WannaCry Global Attack – May 2017

IST623 – Group Project

Lauren Foltz
Brandon Galloway
Eugene Lee
Laurel Moczydlowski

Table of Contents

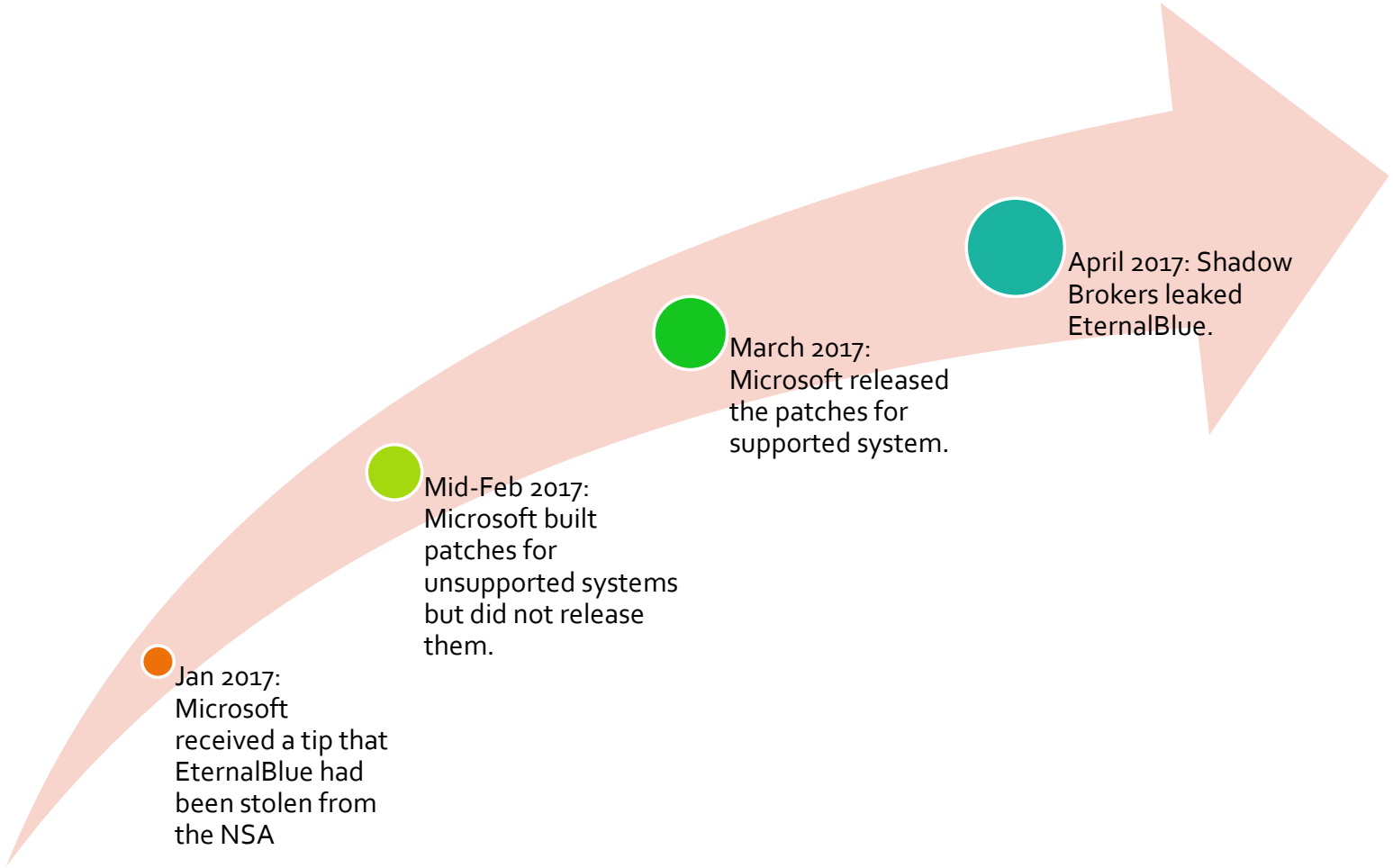
What is WannaCry

WannaCry is malicious software which will covertly encrypt files. It is a type of malware called **Ransomware**.

The **uniqueness** of WannaCry is that it is able to identify vulnerable targets on the local network and spread that way as well. This behavior is typically classified as a **worm.**

WannaCry combined both techniques and led to a wider impact.

Timeline Leading up to WannaCry



How the attack spread

Friday May 12th , 2017 – 3:24 AM EST

1. First infected computer struck, this quickly spread to Telefonica in Spain.

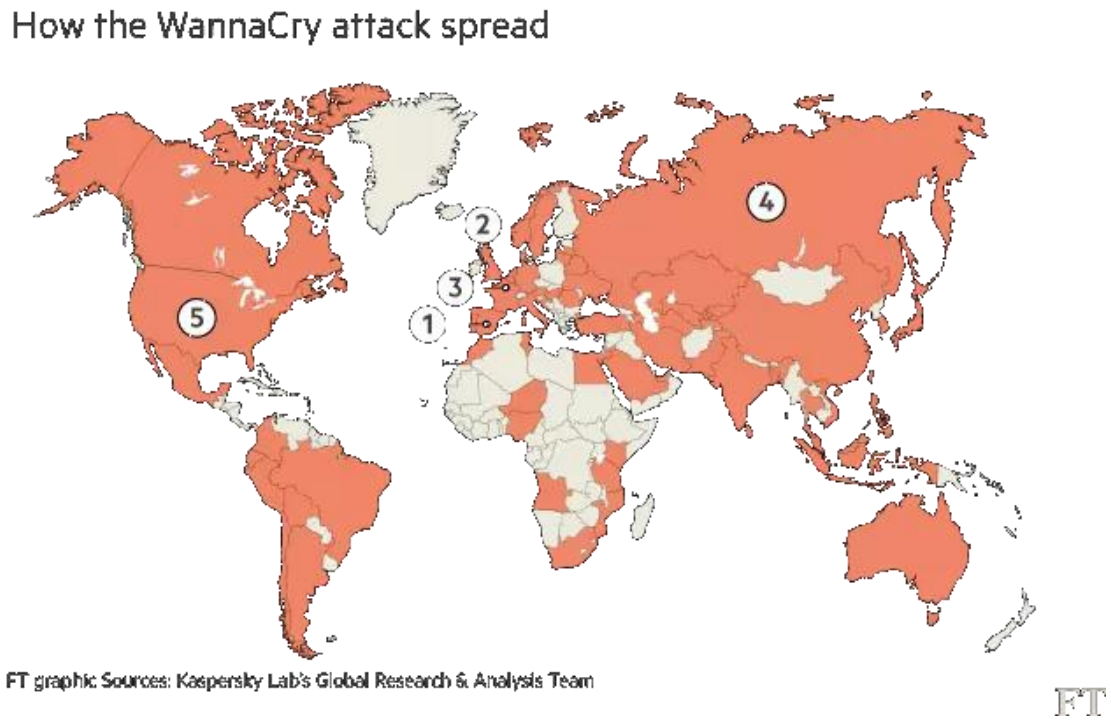
2.6:00 AMThe attack quickly spread to the UK attacking hospitals and clinics.

3.Renault in France, and Deutsche Bahn in Germany were attacked next.

4. Russia was the next country to be impacted, including the Ministry of the Interior, MegaFone, Sberbank.

5. Finally the US was hit, FedEx being one of the major organizations impacted. (Jones, 2017)

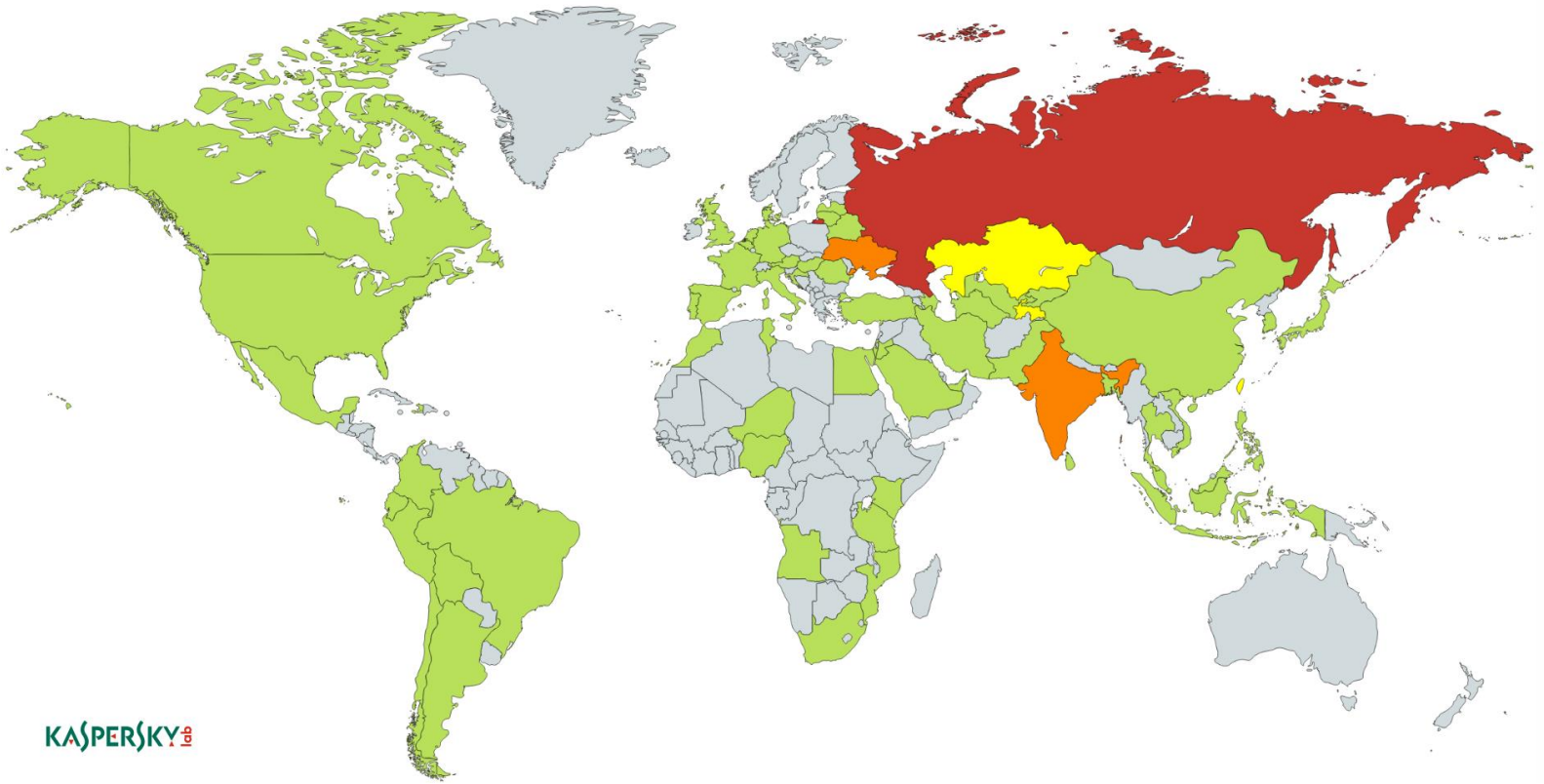
By the afternoon on May 12th , a 22 year old researcher Marcus Hutchins found a way to slow the spread of the infection. Microsoft released a patch later that evening and an additional security update on the 13th for it's other platforms. (Hayden, 2017)



Source: Financial Times (Jones, 2017)

Who was impacted?

150 countries



Who was Impacted?

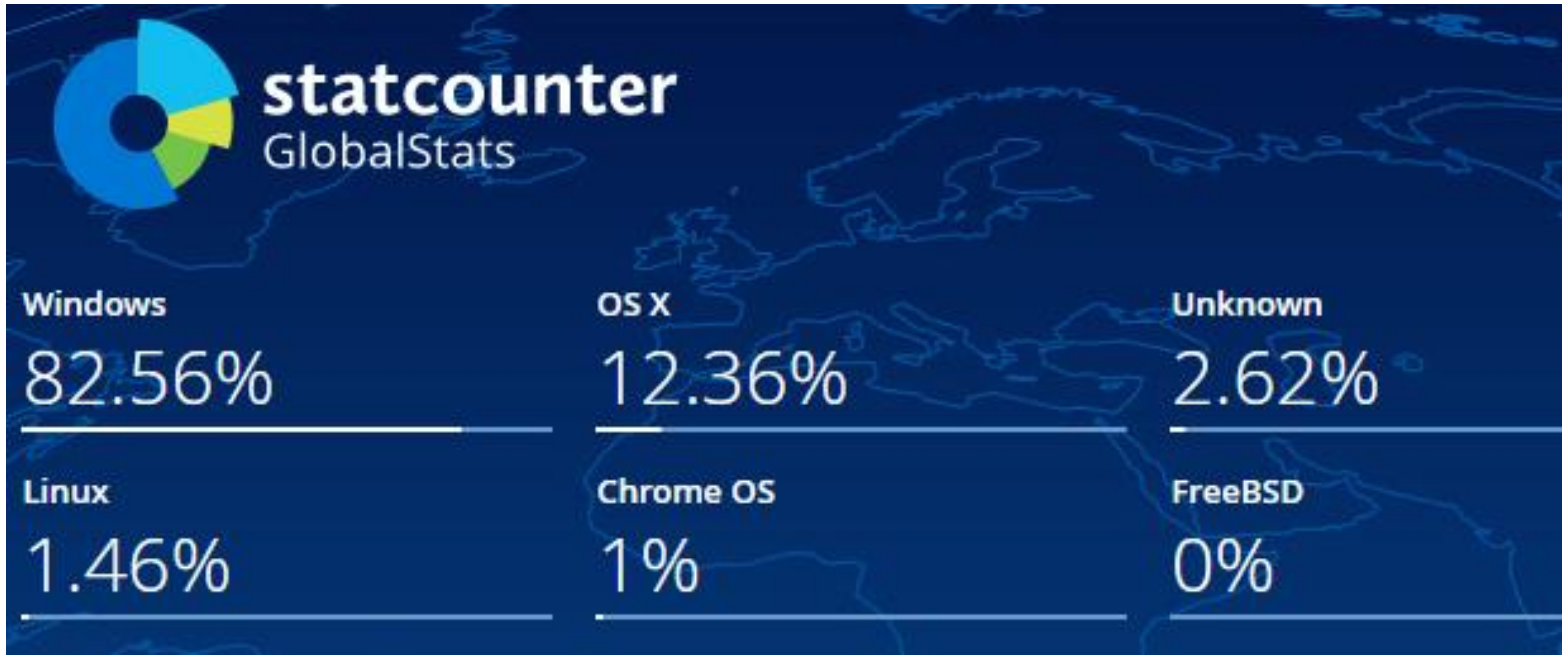
~ 300,000 computers infected worldwide

Who was Impacted?

Vulnerable Systems

- Only systems running Windows were vulnerable to the MS-17-010 bug.
- Windows market share for desktops/laptops below

  (doesn't include servers or supercomputers).



Who was Impacted?

Vulnerable Windows Software

3/14 Patch Available

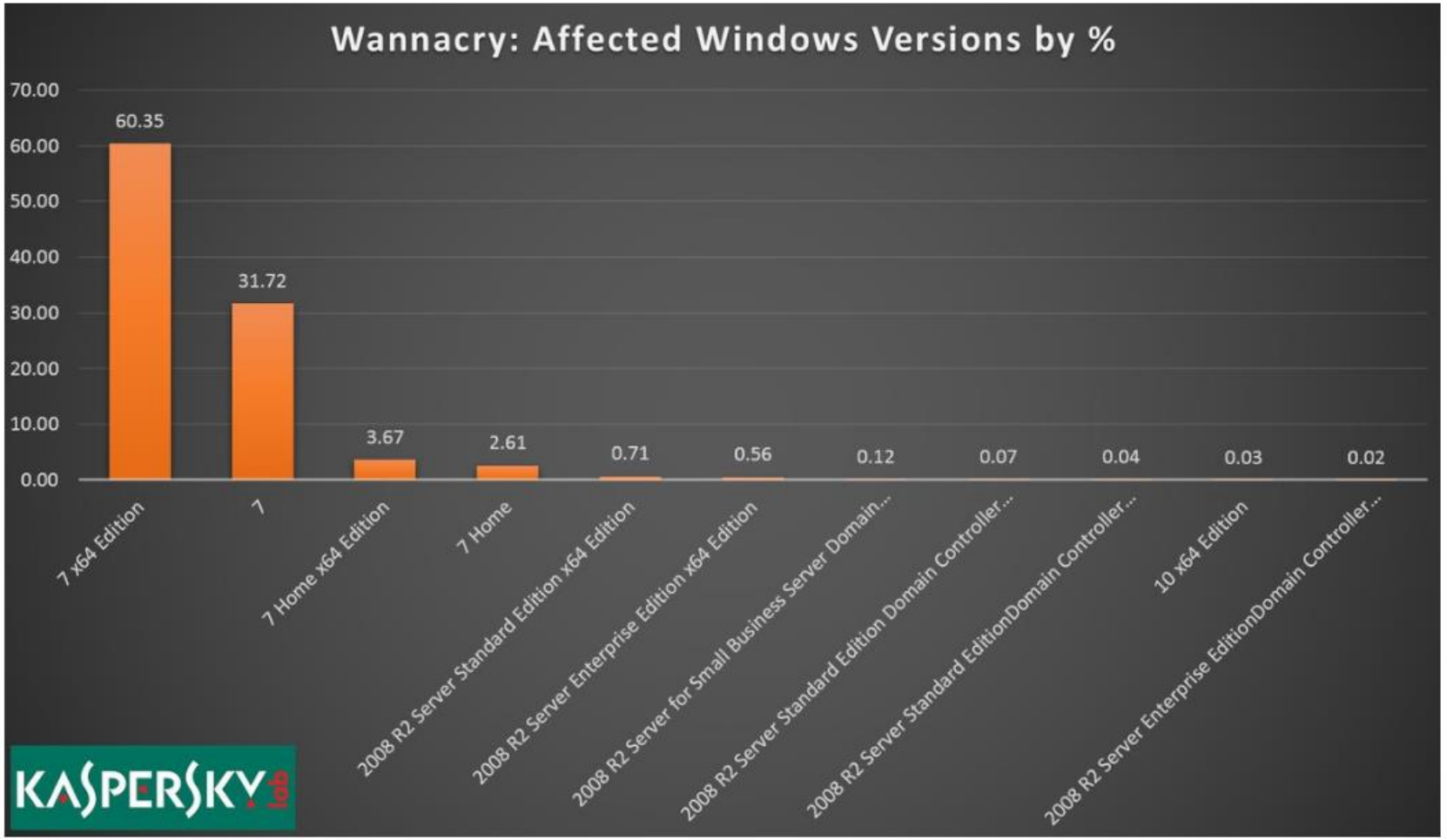
- Windows Vista
- Windows 7
- Windows 8.1
- Windows 10
- Windows Server 2008
- Windows Server 2012
- Windows Server 2016

3/14 Patch NOT Available

- Windows XP
- Windows 8
- Windows Server 2003

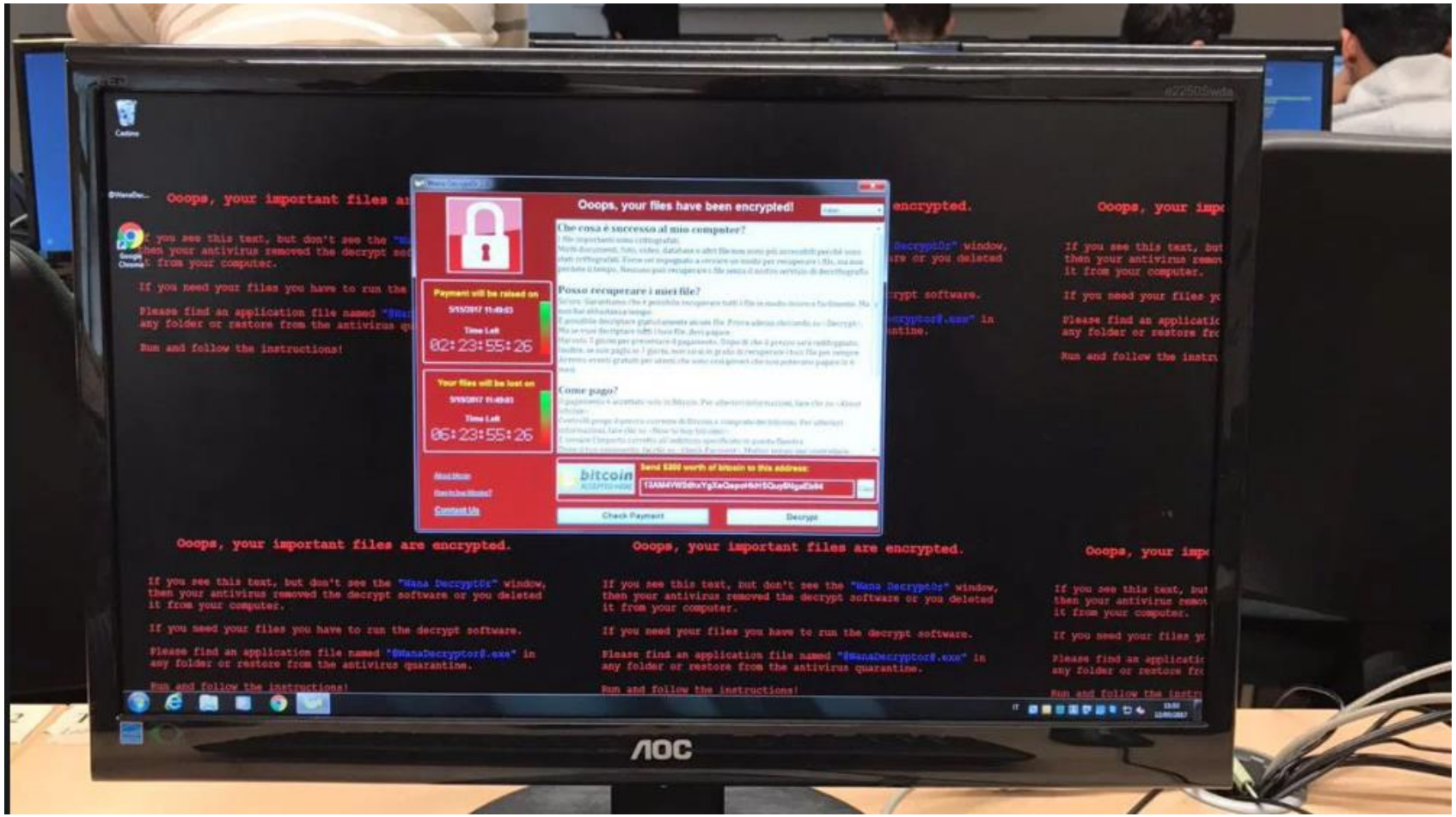
Who was impacted?

Actual Systems Infected



What was the immediate impact?

Interruption to Operations

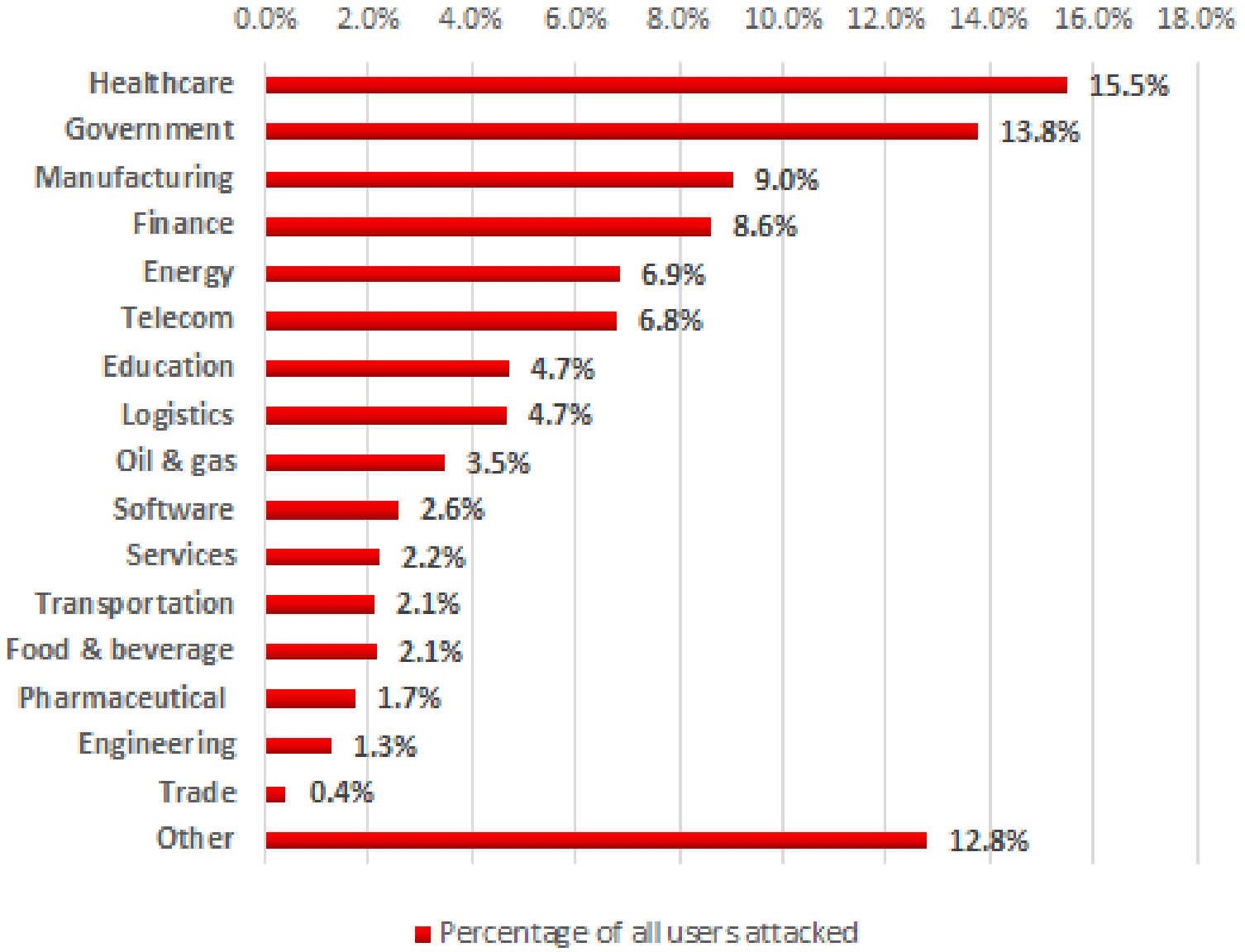


What was the immediate impact?

Security Property: Availability

Who was impacted?

Industries



Remediation and Recovery

Technical Details

- Operating Systems Affected (XP, 7, 2003, 2008)
- Enters organizations and spreads throughout using SMB (Port 445 & 139)
- Encrypts files accessible to machine using AES 128 & Deletes shadow copies
- Checks IP address & scans network for other vulnerable targets
- System attempts to contact “home-website”.

Remediation and Recovery

Recovery

- UK researcher paused outbreak by registering "home-website" domain

- Web-proxies continued to allow spread

- MS released MS17-010 update updating how remote code execution is handled in SMBv1 for supported operating system March 14

- MS released update on May 15 for out-of-support operating systems (Very Rare)

Remediation and Recovery

Avoidance

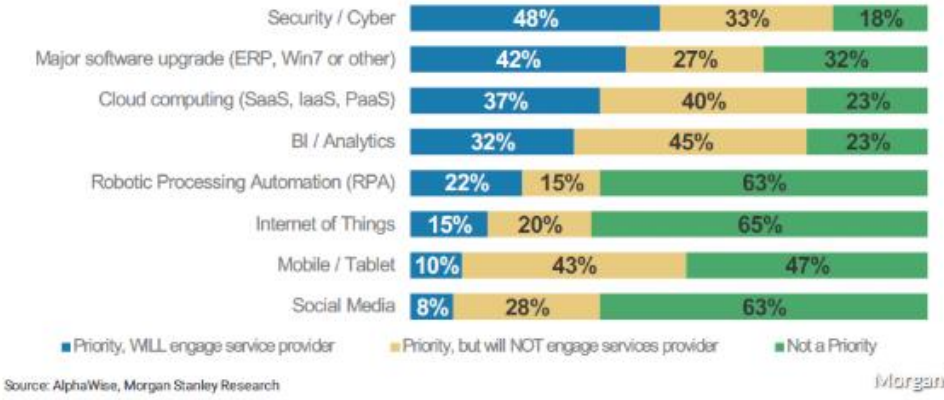
- Keep Servers & Workstations updated
- Stay within product lifecycles
- Ensure Antivirus has Ransomware module
- Follow best-practice when configuring firewall
- Practice Principal of Least Permission

Long-Term Effects

- People
  - Social Engineering
  - Stronger Governance around systems
  - New DHS Cyber Hub
- Process
  - Patching
  - External audits and company
- Technology
  - Edge Protection- IDS/SIEM/DLP/Firewall
  - Servers/Desktops - Anti Virus/Malware Scanning/Encryption

Exhibit 55: Priority Initiatives in 2018

Key Initiatives in 2018



Source: AlphaWise, Morgan Stanley Research

Morgan Stanley

Conclusion and Reflections

The initial attack was in May however the exploit was originally discovered by the NSA and later stolen in January 2017 which eventually led the WannaCry Global attack.

Over 150 countries were impacted and over 300,000 computers world wide.

The majority of systems that were impacted were Windows Devices. Of those Windows machines the largest group infected were Windows 7 x64 operating systems.

September 6, 2018 a North Korean programmer, Park Jin Hyok, was charged by the US Department of Justice as being a part of the WannaCry attack amongst several other well known attacks.

Interesting Facts

- The original remediator of the virus Marcus Hutchins later admitted to writing the Kronos Baking Malware.
- The original exploitation originated from the NSA, which wasn't shared upon initial discovery.

Questions?

References

- Cellan-Jones, R. (2017, -05-13). Massive cyber-attack hits 99 countries. *BBC News* Retrieved from https://www.bbc.com/news/technology-39901382
- Cellan-Jones, R. (2018, -05-16). NHS cyber-hero 'discussed bank hack role'. *BBC News* Retrieved from https://www.bbc.com/news/technology-44139467
- Cimpanu, C. (2018). How US authorities tracked down the north korean hacker behind WannaCry. Retrieved from https://www.zdnet.com/article/how-us-authorities-tracked-down-the-north-korean-hacker-behind-wannacry/
- Customer guidance for WannaCrypt attacks. (2017). Retrieved from https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

References

- EY. (2017, May). *"WannaCry" Ransomware Attack Technical Intelligence Analysis.* Retrieved from EY: https://www.ey.com/Publication/vwLUAssets/ey-wannacry-ransomware-attack/$File/ey-wannacry-ransomware-attack.pdf
- Greenberg, A. (2017, -04-14T15:42:27.000Z). Major leak suggests NSA was deep in middle east banking system. *Wired,* Retrieved from https://www.wired.com/2017/04/major-leak-suggests-nsa-deep-middle-east-banking-system/
- Hayden, M. E. (2017). How the WannaCry cyberattack spread. Retrieved from https://abcnews.go.com/US/timeline-wannacry-cyberattack/story?id=47416785
- Jones, S. (2017). Timeline: How the WannaCry cyber attack spread. Retrieved from https://www.ft.com/content/82b01aca-38b7-11e7-821a-6027b8a20f23
- Malware, described in leaked NSA documents, cripples computers worldwide. (2017). Retrieved from https://www.washingtonpost.com/world/hospitals-across-england-report-it-failure-amid-suspected-major-cyber-attack/2017/05/12/84e3dc5e-3723-11e7-b373-418f68849a004_story.html
- McNeil, A. (2017, May 19). *How did the WannaCry ransomworm spread?* Retrieved from Malwarebytes: https://blog.malwarebytes.com/cybercrime/2017/05/how-did-wannacry-ransomworm-spread/

References

- Microsoft. (2017, October 11). *Microsoft Security Bulletin MS17-010 - Critical*. Retrieved from Microsoft: https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2017/ms17-010
- Rouse, M. (2018). *principle of least privilege (POLP)* . Retrieved from TechTarget: https://searchsecurity.techtarget.com/definition/principle-of-least-privilege-POLP
- Shaikh, R. (2018, -05-16T10:07:36-04:00). WannaCry hero allegedly admitted to writing kronos malware code. Retrieved from https://wccftech.com/wannacry-hero-writing-kronos-banking/
- Simulated ransomware attack shows vulnerability of industrial controls. (2017).
- Thomson, I. (2017). While microsoft griped about NSA exploit stockpiles, it stockpiled patches: Friday's WinXP fix was built in february. Retrieved from https://www.theregister.co.uk/2017/05/16/microsoft_stockpiling_flaws_too/
- Wannacry timeline: How it happened and the industry response to ransomware attack. (2017). Retrieved from https://www.healthcareitnews.com/news/wannacry-timeline-how-it-happened-and-industry-response-ransomware-attack

References

- WannaCry: Are you safe? (2017, May 12). Retrieved from https://www.kaspersky.com/blog/wannacry-ransomware/16518/
- Ashkenas, J. & Pearce, A. (2017, May 12). Animated Map of How Tens of Thousands of Computers Were Infected With Ransomware. Retrieved from https://www.nytimes.com/interactive/2017/05/12/world/europe/wannacry-ransomware-map.html
- Price, D. (2018, March 27). The True Market Shares of Windows vs Linux Compared. Retrieved from https://www.makeuseof.com/tag/linux-market-share/
- Cimpanu,C. (2017, May 20). Over 90% of All WannaCry Victims were Using Windows 7. Retrieved from https://www.bleepingcomputer.com/news/security/over-98-percent-of-all-wannacry-victims-were-using-windows-7/
- Threat Landscape for Industrial Automation Systems in H1 2017. (2017, September 28) Retrieved from https://ics-cert.kaspersky.com/reports/2017/09/28/threat-landscape-for-industrial-automation-systems-in-h1-2017/
- Wattles, J. and Disis, J. (2017, May 15). Ransomware attack: Who's been hit. Retrieved from https://money.cnn.com/2017/05/15/technology/ransomware-whos-been-hit/index.html