they have sent via email. The email service should include a reporting feature that employees can use whenever they suspect something is wrong. While this is the most difficult task, it is also one of the most important. This encourages employees to take responsibility for security and develops their ability to solve problems independently. K. Thomas & J. van Niekerk [12] propose creating a "goal consensus" environment instead of a top-down, rules-based environment for combating information security apathy. A coercive setting is one where management demands that employees act in a certain way. While a utilitarian setting offers rewards for acting in the desired manner, it can be described as one where they threaten the employees with consequences. The goal consensus environment is one where everyone agrees on the values of the organization and actions comport to those values. To ensure the execution and privilege escalate stages, antivirus must be up-todate, firewall properly configured, and operating systems and software up to date [13].

It is possible to fight this vector if we regularly back up Windows and transfer them to a remote location. This is also a good idea for sensitive data. It should be easy for you to restore. We can use a common backup strategy (three-two-one) which includes three copies of data on two media, one of which is offsite. The ransomware threat is greatly reduced when encrypted data can be accessed from

another location and then restored. Cybereason. SpinOne. Cybereason. These software solutions could be used as backups and antivirus.

These steps, taken together, will help us protect ourselves from the REvil ransomware. It will also make us more prepared to combat and recover from other ransomware infections.

References

[1] jgamblin, "jgamblin/mirai-source-code." [Online]. Available: https://github.com/jgamblin/Mirai-Source-Code

[2] A. Kharpal, "Hack attack leaves 1,400 airline passengers grounded," Jun 2015. [Online]. Available: https://www.cnbc.com/2015/06/22/hack-attack-leaves-1400-passengers-of-polish-airline-lot-grounded.html

[3] G. Lykou, A. Anagnostopoulou, and D. Gritzalis, "Smart airport cybersecurity: Threat mitigation and cyber resilience controls," *Sensors*, vol. 19, no. 1, p. 19, 2018.

[4] A. Wood and J. Stankovic, "Denial of service in sensor networks," *Computer*, vol. 35, no. 10, p. 54–62, 2002.

[5] F. M. Afify, H. M. Kelash, O. S. Faragallah, M. S. Tolba, and H. S. El-Sayed, "Protection against denial of service in automation systems," *International Journal of Computer Applications*, vol. 106, no. 18, p. 11–18, 2014.

[6] T. of Israel Staff, "Screens at iran airport said hacked with anti-regime messages," May 2018. [Online]. Available: https://www.timesofisrael.com/screens-at-iran-airport-said-hacked-with-anti-regime-messages/

[7] Kaspersky Lab Global Research & Analysis Team, "Advanced threat predictions for 2021." [Online]. Available: https://securelist.com/apt-predictions-for-2021/99387/

[8] J. Panettieri, "Sodinokibi ransomware attack hits MSP, New York Airport," Jan 2020. [Online]. Available: https://www.msspalert.com/cybersecurity-news/sodinokibi-hits-msp-new-york-airport/

[9] A. Isaac, C. Ostroff, and B. Hope, "Travelex paid hackers multimillion-dollar ransom before hitting new obstacles," Apr 2020. [Online]. Available: https://www.wsj.com/articles/travelex-paid-hackers-multimillion-dollar-ransom-before-hitting-new-obstacles-11586440800

[10] Nocturnus, "Revil/sodinokibi: The crown prince of ransomware." [Online]. Available: https://www.cybereason.com/blog/the-sodinokibi-ransomware-attack

[11] Mitre Corporation. [Online]. Available: https://attack.mitre.org/

[12] K. Thomson and J. V. Niekerk, "Combating information security apathy by encouraging prosocial organisational behaviour," *Information Management & Computer Security*, vol. 20, no. 1, p. 39–46, 2012.

[13] S. Saxena and H. K. Soni, "Strategies for ransomware removal and prevention," *2018 Fourth International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB)*, 2018.