The NHS cyber-attack: A look at the complex environmental conditions of WannaCry

RAD Magazine, 44, 512, 25-26

Andrew Dwyer

CDT in Cyber Security and the School of Geography and the Environment, University of Oxford

andrew.dwyer@cybersecurity.ox.ac.uk

"NHS seeks to recover from global cyber-attack as security concerns resurface." The Guardian, May 13, 2017[1]

"The ransomware meltdown experts warned about is here." Wired, May 12, 2017[2]

Initial reports of a large cyber-attack involving the NHS emerged on Friday, May 12, 2017.[3] Reports of other organisations facing similar trouble surfaced, with the Spanish telecom company Telefónica, car manufacturer Renault, and logistics business FedEx all being affected.

The attack exposed some of the weaknesses of the NHS as an IT organisation. As perhaps the most high profile organisation affected by the malicious software, or malware, it brought questions to the fore over its responsiveness, and the likelihood of such activities happening again. Certain NHS organisations were severely impacted many days after the initial entry of some components onto networks. It is important to note that the NHS was not a direct target, but was impacted due to its complex environments – computing, medical, political and so on. The mixture of these environmental challenges, with the need for relatively 'open' systems, legacy devices and fiscal constraint, all played a role. This article outlines what the malware WannaCry is, its operation, and preparedness then and now.

The malware

WannaCry is constructed of several components of software to form a single malware form. For those with limited knowledge of malware, it is computer code (or software – that can often mix legitimate and nefarious elements) that causes activities beyond the level of what is expected. In the NHS cyber-attack, there was a combination of components that led to WannaCry being a particularly damaging form.

WannaCry brought together two main components that made it especially effective at propagation and damage: Ransomware and worm.

First, ransomware (**figure 1** shows the WannaCry ransom 'note') is a malware form that uses cryptography (that helps protect communications and keep medical data secure) to 'lock' computer files. Certain files become inaccessible according to a prescribed list of file formats. The computer still turns on in most cases, but many common files are no longer accessible. Due to the quality of the encryption or locking with WannaCry, it is not possible to reverse this process without a key. If there is no back-up of your files, then these are almost certainly lost. Second, the worm component enables the ransomware to spread very quickly according to various techniques and, crucially, is self-propagating.

WannaCry was particularly successful in propagating, and combined ransomware in a new malware form to produce effects that are well-known today. There have been many ransomware variants, most notably CryptoLocker that emerged in 2013, but none have combined them with worms in such a damaging way. Its uniqueness is amplified by the worming capacity in particular, which could move around the internal networks of NHS organisations, and test them from internet-facing machines. There is peculiar lineage from the US National Security Agency's (roughly equivalent to the UK's Government Communications Headquarters) toolsets that are used for their strategic actions. The Shadow Brokers group gained access to these tools and released these to the internet.[4] The dump that included a specific technique exploited in the WannaCry malware was released April 14, 2017, less than a month before the attack. The EternalBlue exploit that this included allowed for a manipulation of a protocol used by computers to share information between one another.

The malware's operation

The ransomware component of WannaCry had previously been identified, but due to its insignificant volume, had not been provided protection by many endpoint (anti-virus) businesses. **Figure 2** provides a simple overview of how the worming component utilised the EternalBlue exploit. The exploit targeted the server message block (SMB) allowing an attacker to remotely execute their code on a computer. This has two main methods, both using what are called computer ports that allow computers to communicate, in this case the TCP 445 port. Without sinking into technicality, the initial vector of infiltration comes through an open port 445 to the internet. It is usual to close all SMB ports that externally face the internet, as they typically involve internal networking. As shown in **figure 2**, an infected computer will search random IP addresses to look for the SMB vulnerability in the port. If found, it will attempt to exploit this, and propagate as shown via the network route. Once this exploit is completed, unless there is specialist protection, and it is a specific Windows operating system, the ransomware encrypts, or locks, files.

The malware produces a screen (**figure 1**) in which you can purchase the cryptocurrency Bitcoin to pay the ransom. However, it is unlikely to unlock encrypted files if the ransom is paid, due to poor implementation of the keys to do so. In total, around £105,000 was paid to the malware authors at the time of writing.[5] This could have been much higher was it not for a 'kill-switch' in the malware. This connected to a certain website stopping the ransomware from encrypting files, which was found and activated late Friday afternoon, limiting the worm component spreading and the ransomware packed inside it. However, advice to stop internet connections increased propagation as no connection could be made to the website, allowing further encryption of files in organisations that ceased internet connection.

Did we know this was going to happen?

It is unlikely the impact of the malware form WannaCry could have been foreseen due to the complex environments it emerged within. Not all NHS organisations were affected by WannaCry due to the specific environments that are crafted at various levels. It is out of the scope and intention of this short overview to question practices of individual organisations and their interdependencies, such as through the new Health and Social Care Network, formerly N3, that support services such as PACS. Yet, there was an initial assumption in the media, and among security professionals, that medical networks and, in particular, the NHS had been affected heavily due to their above-average dependence on legacy operating systems such as Windows XP. Legacy systems were of limited fault this time however, including those that support specialist medical software, as WannaCry crashed the computer before being able to encrypt files, which would still lead to unexpected malfunction.[6] So, although Windows XP was not an assistant in malware propagation, it was still impacted heavily – and for those analysing, it was unknown until further inspection whether a computer has been compromised.

Most critical in the prevention of the vulnerability being exploited was the release of a patch by Microsoft on March 14, two months prior to the attack.[7] The deployment of a patch is frequently difficult to organisationally implement. This is no truer than in medical environments, where certain IT operations cannot simply be updated without due assessment of risk. Constraints include compliance, testing and auditing specialist legacy medical software for an update, developing agreement between stakeholders, and responding to multiple new threats. Thus, although two months may seem to be a considerable amount of time, the exceptionally complex multitude of specialist software and rather low number of IT personnel who have a raft of competing pressures, it is not surprising that this could not be implemented across all NHS environments in an even fashion.

Is it likely to happen again in the future?

The NHS cyber-attack had implications beyond medical environments and became a flashpoint during the 2017 UK general election. Clearly, the impacts at some NHS organisations were unacceptable and an adequate response is required due to the severe medical implications. WannaCry may have been stymied due to a previous malware form: The Adylkuzz 'crypto-miner' that uses computing power to generate virtual currency, utilising the same vulnerability, closing the port and preventing other malware from exploiting this.[8] In the complex mixing of environments beyond the medical, it is incredibly difficult to assess risk of future cyber-attacks. Thus, disruption in the future should be expected. Yet deploying greater awareness to preventing movements on networks should be considered, rather than a current fixation on singular medical devices, although these are important to maintain. By moving to network protection, or securing the environment, it could limit the impact of WannaCry-style events.

There have been positive developments to coordinate the NHS response, with NHS Digital tendering for a new Security Operations Centre to deal with emerging threats.[9] However, speaking to those who attended the UK Radiation and Oncology Congress revealed that a lack of central coordination and communication was received, which likely perpetuated the delay in bringing systems online. It will take time for the issues to be resolved and to develop strategies both centrally and within individual organisations, and discover why some were affected and others not. A look at the different environments that surround the NHS allows for an explanation of why WannaCry was so impactful on systems and reputation, but this is unlikely to be resolved quickly.

References

1, *NHS seeks to recover from global cyber-attack as security concerns resurface. The Guardian (internet), cited 2017 Sep 27. Available from: https://www.theguardian.com/society/2017/may/12/hospitals-across-england-hit-by-large-scale-cyber-attack.*

2, *The ransomware meltdown experts warned about is here. WIRED (internet), cited 2017 Sep 27. Available from: https://www.wired.com/2017/05/ransomware-meltdown-experts-warned/.*

3, *Statement on reported NHS cyber attack – NHS Digital (internet), cited 2017 Sep 11). Available from: https://digital.nhs.uk/article/1491/Statement-on-reported-NHS-cyber-attack.*

4, *Shane S. Malware case is major blow for the NSA. The New York Times (internet) 2017 May 16. Cited 2017 Sep 26. Available from: https://www.nytimes.com/2017/05/16/us/nsa-malware-case-shadow-brokers.html.*

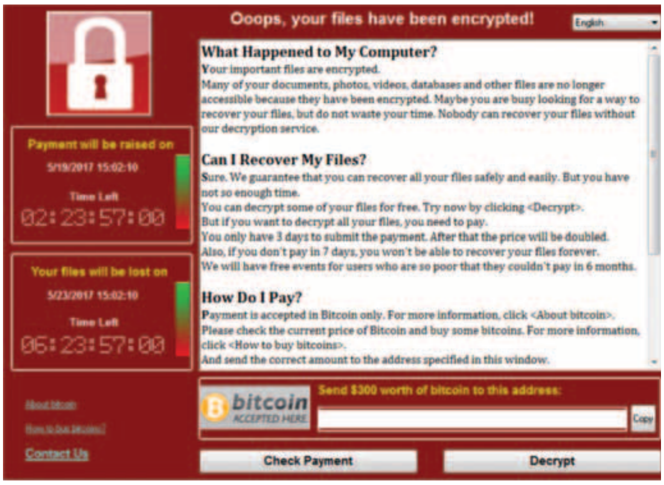
5, *Lee D. WannaCry ransomware bitcoins move from online wallets. BBC News (internet). 2017 Aug 3. Cited 2017 Sep 6. Available from: http://web.archive.org/web/20170808062123/http://www.bbc.co.uk/news/technology-40811972.*

6, *Brandom R. Windows XP computers were mostly immune to WannaCry. The Verge (internet). Cited 2017 Sep 26. Available from: https://www.theverge.com/2017/5/30/15712542/windows-xp-wannacry-protect-ransomware-blue-screen.*

7, *Microsoft Security Bulletin MS17-010 – Critical (internet), cited 2017 Sep 6. Available from: https://technet.microsoft.com/en-us/library/security/ms17-010.aspx.*

8, *Proofpoint. Adylkuzz cryptocurrency mining malware spreading for weeks via EternalBlue/DoublePulsar (internet). Proofpoint 2017. Cited 2017 Sep 26. Available from: https://www.proofpoint.com/us/threat-insight/post/adylkuzz-cryptocurrency-mining-malware-spreading-for-weeks-via-eternalblue-doublepulsar.*

9, *NHS Digital. Fit for 2020: Report from the NHS Digital Capability Review. NHS 2017 Jul (internet), cited 2017 Sep 26. Available from: https://digital.nhs.uk/media/31743/NHSDigital-Fit-for-2020-report-FINAL-120717/pdf/NHSDigital-Fit-for-2020-report-FINAL-1207171.*



Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

Payment will be raised on
5/19/2017 15:02:10
Time Left
02:23:57:00

Your files will be lost on
5/23/2017 15:02:10
Time Left
06:23:57:00

Send $300 worth of bitcoin to this address:

Figure 1

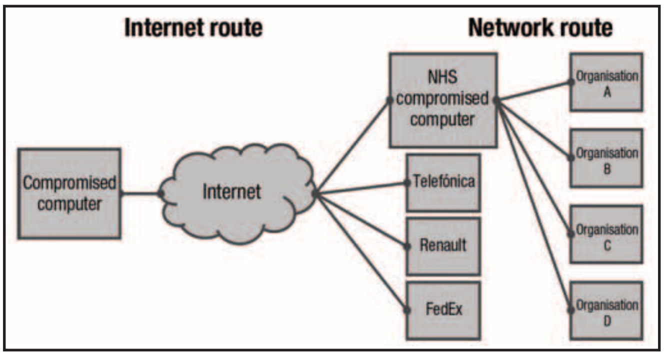


Figure 2