WannaCry

In May 2017, the world witnessed a brutal cyberattack. The WannaCry ransomware campaign paralysed services globally, exposing vulnerabilities and forcing a re-evaluation of our digital defences.

The Day the World Stood Still

May 12, 2017

A massive global ransomware campaign launched, impacting organizations across 150 countries within hours.

NHS Under Attack

One of the most severely affected networks was the UK's National Health Service, leading to cancelled appointments and critical disruptions to patient care.

Cybersecurity firm **FireEye** immediately began analysis, racing against the clock to understand the threat.

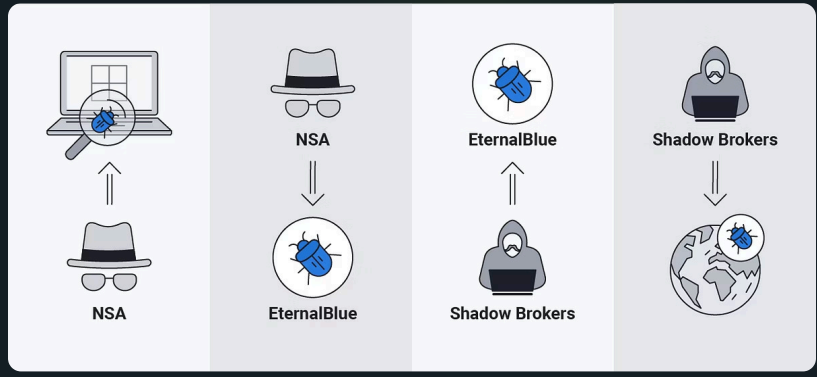
Stolen Tools

Shadow Brokers

- Claimed to have hacked the NSA
- Stealing a tone of sensitive cyber tools and exploits
- Released these powerful assets publicly.

EternalBlue

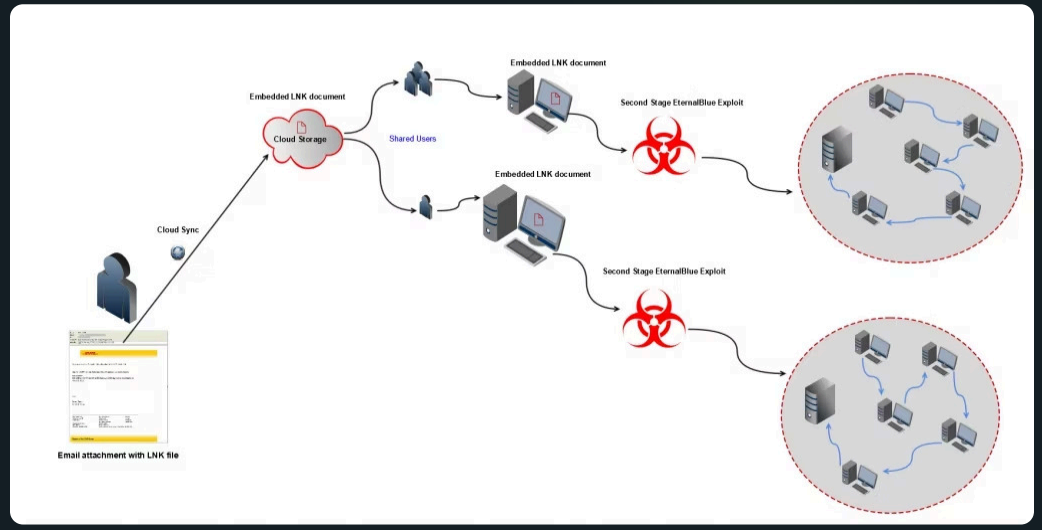
Among the leaked tools was "EternalBlue," an exploit that became the backbone of the WannaCry attack. It targeted a critical vulnerability, enabling rapid, widespread infection.



How EternalBlue Facilitated the Spread

EternalBlue exploited a significant flaw within the **Server Message Block (SMB)** protocol, commonly used for file sharing across Windows networks.

This vulnerability allowed WannaCry to behave like a worm, self-replicating and spreading automatically across vulnerable networks. A single infected PC could compromise an entire network in minutes.



The Unpatched Vulnerability

- Microsoft releasing a patch for the EternalBlue vulnerability months before the attack, but many organisations had not installed it.
- Highlight a persistent challenge in cybersecurity: the gap between patch availability and widespread implementation.

Windows XP & Legacy Systems

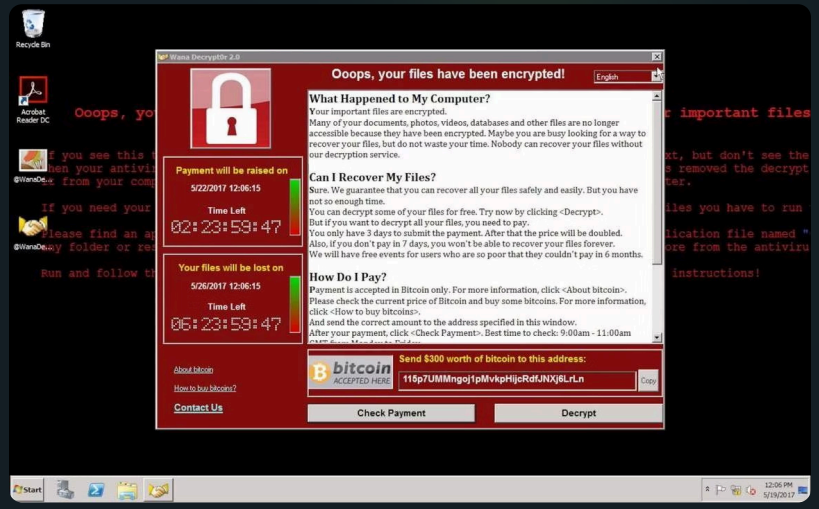
Compounding the problem, Windows XP, an operating system no longer supported by Microsoft, was highly vulnerable. In an unprecedented move, Microsoft released an emergency patch for XP just days after the attack began.

Lesson Learned:

Patch management is not optional; it is fundamental to cybersecurity.

Impact on the Computer

Once infected, WannaCry encrypts all files on the computer, rendering them completely inaccessible. A demanding message then appears on the screen, instructing victims to pay a ransom in Bitcoin to regain access to their valuable data.



It say that if you don't pay the ransom within the specified time frame will results in permanent data loss.

However, the malware has no built-in mechanism to actually decrypt the files, even if the ransom is paid.

A Kill Switch Discovered

WannaCry contained a **shutdown mechanism**. It was programmed to check for the existence of a specific URL. If this URL was active and responded, the ransomware would immediately stop its encryption activities.

This unintentional fail-safe became the key to halting its global rampage.

Marcus Hutchins

A 22-year-old British cybersecurity researcher, stumbled upon this critical domain within the malware's code.

Activating the Kill Switch

Realising it was unregistered, he promptly registered the domain, inadvertently activating the kill switch and preventing hundreds of thousands of further infections.

Global Impact

Hutchins' quick thinking turned him into an accidental hero, saving organisations billions in potential damages and recovery costs worldwide.

WannaCry's Devastating Reach

230,000

Computers Infected

Across 150 countries, rendering systems unusable and data inaccessible.

$140,000

Ransom Collected

Paid by approximately 330 victims in Bitcoin, a surprisingly low figure given the scale of the attack.

The true cost, however, extends far beyond the ransom, encompassing lost productivity, recovery efforts, and reputation damage.

Geopolitical Attribution

EU Sanctions

WannaCry was the first cyberattack to trigger EU sanctions against a country, setting a precedent for accountability..

Lazarus Group

UK and US intelligence linked WannaCry to the Lazarus Group, a North Korea-backed hacking organisation.

Key Takeaways & Moving Forward

1 Vigilant Patch Management

Applying security updates promptly is key to stopping known vulnerabilities.

2 Cyber Resilience

Organisations need strong incident response plans and regular backups to ensure fast recovery.

3 International Collaboration

Fighting global cyber threats demands coordination between governments, law enforcement, and cybersecurity experts.

4 User Awareness

Educating employees is vital — a vigilant workforce is the first defence against phishing and social engineering.

Question?

Feedback?

Sources

- https://en.wikipedia.org/wiki/WannaCry_ransomware_attack
- https://any.run/malware-trends/wannacry/
- https://darknetdiaries.com/episode/73/ (44:51 minutes)