Case Studies in Cyber Security

HyperionDev

Lecture – Housekeeping

- The use of disrespectful language is prohibited in the questions, this is a supportive, learning environment - please engage accordingly.
- No question is daft or silly - **ask them!**
- There are Q/A sessions midway and at the end of the session, should you wish to ask any follow-up questions.
- You can also submit questions here: hyperiondev.com/sbc4-cs-questions
- For all non-academic questions, please submit a query: www.hyperiondev.com/support
- Report a safeguarding incident: hyperiondev.com/safeguardreporting
- We would love your feedback on lectures: https://hyperionde.wufoo.com/forms/zsgv4m40ui4i0g/

Previously:

- Introduced to Burp Suite Functionality and how it could be used to intercept/manipulate HTTP requests

Objectives

Dive into past attacks and for each attack:

- Discuss the consequences
- Explore some key take aways

TARGET STATEMENT ON SECURITY BREACH

"WE TAKE THIS MATTER VERY SERIOUSLY AND ARE WORKING WITH LAW ENFORCEMENT TO BRING THOSE RESPONSIBLE TO JUSTICE."

GREGG STEINHAFEL
TARGET CHAIRMAN,
PRESIDENT AND CEO

https://media2.s-nbcnews.com/i/MSNBC/Components/Video/_NEW/tdy_target_131219.jpg

Target Data Breach (2013)

One of the most prominent cybersecurity incidents in recent memory was the 2013 holiday shopping season Target data breach.

Data Theft and Attackers' Access to the Target's Network

- Through a third-party HVAC contractor with authorized access to Target's systems, the attackers were able to access Target's network.
- It's thought that the attackers gained access to Target's network by compromising the credentials of an HVAC contractor employee using spear-phishing emails.
- Once inside, the intruders made lateral movements throughout the network until they were able to access Target's Point-of-Sale (POS) systems.
- In order to capture and exfiltrate private customer data, including credit card information, they installed malware on the POS systems.

Repercussions

- Target suffered serious repercussions from the breach in terms of its reputation and financial situation.
- Along with the personal data of about 70 million customers, about 40 million credit and debit card numbers belonged to stolen customers.
- Customer trust was lost as a result of the incident, and Target's brand reputation was harmed.
- Due to the breach, Target was the target of numerous lawsuits, investigations, and significant financial costs.
- Over $250 million was estimated to have been spent on the breach overall, including legal settlements, remediation work, and lost revenue.

Lessons To Be learnt

Target's network was improperly segmented, allowing attackers to move laterally and access sensitive systems. Network segmentation can be used to contain attackers inside particular network segments and lessen the impact of a breach.

Threat Detection and Monitoring: The breach went a significant amount of time without being discovered. Implementing effective threat detection tools like intrusion detection systems (IDS) and security monitoring can assist in quickly identifying and responding to security incidents.

Target's incident response plan was not properly developed or carried out, which caused delays in discovering and containing the breach. Companies should create clearly defined incident response plans, test them frequently, and have an organized response strategy in place.

Vendor Risk Management: The breach happened as a result of the credentials of a third-party vendor being compromised. The security risks posed by third-party vendors should be evaluated and managed by organizations, including by putting in place the proper access controls, keeping an eye on their activities, and adhering to security best practices.

WannaCry Ransomware

www.blackfog.com

WannaCry Ransomware (2017)

The global cyberattack caused by the WannaCry ransomware in May 2017 had an effect on organizations from various industries.

Windows Vulnerability Exploitation and Quick Spread:

- The U.S. National Security Agency (NSA) originally created EternalBlue, a vulnerability in the Windows operating system that was used by WannaCry.
- Targeting unpatched or exposed systems, the attackers spread the ransomware worm across networks using the EternalBlue exploit.
- After infecting a system, WannaCry would encrypt the files on the compromised system and demand a Bitcoin ransom to decrypt them.
- WannaCry spread quickly across connected networks and within businesses thanks to its worm-like characteristics.

Repercussions & Catalysts

- Organizations all over the world were significantly impacted by the WannaCry attack, which also had an effect on industries like healthcare, government, finance, transportation, and more.
- Particularly affected were healthcare organizations, with some hospitals being forced to divert patients and delay operations as a result of encrypted systems.
- Large corporations and government organizations also suffered operational setbacks and monetary losses as a result of the attack.
- The prevalence of unpatched systems, especially those using outdated versions of Windows, played a major role in the rapid spread of WannaCry.
- Many organizations were exposed to the EternalBlue exploit because they had not installed the necessary security updates and patches.
- The attack also made clear how crucial vulnerability management and prompt patching are to preventing such widespread incidents.

Lessons To Be learnt

Timely Patching: Regularly applying security patches and updates is crucial to protect against known vulnerabilities. Organizations should establish effective patch management processes to ensure timely deployment of patches.

Vulnerability Management: Implementing a robust vulnerability management program helps identify and prioritize vulnerabilities in systems, enabling proactive mitigation and patching.

Network Segmentation: Segmenting networks into distinct security zones can help contain the spread of malware and limit the impact of an attack, as it prevents lateral movement across the network.

Backup and Recovery Strategies: Maintaining regular backups of critical data and testing the effectiveness of backup and recovery procedures is essential for minimizing the impact of ransomware attacks. It enables organizations to restore their systems and data without paying the ransom.

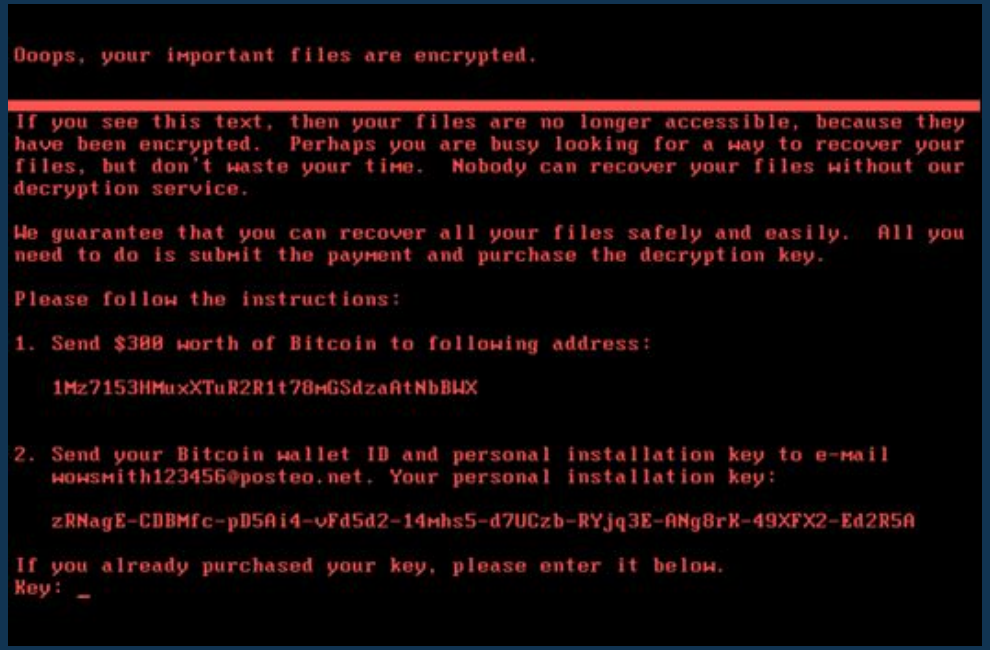
Hyperiondev

https://cdn.mos.cms.futurecdn.net/D8cbEbadAxpUWsa3vcRnoY.png

NotPetya Attack (2017)

The NotPetya cyber attack that occurred in 2017 was a significant global incident that had devastating consequences for businesses and critical infrastructure.

The attack was initially disguised as a ransomware attack, but it was later revealed to be a destructive wiper malware designed to cause widespread disruption.



https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.crowdstrike.com%2Fblog%2Fpetrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft%2F&psig=AOvVaw09ymWQGWTXmN_Esb3-9mN&ust=1686931272734000&source=images&cd=vfe&ved=0CBEQjRxqFwoTCJDn_O3Sxf8CFQAAAAAdAAAAABAI

Hyperiondev

Repercussions & Catalysts

- NotPetya spread rapidly through multiple infection vectors, primarily targeting organizations in Ukraine. However, it quickly infected networks worldwide due to its ability to exploit vulnerable systems.

- The attack utilized various propagation methods, including a compromised update of a Ukrainian accounting software called M.E.Doc, phishing emails, and the EternalBlue exploit (similar to the one used in the WannaCry attack).

- The NotPetya attack severely damaged critical infrastructure and businesses around the world. Numerous businesses, including multinational corporations, suffered serious disruptions and monetary losses. There was widespread chaos as a result of the impact on vital services like transportation, healthcare, and shipping.

- Businesses experienced data loss, system outages, disruptions to their supply chains, and expensive recovery procedures. Organizations with poor backup and recovery plans were particularly hard-hit by NotPetya, making system restoration and data recovery challenging.

Lessons To Be learnt

Planning for Incident Response: NotPetya brought home how important it is to have an incident response plan that is well thought out. To swiftly detect, respond to, and mitigate cyber attacks, organizations need a clear and tried strategy. This covers incident containment procedures, communication standards, and recovery procedures.

Vulnerability Management: Implementing a robust vulnerability management program helps identify and prioritize vulnerabilities in systems, enabling proactive mitigation and patching.

Network Segmentation: Segmenting networks into distinct security zones can help contain the spread of malware and limit the impact of an attack, as it prevents lateral movement across the network.

Backup and Recovery Strategies: Maintaining regular backups of critical data and testing the effectiveness of backup and recovery procedures is essential for minimizing the impact of ransomware attacks. It enables organizations to restore their systems and data without paying the ransom.

Wrapping up

The workshop covered a number of case studies in cyber security, including the NotPetya cyber attack, WannaCry ransomware attack, Target data breach, and phishing and social engineering incidents.

These actual instances highlighted the value of preventative security measures. The importance of network segmentation, prompt patching, threat detection, incident response planning, security awareness training, and secure software supply chains were among the most important lessons learned.

By putting these lessons into practice, organizations can better protect sensitive data, maintain a strong security posture, and increase their cyber resilience in the face of changing cyberthreats.

Next up

Securing Web Applications (Zahir)

Hyperiondev

Thank you for joining us

1. Take regular breaks
2. Stay hydrated
3. Avoid prolonged screen time
4. Practice good posture
5. Get regular exercise

"With great power, comes great responsibility."

Questions and Answers