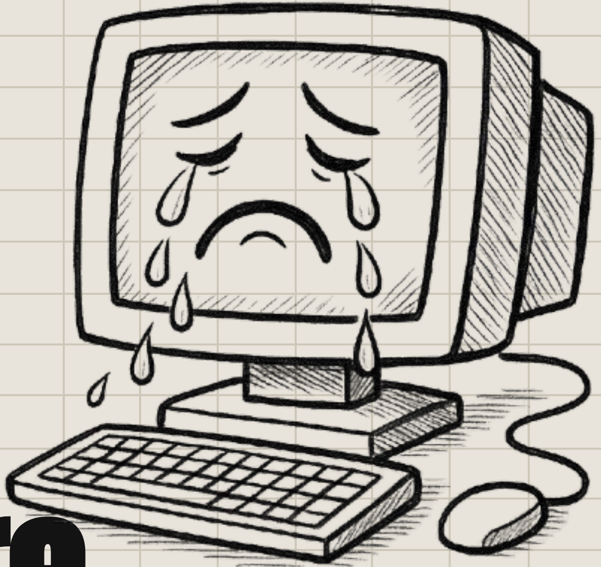
Pelumi | Gene | Shan | Tch | Anth

Welcome to LuGESTA NEWS where WannaCry makes your PC cry… but this presentation won't

WannaCry Ransomeware Attack



L

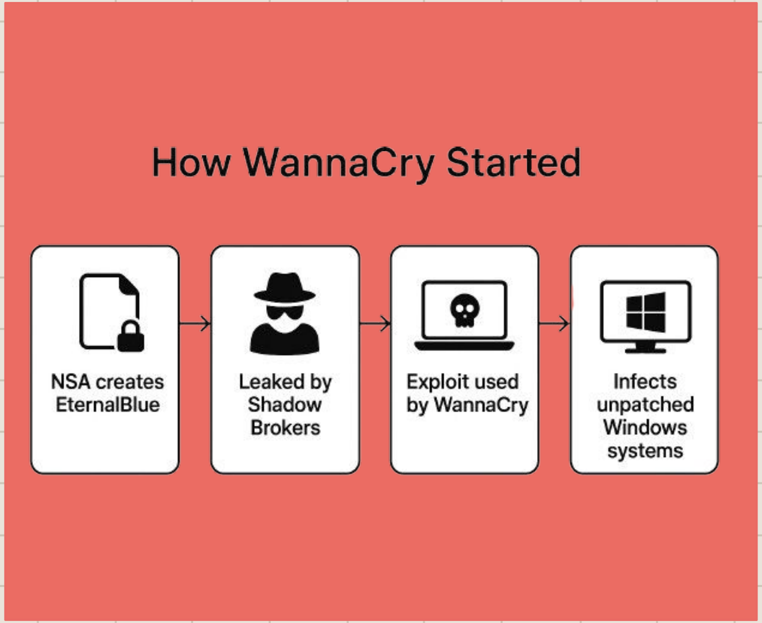
G

WannaCry Ransomware Attack

- Ransomware cryptoworm that encrypts files and demands Bitcoin ransom.
- Occurred in **May 2017** as a global cyberattack.
- Spread via **EternalBlue exploit** in Windows.
- Exploit was leaked by **Shadow Brokers**.
- Hit **unpatched and outdated systems**.

Spread

- Began **07:44 UTC, May 12, 2017**.
- **Encrypted files**, demanded Bitcoin.
- Damages: **Hundreds of millions to billions**.
- Believed origin: **North Korea**.
- **2018 variant** hit **TSMC** (10,000 machines infected).



How WannaCry Started

NSA creates EternalBlue → Leaked by Shadow Brokers → Exploit used by WannaCry → Infects unpatched Windows systems

Infected system

Alias

Transformations:

- Wanna → Wana
- Cryptor → Crypt0r
- Cryptor → Decryptor
- Cryptor → Crypt → Cry
- Addition of "2.0"

Short names:

- Wanna → WN → W
- Cry → CRY

Losses

Up to US$4 billion

Suspects

Lazarus Group

Convicted

None

Type: Worm

Subtype

Ransomware

Origin

Pyongyang, North Korea (not confirmed)

Technical details

Platform : Microsoft Windows

Filename: `mssecsvc.exe`

Size: 3.64 MB

Ports used: Server Message Block

Abused exploits: CVE-2017-0145

Written in: Microsoft Visual C++ 6.0

Cyberattack event

Date: 12 May 2017 – 15 May 2017 (initial outbreak)

Location: Worldwide

Theme: Ransomware encrypting files with US$300–600 demand (via Bitcoin)

Outcome: 300,000+ computers infected

HOW DID IT STOP??!!!

Key Actions That Stopped WannaCry

CRY NO MORE!!

Discovery of a Kill Switch Domain

- ○ A cybersecurity researcher, Marcus Hutchins, found a domain name embedded in the malware’s code.

- ○ When he registered the domain, it acted as a "kill switch," stopping the ransomware from spreading further.

Design your network to resist lateral movement from the start.

Emergency Patching by Microsoft

- Microsoft released critical patches for supported systems via security bulletin MS17-010.

- They also took the rare step of issuing patches for unsupported systems like Windows XP, Windows 8, and Windows Server 2003 to curb the outbreak.

Wanna Cry?
WannaCry
The Nightmare for Vulnerable Windows Systems
WANNA CRY?
YOUR PERSONAL FILES ARE ENCRYPTED
YOUR PERSONAL FILES ARE ENCRYPTED
Make payment or private key will be destroyed in

Network Segmentation and Shutdowns

- Affected organizations isolated infected machines and shut down vulnerable systems to prevent lateral movement.

- Some hospitals and companies temporarily went offline to contain the damage.

ADVICE: 🧱 **Segment your network** to isolate critical systems and limit malware spread.

Public Education, Global Awareness and Response

- Widespread media attention helped raise awareness about the vulnerability and the importance of applying patches.
- Rapid sharing of threat intelligence among cybersecurity communities helped organizations defend against further infections.
- Antivirus vendors updated their definitions to detect and block WannaCry variants.

WHO WAS RESPONSIBLE? (The chain)

01. **NSA (U.S. NATIONAL SECURITY AGENCY**

A U.S. government agency that creates cyber tools for intelligence and defense. Created the EternalBlue

02. **Shadow Brokers**

A mysterious hacker group known for leaking stolen cyber weapons. Hackers who leaked EternalBlue

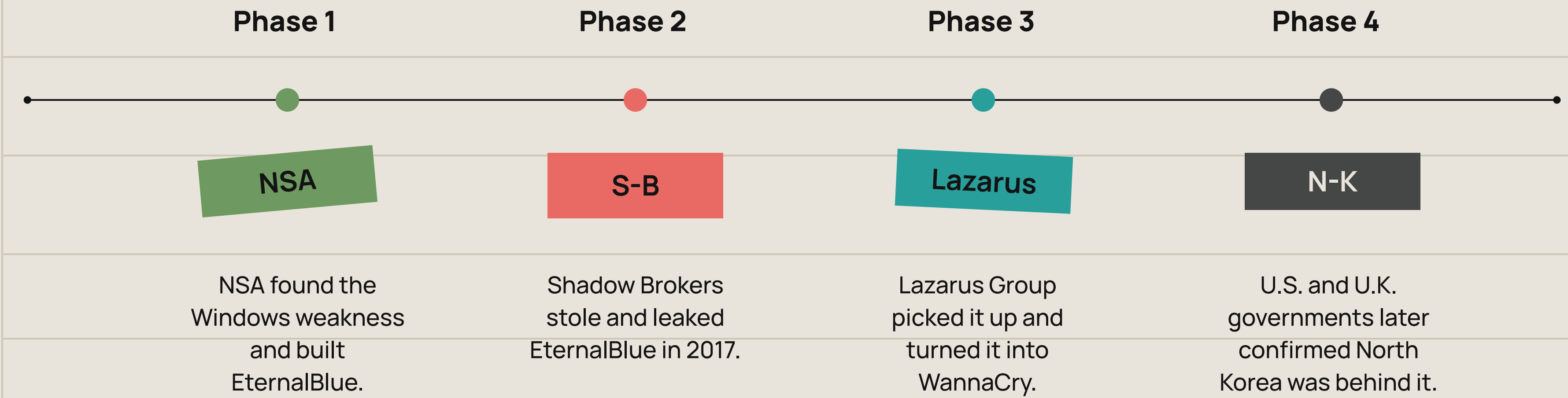
03. **Lazarus GROUP**

A North Korean state-sponsored hacking team linked to major global cyberattacks. North Korean hackers who used EternalBlue

04. **North Korea**

The country behind state-sponsored hackers like Lazarus Group, often using cyberattacks to fund the government or cause disruption. Government backing Lazarus group

TIMELINE



Phase 1

NSA

NSA found the Windows weakness and built EternalBlue.

Phase 2

S-B

Shadow Brokers stole and leaked EternalBlue in 2017.

Phase 3

Lazarus

Lazarus Group picked it up and turned it into WannaCry.

Phase 4

N-K

U.S. and U.K. governments later confirmed North Korea was behind it.

Prevention Strategies

Timely Patching and Updates

Air Gapping

Educate Users

Use Strong Endpoint Protection

- Apply updates as soon as they're released to fix known vulnerabilities.
- Isolate critical systems to prevent malware from spreading laterally.
- Train staff to spot phishing and suspicious activity even if WannaCry didn't use phishing, others do.
- Deploy antivirus tools to detect and block threats early.

Prevention Strategies

Limit Access

Disable Unused Services

Plan for Incidents

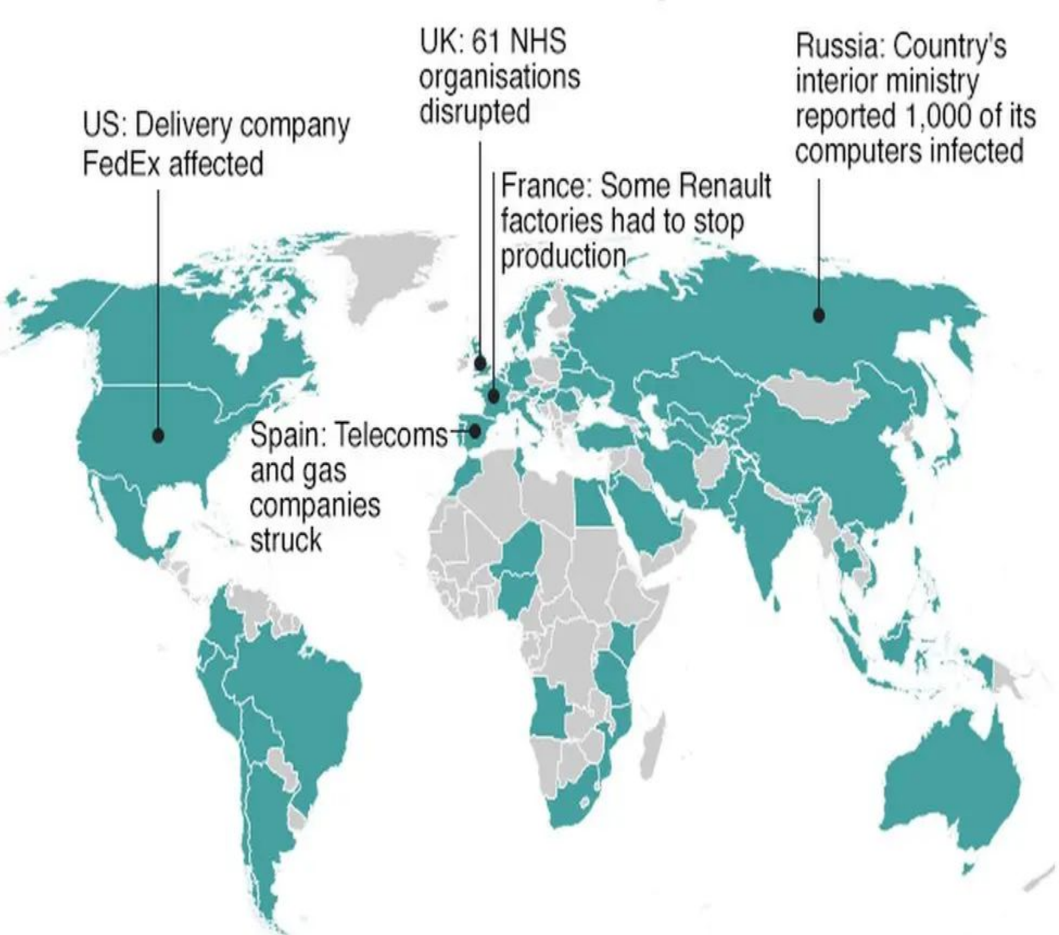
Monitor Threats

- Apply least privilege principles and monitor privileged accounts.
- Turn off legacy devices to reduce attack surfaces. Extremely old, out-of-date Windows systems were at risk.
- Have a tested response plan ready to contain and recover from attacks.
- Use threat intelligence and log analysis to stay ahead of emerging risks.

Global Impact

200,000 computers in 150 countries

The WannaCry ransomware, which hit in May 2017, caused an estimated $4 billion to $8 billion in global financial losses, primarily from business interruption and remediation costs.


US: Delivery company FedEx affected
UK: 61 NHS organisations disrupted
France: Some Renault factories had to stop production
Russia: Country's interior ministry reported 1,000 of its computers infected
Spain: Telecoms and gas companies struck

COUNTRIES IMPACTED THE MOST

- **Russia**: Hardest hit – govt, banks, rail, Megafon.
- **Germany**: Train boards hit, trains fine.
- **S. Korea**: Cinema ads hit, 9 cases
- **UK**: NHS (61 orgs), Nissan factory.

Spain: Telefonica, power firms.

France: Renault halted, resumed.

Japan: 2k PCs/600 firms (Hitachi delays).

China: 30k+ orgs, universities, petrol stations.

Indonesia: Hospitals locked out.

India: Police, firms hit; govt patched.

USA: FedEx disrupted.

Ireland: 3 hospitals, minor.

Australia: 3 SMEs.

.

WannaCry Impact – Conclusion

- **Global scale**: 150+ countries, hundreds of thousands of systems hit
- **Critical sectors**: Healthcare, transport, telecom, manufacturing most disrupted
- **Main cause**: Outdated & unpatched Windows systems
- **Financial loss**: Billions in damages, ransom payments minimal
- **Lesson learned**: Importance of regular updates, backups, and cyber awareness
- **Aftermath**: Sparked major push for stronger cybersecurity & patch management

TIME TO CRY!!!!

1. What vulnerability did the WannaCry ransomware exploit to spread across Windows systems?

- BlueKeep
- EternalBlue
- Heartbleed
- Shellshock

2. Which organization was believed to be behind the WannaCry ransomware attack?

- APT28
- Anonymous
- Shadow Brokers
- Lazarus Group

3. What action helped stop the spread of the WannaCry ransomware?

- Disabling internet access
- Rebooting infected systems
- Registering a kill switch domain
- Installing antivirus software

4. Approximately how many computers were infected during the WannaCry ransomware attack?

- 100,000
- 30,000
- 300,000
- 1 million

5. What was the typical ransom amount demanded by WannaCry?

- $300 to $600
- $1,000
- $5,000
- $100

6. Which operating system was primarily targeted by WannaCry?

- macOS
- Microsoft Windows
- Linux
- Android

7. What was the filename of the WannaCry executable?

- wannacry.exe
- ransomware.exe
- mssecsvc.exe
- cryptoworm.exe

8. Which protocol did WannaCry abuse to spread across networks?

- SMTP
- HTTP
- FTP
- SMB

9. Which cybersecurity researcher helped stop WannaCry by activating its kill switch?

- Marcus Hutchins
- Brian Krebs
- Edward Snowden
- Kevin Mitnick

10. What emergency action did Microsoft take in response to WannaCry?

- Disabled SMB protocol globally
- Issued updates for unsupported systems like Windows XP
- Released patches only for Windows 10
- Removed EternalBlue from all systems