Incident Response Team

Report №3

The WannaCry Ransomware Attack

May 12, 2017

04.10.2025

Almaty

Table of Contents

Introduction

On May 12, 2017, the digital world witnessed a terrifying glimpse of a global cyber-pandemic. The WannaCry ransomware attack erupted with unprecedented speed, infecting over 200,000 computers across 150 countries in a single weekend. Unlike typical ransomware that relies on tricking users, WannaCry was a worm, automatically spreading itself across networks by exploiting a critical vulnerability in Microsoft Windows.

It was a perfect storm that caused chaos worldwide:

- It used a powerful hacking tool called "*EternalBlue*", which was allegedly developed by the U.S. National Security Agency (NSA) and then leaked to the public.
- The attack didn't just target one company. It hit everyone who was vulnerable, crippling hospitals in the UK, shutting down factories, and disrupting railways and telecoms.
- WannaCry showed, in the scariest way possible, why keeping software updated is so crucial. Many of the affected systems simply hadn't installed a security patch that Microsoft had released two months earlier.

The incident served as a brutal lesson, highlighting the devastating domino effect that can occur when powerful cyber-weapons fall into the wrong hands.

The Algorithm of The Attack

Stage 1: Initial Infection and Network Discovery

- The attack could begin in two ways: either by a single user inside a network accidentally executing the ransomware dropper (e.g., from a phishing email), or by the worm proactively finding its way in from another infected machine on the same network.
- Once on a computer, the malware first checked for a "kill switch" domain. If it could connect to it, the malware would shut down. This was likely an anti-analysis feature. If it *couldn't* connect (which was the case for most), it proceeded.
- The malware then scanned the local network, looking for other vulnerable Windows machines.

Stage 2: Exploitation and Lateral Movement

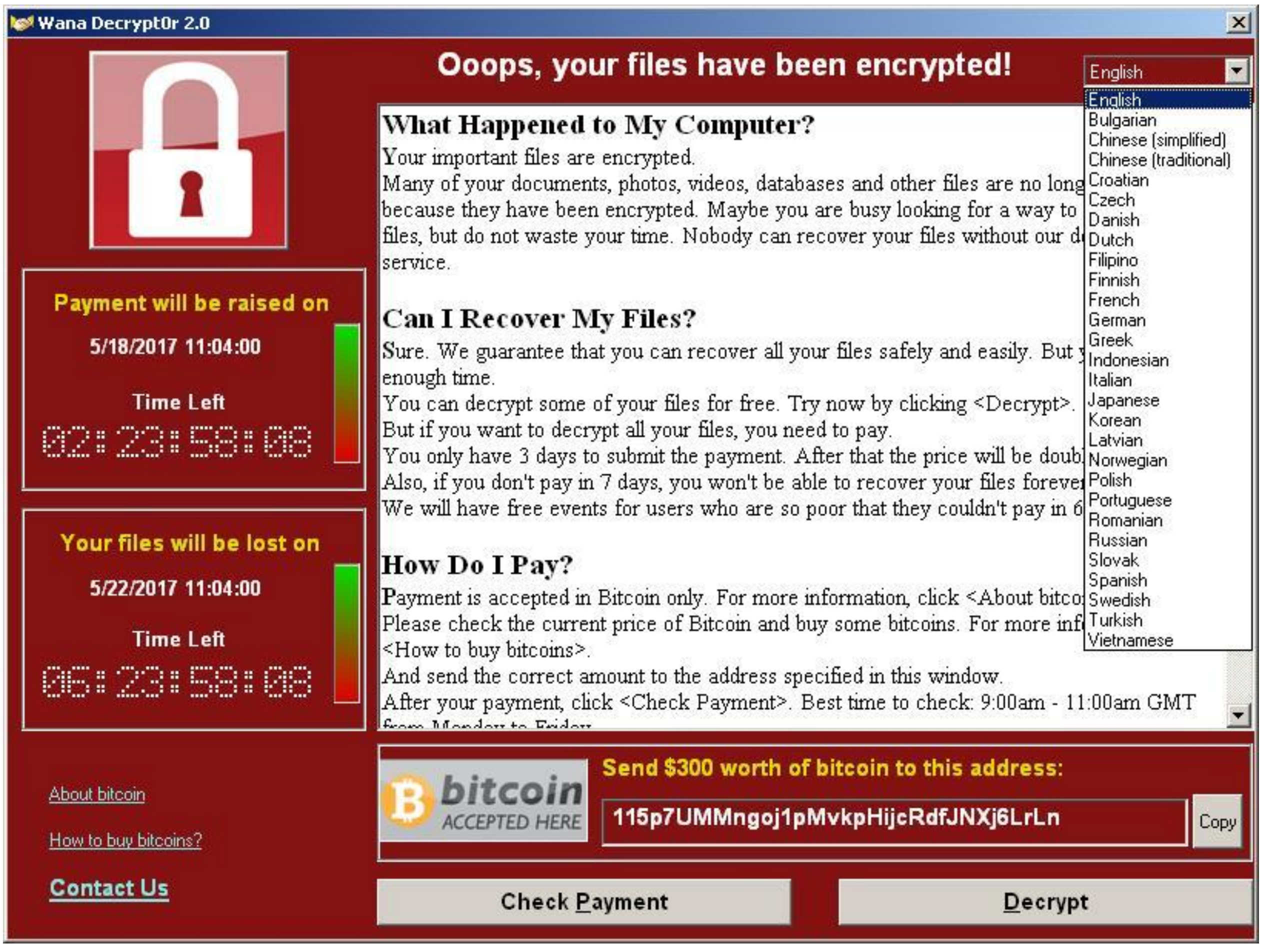
- Upon finding other computers, WannaCry used the "EternalBlue" exploit. This exploit targeted a vulnerability in the Windows Server Message Block (SMB) protocol, which handles file and printer sharing.
- EternalBlue allowed the attacker to execute arbitrary code on the remote, vulnerable system without any username or password. WannaCry used this to upload its own payload and create a service to run it.
- This process then repeated from every newly infected machine, creating a chain reaction. Each computer became a new launching pad to infect others, both on its local network and across the internet, leading to the explosive global spread.

Stage 3: Payload Detonation & Encryption

- After spreading, the core ransomware payload was activated on all infected systems. It began encrypting files on the hard drive, targeting specific, valuable file extensions like .docx, .pdf, and .jpg.
- Once encryption was complete, it displayed the now-infamous ransom note, demanding a payment of $300-$600 in Bitcoin to restore the files. A timer counted down, threatening to increase the price or delete the files entirely.

Stage 4: Devastating Impact

- The encryption of critical data caused immediate operational paralysis for victims, most notably seen in the UK's National Health Service (NHS), where appointments were canceled and surgeries postponed.
- The sheer scale and speed of the attack created a global incident, highlighting critical failures in patch management and the dangers of weaponized government exploits being leaked.



Ooops, your files have been encrypted!

Payment will be raised on

5/18/2017 11:04:00

Time Left

02:23:58:08

Your files will be lost on

5/22/2017 11:04:00

Time Left

06:23:58:08

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no long
because they have been encrypted. Maybe you are busy looking for a way to
files, but do not waste your time. Nobody can recover your files without our d
service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But y
enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doub
Also, if you don't pay in 7 days, you won't be able to recover your files foreve
We will have free events for users who are so poor that they couldn't pay in 6

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitco
Please check the current price of Bitcoin and buy some bitcoins. For more inf
<How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT
from Monday to Friday

Send $300 worth of bitcoin to this address:

115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

The Damage Made

Victims

The WannaCry attack caused immediate, tangible chaos and its financial impact was felt across the globe. The damage went far beyond just locked computers; it disrupted essential services and cost organizations billions!

КАТЕГОРИЗУЦ ЖЕРТВ – компании и обычные люди

The victims were widespread and diverse, showing that the worm did not discriminate. The most severely impacted included:

- The UK's National Health Service (NHS) - over 80 hospitals were infected, leading to canceled appointments and redirected ambulances, creating a direct risk to patient care
    - Global Corporations - companies like FedEx, Renault, and Telefónica had their operations frozen, halting production lines and delivery services
    - Government Agencies - systems in Russia, China, and Spain were also severely affected

Consequences

ГЛАВНЫЙ УЩЕРБ – ФИНАНСОВЫЕ И ПОТЕРЯ ДАННЫХ

- *Operational Disruption*

    - The primary damage was the complete halt of business and service operations. Critical computer systems were rendered unusable, forcing a return to paper-based manual processes where possible
- *Massive Financial Losses*
    - The total global financial impact is estimated to be in the billions of dollars. This includes costs from ransom payments, downtime, lost business, and massive IT cleanup and recovery efforts
- *Risk to Human Safety*
    - The NHS case proved that a cyberattack could have life-or-death consequences by disrupting critical healthcare infrastructure
- *Reputational Damage*
    - Organizations, especially the NHS, faced public scrutiny for failing to apply critical security patches in a timely manner, eroding public trust

Vendors’ Recommendations

The core lesson from WannaCry is that foundational cybersecurity hygiene, especially timely patching, is non-negotiable. The attack exploited a known vulnerability for which a patch had been available for over two months. A proactive, layered defense is the only effective strategy.

Microsoft – microsoft.com

Preventive recommendation: immediately deploy all critical security updates and patches. Enable built-in protections like Windows Defender Antivirus and use Attack Surface Reduction (ASR) rules to block malicious behaviors.

Kaspersky – kaspersky.com

Preventive recommendation: use a reliable security solution with behavior-based detection and exploit prevention. Implement network segmentation to limit the spread of malware.

Fortinet – fortinet.com

Preventive recommendation: deploy Next-Generation Firewalls (NGFWs) with Intrusion Prevention Systems (IPS) to block exploitation attempts. Use anti-botnet services to prevent communication with malicious servers. Segment the internal network strictly and utilize DNS security filtering services to block malicious communications.

My Recommendations

My role: tech employee, pentester.
As a *pentester* I focus on mimicking and tracing back the attacker’s doings. I would…

Phase 1: Simulate the Attack

Step 1: Reconnaissance

- Use network scanning tools (like Nmap) to find all hosts with port 445 (SMB) open
- Use vulnerability scanners to identify systems missing the MS17-010 patch and vulnerable to the EternalBlue exploit

Step 2: Gaining Initial Foothold

- Craft a simulated payload that uses the EternalBlue exploit to achieve remote code execution on a vulnerable target
- Use this access to drop a simple beacon or agent on the system to simulate the initial infection

Step 3: Lateral Movement and Propagation

- From the first compromised machine, scan the internal network for other vulnerable systems
- Use the same EternalBlue exploit to move laterally, attempting to infect those systems and spread the simulated attack

Step 4: Detection

- On compromised systems, simulate ransomware behavior by creating and encrypting dummy files with a test ransom note.
- Document the time it takes for Blue Team to detect the exploit attempts, lateral movement, or file encryption activities

Phase 2: Cooperate with Blue Team

Step 5: Share Findings & Tune Detection

- Provide the Blue Team with the IPs of vulnerable systems and the exact network traffic signatures of the EternalBlue exploit
- Work together to create EDR alerts for suspicious SMB traffic and lateral movement patterns using legitimate admin tools

Step 6: Harden Defenses Based on Results

- If exploitation was successful - mandate the immediate patching of all systems against MS17-010 and the disabling of SMBv1 protocol.
- If lateral movement was successful - advocate for strict network segmentation to isolate critical servers and subnets
- If detection was slow - push for the implementation of a NGFW/IPS to block exploit traffic at the network level

Step 7: Re-Test

- After patches and segmentation are in place, re-scan the network to confirm no vulnerable systems remain
- Attempt the attack again to verify that the lateral movement is now blocked and exploits are prevented

References

1. “WannaCry ransomware overview”, Malwarebytes, https://www.malwarebytes.com/wannacry
2. “What was the WannaCry ransomware attack?”, CloudFlare, https://www.cloudflare.com/ru-ru/learning/security/ransomware/wannacry-ransomware/
3. “What is WannaCry ransomware?”, Kaspersky, https://www.kaspersky.com/resource-center/threats/ransomware-wannacry
4. “What is WannaCry Ransomware? Does WannaCry still exists?”, Fortinet, https://www.fortinet.com/resources/cyberglossary/wannacry-ransomware-attack
5. “WannaCry: how the widespread ransomware changed cybersecurity”, IBM, https://www.ibm.com/think/x-force/wannacry-worm-ransomware-changed-cybersecurity
6. “NHS England business continuity management toolkit case study: WannaCry attack”, https://www.england.nhs.uk/long-read/case-study-wannacry-attack/