WannaCry Ransomware (2017) – Case Study

1. Introduction

In May 2017, more than one company was attacked. Organizations from various fields got hit by the same ransomware named WannaCry that spread across the globe within days. Hospitals in the UK, giant firms like FedEx, Nissan, Renault – even government offices were all victims to it. In total over 200,000 computers from more than 150 countries downloaded this virus onto their systems. The reason this made such big news was due to how it proved just how fast damage on a global scale could happen from one unpatched vulnerability.

2. Attack Overview

A ransomware worm. That means as soon as it infects a system, it locks or encrypts the files and demands money (in Bitcoin) to unlock them. If the ransom is not paid fast, the price goes up.

The infection was done using external penetrations. One of the best known is through EternalBlue, which was not made by some arbitrary hacker but was developed by the USA's NSA for their own use. It got leaked online by a group called Shadow Brokers with WannaCry ransomware attack payloads.

3. Vulnerability Exploited

The weak spot was stupidly simple: ancient, unpatched versions of Microsoft Windows. Any organization that failed to apply the critical security update from Microsoft would be basically wide open to attack. Many IT teams were slow to upgrade, or run legacy systems like Windows XP, so exposure was even more pronounced.

4. Attack Execution

Here's what happened in essence:

1.Shadow Brokers dumped EternalBlue on the web.

2.WannaCry ransomware was using this exploit.

3.That “worm-like” behavior of automatically infecting one machine and then spreading to others without requiring anyone to click a link or open a file is what made it spread so fast and so far.

5. Impact Assessment

- **Confidentiality:** Technically, there was no private data stolen. It was not about spying. It was about ransom.
- **Integrity:** The files were not tampered with, though were encrypted and locked so could not be used by people.
- **Availability:**This was perhaps the most severe impact. Appointments were canceled in UK NHS Hospitals, and ambulances were even being diverted. Companies like FedEx, Nissan, and Renault were at a standstill. It literally paralyzed, creating shutdowns, and havoc in many industries.

6. Mitigation & Response

The attack wasn’t ended interestingly by law enforcement. A young security researcher, Marcus Hutchins found something weird in the code. It was trying to connect to a strange, random domain name. Hutchins registered that domain it cost him about $10—and accidentally triggered a kill switch in the malware. Later, Microsoft also pushed out emergency security patches, even for **old systems like Windows XP** that they had stopped supporting years before.

7. Lessons Learned

- Lesson from this attack is very clear:
- Always update the systems at the earliest and as and when patches are available.
- Frequent backups should be maintained as ransomware should not hold your data hostage.
- Organizations should not rely on outdated operating systems.

- Cyber security awareness is highly emphasized; action needs to be fast once a threat has been unearthed.

References

BBC News (2017). WannaCry cyber-attack: Who was affected?

The Guardian. NHS and global companies hit by WannaCry ransomware (2017).

Symantec Report. Technical analysis of WannaCry ransomware (2017).

Target POS Breach (2013) – Case Study

1. Introduction

Target Corporation, one of the super-large chains of retail stores in the United States, experienced a major cybersecurity incident over late 2013. The window of compromise extended between November and December of 2013 and was publicly revealed on December 19, 2013.

2. Attack Overview

- **Type of Attack:** Supply-chain attack leveraging POS malware.

- **Initial Access Vector**: Attackers first compromised an HVAC third-party vendor (Fazio Mechanical Services) by means of phishing and then leveraged stolen credentials to gain access to Target's internal network.

3. Vulnerability Exploited

- Insufficient third-party security controls.

- Network segmentation between vendor systems and payment systems is weak.
- Intrusion alerts from security tools are ignored.

4. Attack Execution

1-The vendor gets compromised by a phishing attack.

2-The Vendor credentials are used for Target's remote access system.

3-Attackers laterally move into the POS systems.

4-BlackPOS (Kaptoxa) malware used to scrape payment card data.

5-Sent data to attacker-controlled servers located in the U.S. and Russia.

5. Impact Assessment

- **Confidentiality:** 40M payment card numbers and about 70M customer records by name, email, and address.
- **Integrity:**No evidence of data manipulation.

- **Availability:** Business operations continued; no major service outages.

6. Mitigation & Response

- Target removed the malware. It notified the affected customers. Free credit monitoring was offered to them.

- There is stronger network segmentation security control in place plus other security controls. Acceleration in adopting EMV chip-and-PIN technology has been fostered by incidents like this one.

- Total cost in excess of $162 million, including a settlement amounting to $18.5 million with U.S. states.

7. Lessons Learned

1-Continuous monitoring and alertness to responses is key.

2-Demand strict security oversight over third-party vendors.

3-Network segmentation, multi-factor authentication, encryption in use, and regular security audits are the practices that organizations have to practice to reduce the risks of breaches.

References

1-U.S. Senate Committee on Commerce, Science, and Transportation. 2014. A “Kill Chain” Analysis of the 2013 Target Data Breach.

2-Verizon. 2014 Data Breach Investigations Report (DBIR).

3-Krebs, B. 2014. Target Hackers Broke in via HVAC Company. KrebsOnSecurity.