Threat Intelligence Report: WannaCry Ransomware Attack(2017)

1. Executive Summary

The WannaCry ransomware outbreak occurred in May 2017 and was a global-scale cyber event. WannaCry was an unprecedented cyber Attack, which was record-breaking in terms of speed and virality. The Attack hit about 230,000 computers around the world, including several countries, such as the U.K., Russia, and India, and WannaCry was a self-propagating ransomware, which used the vulnerability in Microsoft's SMB protocol to propagate through a network. The case is covered in this report to emphasize that even a single vulnerability may generate massive losses for an organization.

2. Introduction

The WannaCry ransomware attack, also known as WCry or WanaCryptor, was widely covered cyber incidents of its time. It was first discovered on May 12, 2017 and classified as crypto-ransomware, combining file encryption and extortion techniques of a ransomware with the self-propagating capabilities of a computer worm.

The attack exploited a known vulnerability in the Windows Server Message Block (SMBv1) protocol, commonly referred to as **EternalBlue**, which was leaked by the "Shadow Brokers" group. This vulnerability allowed remote code execution on unpatched Microsoft Windows systems, enabling WannaCry to spread rapidly without requiring user interaction.

Once a system was infected, the malware scanned internal networks and the internet for other vulnerable machines with TCP port 445 open and attempted to compromise them. After encrypting files, the attackers demanded a ransom payment ranging from $300 to $600 in Bitcoin for decrypting them.

The WannaCry attack demonstrated the critical importance of timely patch management, secure system configurations, and cybersecurity awareness among internal stakeholders.

3. Background

Before the WannaCry ransomware attack, many organizations were using outdated or unpatched versions of Microsoft Windows systems, it exploited a critical vulnerability in SMB protocol called “EternalBlue”, was originally developed by the U.S.National Security Agency (NSA) and later leaked publicly by a hacking group (Shadow Brokers) in April 2017. Attackers took substantial advantage of that, deploying a dangerous virus that replicates both ransomware and worms. Although Microsoft had released security patches addressing these vulnerabilities. Still organizational personnel are not followed up with regular system updates, and vulnerability management.

At the time, cybersecurity awareness and vulnerability management practices varied significantly across industries, particularly within critical infrastructure sectors such as healthcare. These conditions created an environment in which a wormable ransomware attack could spread rapidly once a widely exploited vulnerability became publicly available.

4. Attack Timeline

Date and Time	**Event**
May 12, 2017, 07:44 UTC	Evidence pointing to an initial infection in Asia.
May 12, 2017, 03:24 am EDT	Starting to spread in European countries
May 12, 2017, Late morning	First NHS trusts report problems in United Kingdom
May 12, 2017, 01:06 pm	First notification to NHS England’s Emergency response team
May 12, 2017, 04:00 pm	NHS declared Wannacry a national major incident
May 12,2017	A spanish mobile company compromised, affect thousands of computer
May 12, 2017, Within 24 hours	Ransomware reported to infect 230,000+ computer systems in more than 150 countries

Date and Time	Event
May 12, 2017, Afternoon	Marcus Hutchins a security researcher identified and registered the kill switch domain
May 12, 2017, 15:03 UTC	Kill switch halts initial attack wave
May 13-15, 2017	New WannaCry variants emerge without kill switch dependency
May 15, 2017 onwards	Secondary infection waves from varionts continue to propagate.

5. Technical Analysis

5.1 Vulnerability Exploited

- **CVE ID:** CVE-2017-0144
- **Vulnerability Exploited:** Eternal blue
- **Affected Protocol:** Server Message Block (SMB) v1
- **Vulnerability Type:** Remote code execution
- **Affected Systems:** Windows Server 2003, Windows Vista, Windows 7, Windows Server 2008, Windows Server 2008 R2, Windows 8, Windows 8.1, Windows Server 2012, Windows Server 2012 R2, and Windows XP
- **Patch Release:** Prior to the malware attack Microsoft released MS17-010 security updates in March 2017
- **CVSS Severity:** Critical
- **Root Cause:** Unpatched Systems were highly vulnerable and supported attackers to execute arbitrary code with System privileges.

5.2 Malware Architecture

Wannacry applies a multi-component architecture combining functionalities:

- **SMB Worm component:** Responsible for self propagation
- **EternalBlue Exploit Payload:** Executes remote codes on vulnerable SMBv1 systems

- **DoublePulsar Backdoor Detection:** Checks for pre-existing compromised systems
- **Encryption Engine:** Implements file encryption using AES and RSA cryptography
- **Ransom Notification Interface:** Displays extortion demands to users

5.3 Infection Vectors and Procedure

Evidence indicates that early infections originate through exposed SMB services, the attack does not involve any social engineering. The infection vectors include:

- **Exposed SMB Ports:** TCP port 445(SMB service) direct exposure to the internet without any authentication.
- **Absence of Network Segmentation:** Missing controls of proper firewall rules restricting SMB traffic
- **Unpatched Systems:** Systems running vulnerable SMBv1 protocol without MS17-010 patches applied
- **Credential-Based Access:** Compromised RDP or SMB credentials allowing unauthorized access

Attack Flow:

- Scanning for vulnerable SMB services on TCP port 445.
- Exploiting scanned vulnerability using backdoor, EternalBlue.
- Installation of DoublePulsar backdoor.
- Deployment of WannaCry ransomware payload.
- File encryption and display of ransom demand of 300 USD.

5.4 File Encryption Process

WannaCry encrypts victim files using a hybrid cryptography approach:

- **Symmetric Encryption:** Files are encrypted using the Advanced Encryption Standard (AES) algorithm
- **Asymmetric Encryption:** The AES keys are encrypted using RSA-2048 public key cryptography
- **Key Management:** RSA private key remains controlled by the attackers, making decryption of the files in attackers regulation.
- **Files Extensions:** Encrypted files are appended with the .WCRY extension

5.5 Mapping of MITRE ATT&CK

Factors	Techniques	ID
Initial Access	Exploit Public-Facing Application	(T1190)
Execution	Command and Scripting Interpreter	(T1059)
Persistence	Boot or Logon Autostart Execution	T1547
Lateral Movement	SMB/Windows Admin Shares	T1021.002
Impact	Data Encrypted for Impact	T1486

6. Impact Analysis

A wide range of governments, companies, universities, and hospitals were publicly reported as victims of the 2017 WannaCry ransomware outbreak. The following list highlights notable affected entities; however, it is not exhaustive, as many organizations did not publicly disclose the impact or were affected indirectly.

Government and Public sector

Organization Name	Disrupted Services
Andhra Pradesh Police (India)	100 systems were affected
Gujarat government (India)	120 computers connected to Gujarat government's IT network
KDMC, Maharashtra (India)	25 computers
Department of Power, Bengal (India)	Computers of four blocks in West Midnapore
Ministry of Internal Affairs, Russia	1,000 computers
Deutsche Bahn, Germany	Hundreds of Windows systems and station display boards disrupted

Healthcare and hospitals

Organization Name	Disrupted Services
National Health Service (NHS), England	1% of NHS devices in England, Up to 70,000 devices may have been affected or taken offline as a precaution
NHS, Scotland (UK)	7 of 14 Scottish health boards disrupted, an estimate of tens-of-thousands-of-devices impacted
NHS trusts and primary care (England)	Directly or indirectly around 81 of 236 trusts affected, also at least 603 primary care and related organizations impacted. More than 1,200 diagnostic devices (e.g., MRI, blood analyzers) infected or disconnected.
Dharmais Cancer Hospital, Indonesia	nearly all computers" at Dharmais Hospital were hit, locking patient records and billing

Education and research institutions

Organization Name	Disrupted Services
Dalian Maritime University, China	Reports describe infections on campus PCs and internal servers
Other Chinese universities	Nearly 30,000 institutions, including universities, faced infection

Telecoms and internet providers

Organization Name	Disrupted Services
Telefónica, Spain	Contemporary reports describe "hundreds of computers" infected inside Telefónica's intranet
Portugal Telecom, Portugal	Reportedly first European telecoms affected

MegaFon, Russia	A number of computers

Transportation, automotive, and logistics

Organization Name	**Disrupted Services**
FedEx (TNT Express), US / global	Filings and reports describe “critical systems” and “a large number of workstations and servers,” were affected
LATAM Airlines, Latin America	Some internal IT systems and flight-related support tools
Renault, France	Reports say production systems and office PCs were affected

Technology, media, and other private companies

Organization Name	**Disrupted Services**
Boeing (US)	A small number of systems” affected and no production or flight safety impact
Hitachi (Japan)	Reported that parts of its internal network were hit, causing issues such as email delays and system outages; sources describe “some computers and servers” affected
Automobile Dacia (Romania)	Included in reports of Renault-group entities impacted, with production temporarily disrupted at the Mioveni plant
CJ CGV (South Korea)	CGV cinema operations saw WannaCry infections on ticketing and back-office PCs

7. Attribution and Threat Actors

Suspected Attribution:

- Some security researchers and intelligence analysts considered that Lazarus Group, which is funded by the North Korean state, may have been involved. However, this remains speculation and has not been confirmed by any government officials.

Confirmed Facts:

- The backdoor which was the main reason of the exploit “EternalBlue” was developed by NSA and later leaked by the attackers group “Shadow Brokers”.
- Multiple variants of WannaCry were developed and deployed by some unknown actors.
- The ransom payment mechanism utilized cryptocurrency (Bitcoin) for the payment.

8. Detection Opportunities

- Prior monitoring of SMB traffic.
- Intrusion detection and prevention signatures targeting EternalBlue activity.
- SIEM alerts indicating widespread file encryption activity.
- Endpoint alerts flagging unauthorized or suspicious processes.

9. Prevention and Mitigation Strategies

9.1 Prevention During Active Threat

- **Network Isolation :** Infected systems were disconnected from the network to prevent intra-network spread.
- **Restoration:** Restoring system services from uninfected backups.
- **Incident Response:** Activating incident response team and proceeding to access compromise scope.
- **Reporting to law enforcement agencies:** Reporting to higher authorities about compromises. .

9.2 Long-Term Mitigation

- **Patch Management:** Deployment of MS17-010 security patches to all Windows systems and regular update of softwares with vulnerability scanning.
- **Network Hardening:** Disabling SMBv1 protocol on all the systems, implantation of network segmentation to limit the spreading, applying firewalls on the SMB traffic.
- **Backup and Disaster Recovery:** Implementation of automated and regularly checked backup procedures with restoration testing .
- **Detection and Monitoring:** Applying endpoint protection and IDS solutions.
- **Awareness Training:** Training employees and users on social engineering and phishing vectors with importance of patch management and security updates regarding ransomware threats. Incident reporting procedures and policy compliance.

10. Lessons Learned

- Importance of patch management and regular software updates.
- Cyber hygiene failure could lead to big data failures and financial, operational loss.
- Even minor vulnerabilities can have a serious impact.
- Legacy protocols are associated with substantial security risks.
- Aware and trained employees are vital in preventing security incidents.
- Recognition that cyber threats are international in nature and require cross-border law enforcement.
- Cyber insurance products are designed to mitigate financial impacts.

11. Conclusion

The famous WannaCry ransomware attack in May 2017 has become a landmark case study in cybersecurity. This case basically shows just how much disruption can be caused by something as small as one unpatched vulnerability. It affected more than 230,000 computers across 150 countries and caused billions of dollars in damage. Since then, it has become one of the most important case studies among both beginners and professionals in the field of cybersecurity.

Quite a few analyses and research studies have been conducted based on this incident. In one such study, according to the research done by Kaspersky Lab, less than 0.1% of the infected computers were running Windows XP while 98% were using Windows 7. The attack highlights how apparently insignificant vulnerabilities, if not patched, can

become one of the major cybercrimes of that time. Even with all those investigations, finding out the primary victim of that attack is still quite difficult today.

12. References

[1] Wikipedia contributors. (2017). *WannaCry ransomware attack*. *Wikipedia, The Free Encyclopedia*.
https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

[2] SecureWorks. (2017). *WCRY (WannaCry) ransomware analysis*. SecureWorks Counter Threat Unit Research.
https://www.secureworks.com/research/wcry-ransomware-analysis

[3] National Audit Office. (2017). *Investigation: WannaCry cyber attack and the NHS*. UK Parliament.
https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf

[4] Ghafur, S., et al. (2019). *A retrospective impact analysis of the WannaCry cyber attack on the NHS*. *EClinicalMedicine, 15*, 64–72.
https://pubmed.ncbi.nlm.nih.gov/31602404/

[5] Kaspersky Lab. (2020). *Ransomware WannaCry: All you need to know*. Kaspersky Resource Center.
https://www.kaspersky.com/resource-center/threats/ransomware-wannacry

[6] Google Cloud. (2024). *WannaCry ransomware campaign: Threat details and analysis*. Google Cloud Blog.
https://cloud.google.com/blog/topics/threat-intelligence/wannacry-ransomware-campaign

[7] BBC NEWS. (2017). Ransomware cyber-attack: Who has been hardest hit?
https://www.bbc.com/news/technology-39899646