IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Wannacry Ransomware Attack: Lessons from a Global Cyber security Crisis

Janhavi Deshpande, Stavan Shinde
Student/Security Researcher
Guru Nanak Khalsa College

Abstract:

The WannaCry ransomware attack in May 2017 caused widespread disruption in government, healthcare, and corporate sectors across 150 countries. The malware exploited a Windows operating system vulnerability, encrypting files and demanding a ransom in Bitcoin for decryption. The attack's origins, propagation, and ramifications are examined, along with the EternalBlue exploit used by WannaCry. The response, involving collaboration among governments, security experts, and cybersecurity firms, serves as a blueprint for future cyber threats. The attack emphasizes proactive security practices, patch management, and increased cybersecurity awareness.

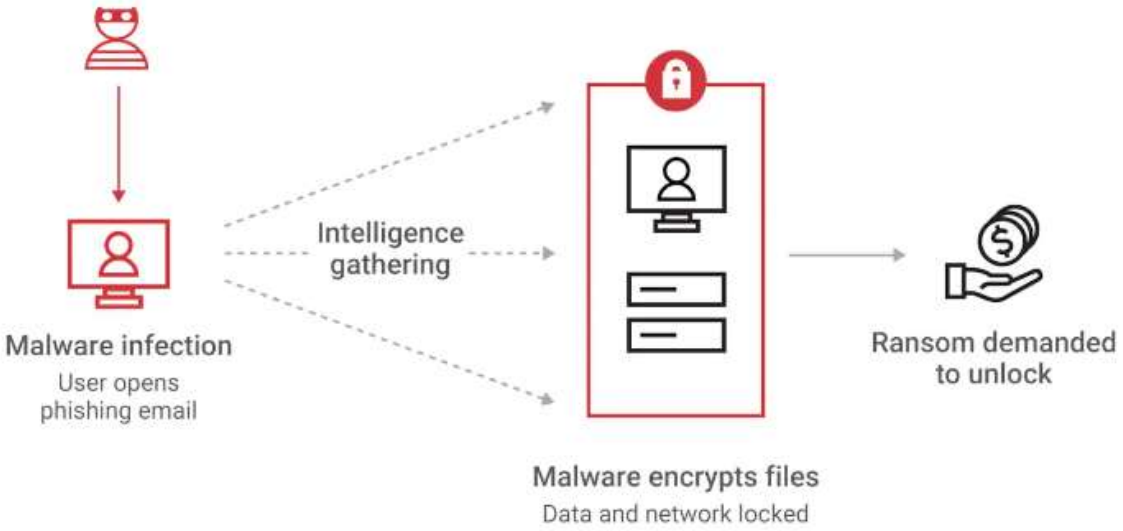
Introduction:

The WannaCry ransomware attack , also known as WannaCrypt0r, had a far-reaching impact on organizations and individuals worldwide. This case study provides an in-depth analysis of the attack and its implications. To understand this attack better let's see what ransomware attacks and EternalBlue means.

Ransomware Attacks

A ransomware attack is a malicious cyberattack where cybercriminals encrypt the victim's data and demand a ransom in exchange for the decryption key. The attackers hold the victim's data hostage, making it inaccessible until a ransom is paid, usually in cryptocurrency like Bitcoin. The ransomware enters a victim's computer or network through malicious email attachments, infected downloads, or exploiting software vulnerabilities. Once inside the victim's system, the ransomware encrypts files and data, rendering them unreadable without the decryption key. After encrypting the victim's data, the ransomware displays a ransom note on the victim's screen, providing instructions on how to pay the ransom to receive the decryption key. The ransom demand can vary widely, ranging from a few hundred dollars to thousands or more. Victims who decide to pay are instructed to communicate with the attackers, often through the Tor network or other anonymizing methods to protect their identity. After the ransom is paid, the attackers are expected to provide a decryption key that will unlock the victim's encrypted data. If the decryption key works as promised, the victim can decrypt their data and regain access to their files. However, there is no guarantee that the attackers will provide a working key, and paying the ransom funds criminal activities.

Ransomware attacks are a significant and evolving threat in cybersecurity, targeting both individuals and organizations. Being proactive with security measures and having effective incident response plans is critical to reducing the risk and impact of such attacks.



(reference : https://en.wikipedia.org/wiki/WannaCry_ransomware_attack)

EternalBlue

EternalBlue is a notorious computer exploit developed by the NSA and leaked by the "Shadow Brokers" in April 2017. It targeted a vulnerability in the Windows operating system, specifically the Server Message Block (SMB) protocol, which is used for sharing files, printers, and other network resources. The exploit was part of a collection of tools used by the NSA's Equation Group for surveillance and cyber operations. The vulnerability, identified as CVE-2017-0144, allowed remote attackers to execute arbitrary code without user interaction. Once leaked, cybercriminals and hacking groups quickly adopted it to launch a wave of cyberattacks, with the WannaCry ransomware attack in May 2017 being the most notable example.

Working of EternalBlue:

1. Target Identification:
To find vulnerable systems, EternalBlue first searches the internet. It searches for hardware that is running out-of-date Windows versions and hasn't had the MS17-010 vulnerability patched.

2. Exploitation:
EternalBlue uses the SMB vulnerability to run arbitrary code on the target system after identifying a vulnerable system. It uses the SMB protocol's weakness to its advantage by sending specially constructed packets to the target system.

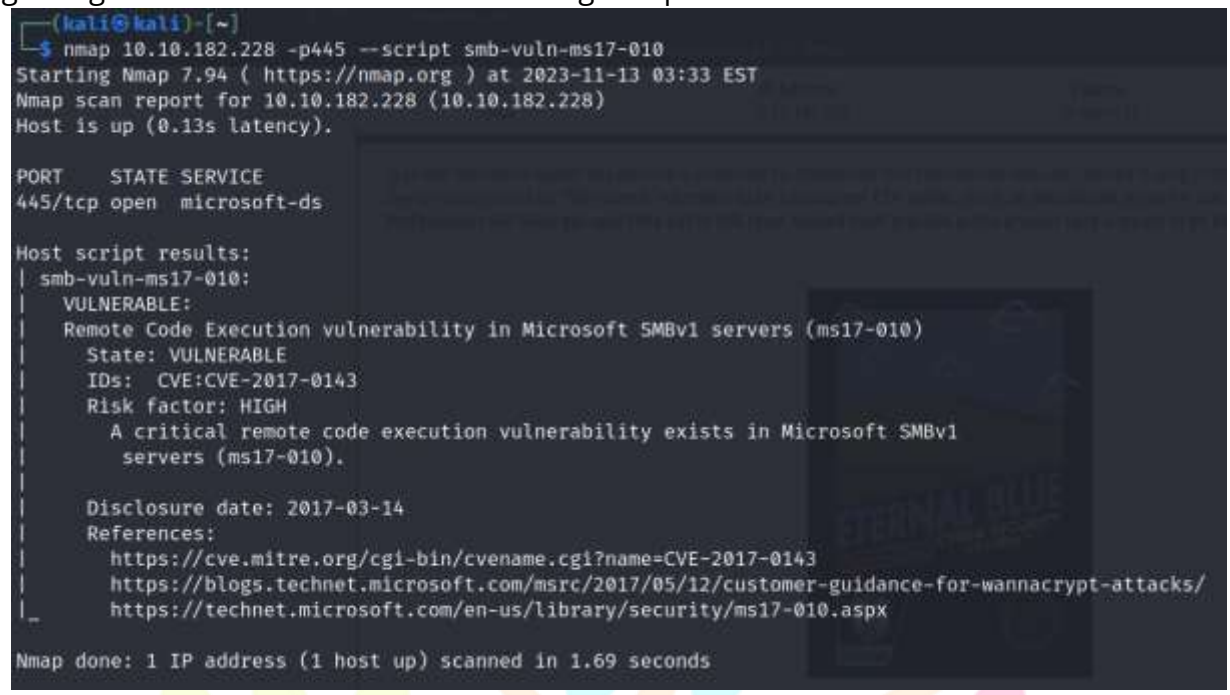
3. Implantation:
EternalBlue installs a backdoor or malicious code on the targeted system after successfully exploiting the vulnerability. This gives the attacker access to the system without authorization and possibly even remote control.

4. Propagation:
EternalBlue's capacity to spread throughout networks is one of its noteworthy features. It has the ability to propagate laterally through an organization's network, infecting additional weak systems.

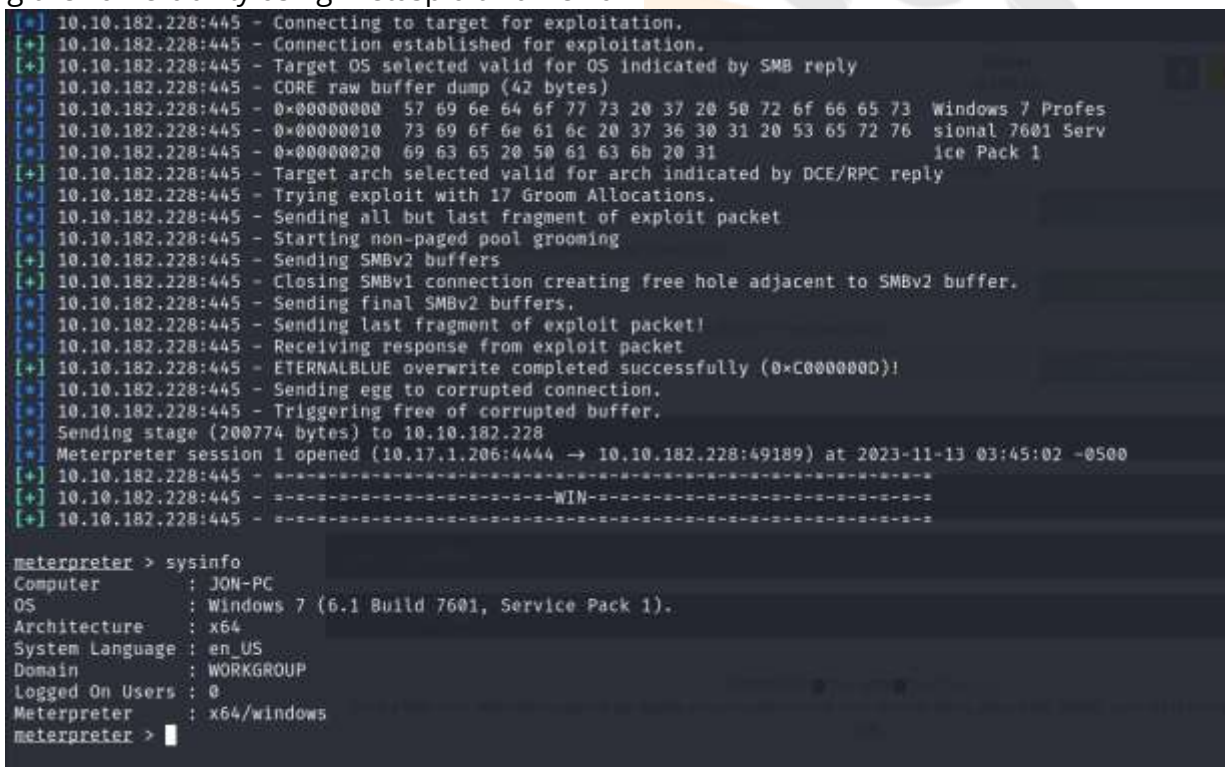
5. Payload Delivery:
EternalBlue is often used as part of a larger attack, delivering additional payloads such as ransomware or other types of malware. In the case of WannaCry, the payload encrypted files on the infected system and demanded a ransom for their release.

Exploiting EternalBlue:

Checking if target is vulnerable to EternalBlue using nmap tool



Exploiting the vulnerability using metasploit framework



Attack Details:

- EternalBlue, a hack developed by the US National Security Agency, exploited a weakness in Microsoft Windows.
- The Shadow Brokers, a group of hackers, made the hack public before the WannaCry attack.

- Microsoft released a security patch to protect against this exploit two months before the attack.
- Many individuals and organizations who didn't regularly update their systems were exposed to the attack.
- The WannaCry ransomware attack initially spread through a phishing campaign, but EternalBlue allowed it to spread.
- The attackers demanded $300 and later $600 bitcoins, with a three-day deadline for payment.

Map of the countries initially affected by Wanancry Ransomware

(Reference : https://en.wikipedia.org/wiki/WannaCry_ransomware_attack)

Impact:

- Disrupted critical infrastructure: Hospitals, banks, transportation systems, government agencies.
- Caused significant financial losses: Ransom payments, data recovery costs, system repairs.
- Global response: Governments and cybersecurity agencies initiated emergency responses.
- Raised global awareness: Attack raised importance of cybersecurity and patch management.

"WannaCry" ransomware attack losses could reach $4 billion

MONEY WATCH

BY JONATHAN BERR

Global financial and economic losses from the "WannaCry" attack that crippled computers in at least 150 countries could swell into the billions of dollars, making it one of the most damaging incidents involving so-called ransomware.

Cyber risk modeling firm Cyence estimates the potential costs from the hack at $4 billion, while other groups predict losses would be in the hundreds of millions. The attack is likely to make 2017 the worst year for ransomare scams, in which hackers seize control of a company's or organization's computers and threaten to destroy data unless payment is made.

In 2016, such schemes caused losses of $1.5 billion, according to market researcher Cybersecurity Ventures. That includes lost productivity and the cost of conducting forensic investigations and restoration of data, said Steve Morgan, founder and editor-in-Chief of Cybersecurity Ventures.

(reference :"WannaCry" ransomware attack losses could reach $4 billion - CBS News)

Known Affected Companies:

West Bengal State Electricity Distribution Company:
Four of the company's offices tested positive for WannaCry infections, according to the Indian state power distribution company.

Iberdrola:
Spanish electrical company Iberdrola disclosed infection following the utility's shutdown of multiple systems to counter the attack.

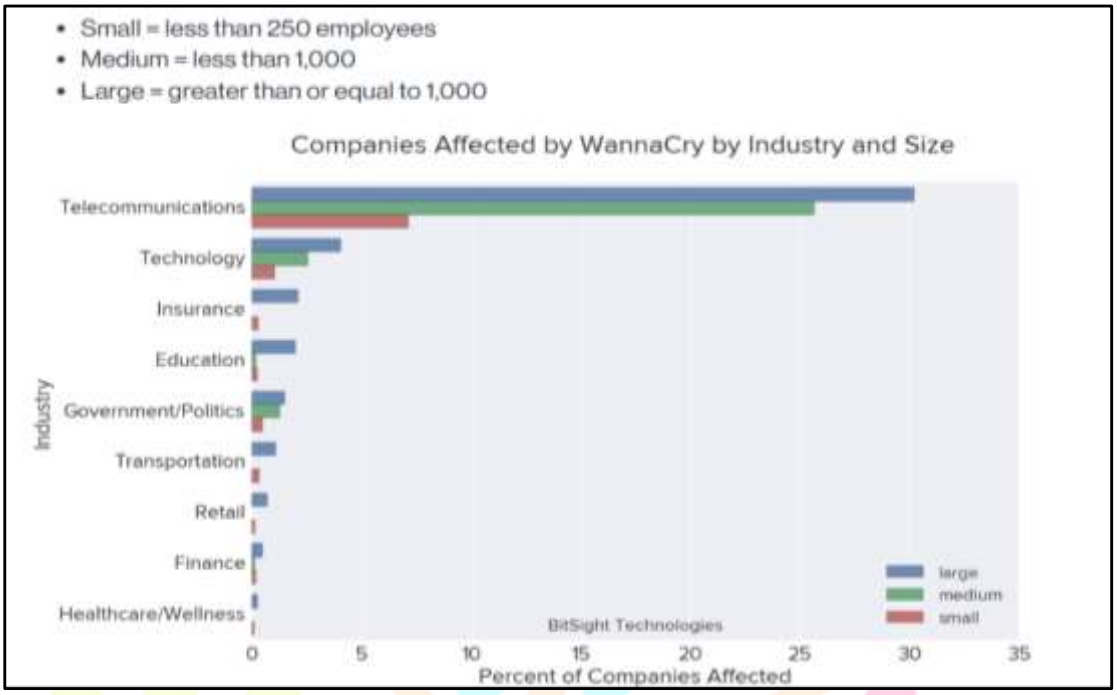
Petrobras:
In response, the social security system, the Foreign Ministry of Brazil, and the state-owned oil company Petrobras reportedly turned off their computers as a precaution.

Governmental Entities & Offices:

NHS:
NHS (National Health Service) is a publicly funded healthcare system in the United Kingdom. It provides healthcare services to the residents of the United Kingdom, including England, Scotland, Wales, and Northern Ireland. The ransomware affected the NHS by causing 200,000 computers to lock out users with red-lettered error messages demanding Bitcoin, and has since been blamed on elite North Korean hackers. The £92m cost is a rough estimate of the total cost of WannaCry as no data was collected on the costs of recovering IT systems or the extent of patience disruption. Following the WannaCry attack, a "Cyber Handbook" was produced to describe the approach and actions to be taken by NHS England, NHS Digital and NHS Improvement in the event of a cyber attack affecting the NHS. Local NHS and care organizations commissioned additional external support to audit systems and processes locally in response to the WannaCry. NHS Digital also continued to provide on-site data security assessments to NHS organizations since WannaCry.

Russian Interior Ministry:
On May 12, hackers tried to attack Windows OS computers in 74 countries. A total of 45,000 ransomware cyber attacks were carried out across the world, while the most attempts at infecting computers were registered in Russia. Hackers asked for a bitcoin ransom payment to unlock infected computers. The Interior Ministry, mobile operator MegaFon and state rail monopoly Russian Railways all reported infections, with employees locked out of their computers.

Andhra Pradesh (Indian police):
Up to eighteen different police units' state police reported having their systems locked out.



Attributes:

The well-known ransomware outbreak known as WannaCry has characteristics that set it apart from previous online dangers. These traits provide insight into the type of assault, how it affected the victims, and the larger difficulties associated with attribution in cyberspace.

Worm-Like Propagation:
Worm-like propagation was WannaCry's most notable feature. In contrast to conventional ransomware, which usually propagates through human acts, WannaCry circulates itself through weak systems that are linked to the internet. The ransomware was able to quickly infect a large number of machines worldwide because of the exploitation of a Windows vulnerability, which enabled its autonomous circulation. WannaCry's worm-like behavior allowed it to spread quickly over the world and cause widespread havoc.

Using the EternalBlue vulnerability:
One of the main reasons WannaCry was successful was the usage of the EternalBlue vulnerability. EternalBlue made it possible for the ransomware to take advantage of a flaw in Microsoft Windows computers. Due to this attack, WannaCry was able to spread quickly and infect a large number of systems. The availability of the exploit and its association with a government entity prompted concerns about appropriate disclosure practices and the possibility that other actors may utilize these vulnerabilities for malicious purposes.

Getting Ready for More Disasters:
The WannaCry attack acted as a global alarm for governments and institutions all over the world. It emphasized the necessity of taking preventative action to fortify cybersecurity, enhance information exchange, and improve incident response capacities.

Lazarus Group:

The Lazarus Group is believed to be a state-sponsored hacking organization, often associated with North Korea. In May 2017, security researchers and cybersecurity experts attributed the WannaCry ransomware attack to the Lazarus Group based on the attack's characteristics and code similarities with previous Lazarus Group activities.

The Lazarus Group is known for conducting financially motivated cyberattacks, often to fund the North Korean regime. In the case of WannaCry, the motive behind the attack was believed to be financial gain, as the ransom payments demanded were meant to generate revenue.

The WannaCry ransomware attack exhibited characteristics similar to the Lazarus Group's past activities, including the use of sophisticated code and techniques. The Lazarus Group is known for its ability to develop and deploy sophisticated malware, which was evident in the WannaCry attack.

The EternalBlue exploit used in the WannaCry attack was originally developed by the U.S. National Security Agency (NSA) and was later leaked by a hacking group known as the "Shadow Brokers." This exploit played a crucial role in the rapid spread of WannaCry. The Lazarus Group was suspected of leveraging the EternalBlue exploit to carry out the attack.

Response and mitigation:

Following the WannaCry attack, governments, cybersecurity companies, and security experts came together in an amazing international cooperative effort to effectively handle the crisis. Few mitigation techniques for the attack are listed below:

Creating Decryption Tools:

A number of cybersecurity researchers and organizations banded together, realizing the gravity of the situation, to create decryption tools that would enable victims to retrieve their encrypted data without having to pay the ransom. These resources were made publicly available to all impacted users across the globe. The commitment of the international cybersecurity community to make these tools available highlighted how critical it is to assist those affected by these attacks and lessen the financial burden on victims.

Providing Updates to Protect Against Future Vulnerabilities:

The WannaCry attack took advantage of a Microsoft Windows vulnerability that was previously known to exist and for which a security update was available. The incident thus brought to light how crucial it is to maintain systems updated with the most recent security patches. Microsoft responded by releasing patches for Windows versions that are no longer supported, like Windows XP, in an effort to help stop such attacks from happening again. It was crucial to coordinate the global distribution of these patches in order to guarantee that the greatest number of systems could be protected.

The killswitch method:

The ‘killswitch’ mitigation for the WannaCry attack was a serendipitous discovery by Marcus Hutchins that played a crucial role in halting the ransomware's global spread and mitigating its impact. The killswitch was essentially a domain name embedded in the WannaCry ransomware code, which, when found to be active, prevented the ransomware from infecting new systems.

Lessons Learned:

The lessons learned through this outrage serve as a valuable guide for organizations and individuals, highlighting the essential steps and practices necessary to protect digital assets in an ever-evolving landscape of cyber threats. Few of them are mentioned below:

Preventive Security Measures:
WannaCry stressed the importance of preventive security measures. Adopting a security-first mentality and putting procedures like frequent system audits, risk assessments, and vulnerability scans into place are essential for both individuals and organizations. Proactive security procedures assist in minimizing the attack surface and lowering the probability of successful breaches by spotting and fixing possible vulnerabilities before cybercriminals take advantage of them.

Timely Patch Management:
The attack made it abundantly clear how crucial it is to update systems and software with security patches. WannaCry took advantage of a known vulnerability for which Microsoft had already issued a patch.

Regular Backups:
During the WannaCry attack, data backups proved to be extremely helpful. Both individuals and organizations should establish routine, secure data backup practices, such as offsite and offline backups. The impact of ransomware attacks can be lessened by having current backups that are easily accessible, since data can be recovered without giving in to ransom demands.

Security Awareness and Training:
Preventing cyberattacks is greatly aided by user awareness and training. Workers and individuals alike must be made aware of the dangers associated with phishing emails, dubious attachments, and social engineering techniques. Users are the first line of defense against cyberattacks because security awareness programmes can assist them in identifying and reporting possible threats.