Wander Barnes

Dr. Brandon C. Strubberg

TCID 4080

September 30th, 2025

Case Study: Wannacry (2017) and the NHS

Introduction

In May 2017, suddenly a new worldwide ransomware worm appeared. From May 15th-17th, it was estimated that over 230,000 computers were affected worldwide. The worm used an NSA-created exploit called EternalBlue. Microsoft patched this vulnerability in supported systems; however, not all administrators updated their systems. The worm quickly spread. Within a day, Microsoft released patches for unsupported systems. Cybersecurity expert Marcus Hutchins found the kill switch solution and helped to slow the spread. Due to the work Hutchins did and other researchers' efforts, further variations were slowed, and the main attack was considered to have ended after 4 days.

The financial impact was estimated to be up to 4 billion dollars due to encrypted files as well as the impact on work. The NHS in the UK was heavily affected, with over 70,000 devices. This included computers, MRI machines, blood-storage equipment, and more.

Background

EternalBlue

Wannacry's beginnings started in 2012 when EternalBlue, an exploit for Windows machines, was developed by the NSA. It was kept for over 5 years until it was stolen and released by a hacker group called the Shadow Brokers (Nakashima and Timberg). EternalBlue worked by targeting the Microsoft Server Message Block (SMB) to send messages designed to execute remote code. This vulnerability impacted many Windows types

Supported by Microsoft at the time (March 2017)

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

Systems with Emergency Patches Released (May 2017)

- Windows XP

- Windows 8
- Windows Server 2003

Who Made WannaCry

Investigators suspect the Lazarus Group, a hacker group, orchestrated the WannaCry attack. This group is widely believed to be connected to and run by the North Korean government; however, its exact size remains unknown. Lazarus has a history of executing high-profile operations:

- Sony Pictures Hack (2014)
- Bangladesh Bank Cyber Heist (2016)
- WannaCry (2017)
- AstraZeneca Attacks (2020)

Wannacry in the Wild

Release and Infection

WannaCry launched on May 12, 2017. While the initial point of origin remains unknown, the worm infected over 230,000 computers within a day. This rapid, worm-like spread was unprecedented as it was not user inflicted. Unlike many worms, no emails were sent, or user action taken. It automatically scanned for and attacked vulnerable machines using the SMB messages. WannaCry leveraged the potent EternalBlue exploit for its deep-cutting intrusions and paired it with the DoublePulsar backdoor, which allowed the worm to secretly install and execute its code on compromised systems. Microsoft had released a patch in March however many systems did not receive it which allowed for Wannacry's quick spread. Most computers targeted were Windows 7 machines surprisingly. This aggressive self-propagation caused worldwide panic, bringing massive systems like the UK's National Health Service (NHS) to a halt.

Infection Stopped

Cybersecurity researcher Marcus Hutchins discovered the kill switch domain. He had been reverse-engineering the malware's code and found it contained an odd, convoluted domain name it attempted to contact (iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com). This domain was the kill switch in which if Wannacry received a response from the domain, it stopped. With this initial action by Marcus Hutchins, helped along with other researchers bring the first and largest wave to a halt. Later waves came out but were quickly stamped out. Sadly, already encrypted computers did not benefit from this, but it prevented further infections.

Impacts of Wannacry

The WannaCry attack delivered an enormous global impact. The financial damages are estimated to be up to $4 billion dollars (Berr). This is due to the massive disruption to many businesses like the NHS where over 70,000 devices were compromised such as heart monitors. This resulted in the cybersecurity industry getting better idk.

Communication

Looking at Wannacry from a communication standpoint, it was very unorganized and chaotic. This was due to a lot of factors but such as the infection starting suddenly and the initial cause of which was not known. Unlike the CrowdStrike situation, where it was easy for Crowdstrike to send out information. Communication to the public came from induvial affected companies to the public.

The most effective strategy was the rapid, transparent information sharing among cybersecurity researchers. The immediate efforts of Marcus Hutchins and other experts, who quickly reverse-engineered the malware and publicized the kill switch, were critical. From a public relations standpoint, Microsoft's quick decision to release emergency patches for unsupported operating systems (like Windows XP) showed proactive leadership and helped mitigate further damage, sending a clear message about the necessary protective action.

A primary gap was the lack of unified, authoritative voices from governments or major international organizations to guide the public. This allowed confusion to spread rapidly. Internally, a key flaw was the failure of many IT departments to effectively communicate the urgency of the MS17-010 patch to administrators' months earlier, which was a fundamental lapse in technical-to-organizational communication (SentinelOne). The main risk that emerged was public distrust in organizations that continued to run critical services on outdated, vulnerable systems, revealing a significant weakness in digital infrastructure management.

Looking at a specific organization's response, the NHS was one of the highest impacted organizations. Although the attack did not directly target the health service, the NHS in England became one of the biggest casualties (Ghafur et al.). The disruption was immense: over 600 organizations were affected, including 34 infected hospital trusts (hospital organization) and 46 affected trusts that reported disruption from preventative action or shared systems (Ghafur et al.). This resulted in the inability to access patient records and charts, and some medical devices.

The analysis of patient activity reveals the severity of the attack on infected hospitals (Ghafur et al.):

- Total admissions saw a 6% decrease, which included a 9% reduction in elective admissions.
- Accident and emergency departments recorded 6% fewer attendances.
- Infected trusts had an average of 50% more appointment cancellations per day than non-infected trusts, resulting in approximately 13,500 cancelled appointments overall during the event.

While there was no statistically significant change in patient mortality, the total economic value of the lower activity at infected trusts alone was estimated at **£5.9 million.** This outcome forcefully revealed the critical risk of running clinical services on legacy platforms and, most importantly, showed that **none of the affected** NHS organizations had followed NHS Digital's advice to apply the necessary Microsoft update patch months earlier (Ghafur et al.).

During the crisis the NHS had to concurrently manage a crisis and update its stakeholders, often leading to delayed and inconsistent information for employees, customers, and the public. A lot of their communication was done after the fact by a couple of days.

Conclusion

The WannaCry ransomware worm of May 2017 stands as a watershed moment, the "perfect storm" that became the most damaging cyberattack the world had seen to date [5]. The crisis was not simply a technical event but a stark exposure of organizational complacency and systemic failure across the world. Its unprecedented spread was fueled by two factors: the rapid deployment of the powerful, state-developed EternalBlue exploit and the widespread, negligent failure of organizations to implement a critical patch released by Microsoft months earlier. This demonstrated that a known risk, when combined with institutional inertia, can quickly transform into a $4 billion global catastrophe.

This case analysis has shown the tangible consequences of this failure, particularly within critical infrastructure. The NHS case study provided quantifiable proof that cybersecurity negligence directly compromises patient care, resulting in a 9% reduction in elective admissions and 13,500 cancelled appointments due to reliance on vulnerable legacy systems (Ghafur et al.).

Ultimately, WannaCry was a "huge wake up call" for enterprise leadership, forcefully raising the awareness of cybersecurity risk from an IT concern to a core business imperative (Gregory). The event's enduring legacy is the resultant shift toward increased collaboration, prioritizing preparedness, and focusing on building "muscle memory" within incident response teams (Gregory). To mitigate future attacks of this magnitude, organizations must view digital resilience as a continuous requirement for public safety. This necessitates not only institutionalizing mandatory patch management protocols but also developing robust communication strategies that empower employees to act confidently when the next unexpected crisis occurs.

Citations

Berr, Jonathan. ""WannaCry" Ransomware Attack Losses Could Reach $4 Billion." *Cbsnews.com*, 16 May 2017, www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/.

Cloudflare. "What Was the WannaCry Ransomware Attack?" *Cloudflare*, www.cloudflare.com/learning/security/ransomware/wannacry-ransomware/.

GeeksforGeeks. "What Is WannaCry and How Does WannaCry Ransomware Works." *GeeksforGeeks*, 8 June 2017, www.geeksforgeeks.org/blogs/what-is-wannacry-how-does-wannacry-ransomware-work/.

Ghafur, S., et al. "A Retrospective Impact Analysis of the WannaCry Cyberattack on the NHS." *Npj Digital Medicine*, vol. 2, no. 1, 2 Oct. 2019, www.nature.com/articles/s41746-019-0161-6.

Gregory, Jennifer. “Articles WannaCry Worm Ransomware Changed Cybersecurity.” *Ibm.com*, 30 Oct. 2020, www.ibm.com/think/x-force/wannacry-worm-ransomware-changed-cybersecurity.

Nakashima, Ellen, and Craig Timberg. “NSA Officials Worried about the Day Its Potent Hacking Tool Would Get Loose. Then It Did.” *The Washington Post*, 16 May 2017, www.washingtonpost.com/business/technology/nsa-officials-worried-about-the-day-its-potent-hacking-tool-would-get-loose-then-it-did/2017/05/16/50670b16-3978-11e7-a058-ddbb23c75d82_story.html.

SentinelOne. “EternalBlue Exploit: What It Is and How It Works.” *SentinelOne*, 27 May 2019, www.sentinelone.com/blog/eternalblue-nsa-developed-exploit-just-wont-die/.

NHS
Example Name

Example Name

123 Example Street

Post Code

17 May 2017

Dear Patient Name

The WannaCry Incident and your NHS Care

This letter is regarding the impacts of the recent WannaCry computer virus and its impact on NHS **care**. On Friday, 12 May 2017, a global cyber-attack known as WannaCry impacted organisations worldwide, including the NHS. This was a form of malicious software or ransomware that targeted older computer systems running Microsoft Windows software.

Impacts on NHS:

- It Locked Our Systems: The ransomware encrypted (locked) the files on some of our computers. This meant staff in directly infected hospitals lost access to digital records, X-rays, and appointment systems.

- It Disrupted Your Care: To contain the virus, many NHS sites, including GP practices, urgently took their IT systems offline. This action caused service disruption, especially in infected hospitals, which saw an overall 6% decrease in-patient admissions. Specifically, we had to cancel 13,500 outpatient appointments in these affected hospitals, and in a few areas, divert ambulances from Accident & Emergency (A&E) departments.

Our Response

Staff in affected areas immediately switched to paper records, using landlines and printed documentation to maintain essential services and patient safety.

We can confirm that we **did not pay the ransom** demanded by the attackers. Critically, we have confirmed that the attackers **did not access, steal, or compromise** any patient data.

Moving Forward

We recognised this attack highlighted critical vulnerabilities in our infrastructure. We learned hard lessons, and we are moving decisively to prevent future issues.

Since the WannaCry incident, the NHS has taken and continues to take the following long-term actions:

- We are implementing security patches for all our systems to ensure that their security is up to date
- We have secured our firewalls to prevent future attacks
- We have developed better disaster response protocols, ensuring staff know exactly how to continue delivering care, even if our IT systems face another disruption.

Yours sincerely,

On behalf of the entire NHS system

Wander Barnes

Dr. Brandon C. Strubberg

TCID 4080

September 30th, 2025

Case Study: Reflection

This case study for me helped to highlight a lot of discussions we have had in Cybersecurity and TCID. With how much Wannacry impacted the NHS it helped me see how across an organization can be debilitated by viruses in different ways. I think it also helped me to see the importance of updates as some NHS trusts did patch their systems prior to the infection.

Reflecting on the chaos Wannacry caused, I can only imagine the immense stress medical staff faced. They were forced to abandon digital records and immediately revert to paper charts. The human experience of that rapid, high-stakes shift is a critical takeaway, that can apply to any workplace. If UCCS were to suddenly face a threat like this, for me with no Teams it would be difficult to communicate with my team well.

I also wanted to add I tried my best to research the brand standards of the NHS well to create a document like they would. I followed their design library here: https://www.england.nhs.uk/nhsidentity/identity-guidelines/.

AI Use Disclosure: AI (Gemini) was used to help proofread, edit and rephrase content for the case study. For the NHS response, an example was generated to show how one would be written. Document was also proof read and edited by AI.