WannaCry Attack Case Study

150 Countries / 200,000 Computers

Samuel Soh

21st July 2021

Attack Category: RansomWare

The WannaCry ransomware attack targeted computers running the Microsoft Windows Operating System by encrypting data and demanding ransom payments in Bitcoins.

Research:

Wikipedia: https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

The 4 days attack affected more than 200,000 computers across 150 countries, resulting in damages of millions to billions of dollars.

The attack began on Friday, 12 May 2017 in Asia at 07:44 UTC, with the initial infection likely through an exposed vulnerable SMB port. Within a day the code was reported to have infected more than 230,000 computers in over 150 countries.

Organizations that had not installed Microsoft's security update from April 2017 were affected by the attack. Those still running unsupported versions of Microsoft Windows, such as Windows XP(, Windows 7) and Windows Server 2003 were at particularly high risk because no security patches had been released since April 2014 for Windows XP (with the exception of one emergency patch released in May 2014) and July 2015 for Windows Server 2003.

Timeline

1 07:44 UTC, Friday, 12 May 2017
Initial infection in Asia

2 15:03 UTC, Friday, 12 May 2017
Halted by registering of kill switch discovered by Marcus Hutchins

3 Saturday, 13 May 2017
Microsoft release out-of-band security updates for EOL Windows products

4 Sunday, 14 May 2017
First variant of WannaCry appear and kill switch discovered by Matt Suiche

5 Monday, 15 May 2017
Second and Third variant of WannaCry appear and kill switch discovered by CheckPoint

6 December 2017
US and UK asserted that North Korea was behind the attack

Vulnerabilities

Key findings:

Security loophole in Microsoft Windows end of life products were exploited

Vulnerability #1

Microsoft Windows security updates were not installed

Vulnerability #2

NSA lost of control over its cyber intelligence tool i.e. EternalBlue

Vulnerability #3

Network security of service ports i.e. SMB were not monitor appropriately

Costs

- Most affected countries are Russia, Ukraine, India and Taiwan
- Largest agency affected is National Health Service hospital in England and Scotland
- Nissan Motor Manufacturing UK and Renault halted production to stop the spread
- Economic loss from the cyber attack could range from hundreds of millions to US$4 billion

Prevention

- Regular, secure backups
- Isolating critical systems
- Install latest security patches
- Having appropriate anti-malware tools