National Health Service Ransomware Attack 2017

Shona Start
Northumbria University, KF7002
shona.start@northumbria.ac.uk

Abstract - The ransomware WannaCry uses DoublePulsar and EternalBlue to take advance of exploits Windows operating systems. It's worm abilities allow it to spread quickly across entire systems. However, many countermeasures and corrective measures can be used to completely prevent a WannaCry attack such as the MS17-010 patch.

Index Terms— WannaCry; Ransomware; EternalBlue; DoublePulsar; NHS Cyber Attack.

I. Introduction

In 2017 a new ransomware worm called WannaCry caused a worldwide cyber-attack. Many organizations and businesses were affected by this malware, however, one of the biggest causalities was the United Kingdom National Health Service (NHS). The ransomware was present on NHS systems for several days and cost the organization an estimated £92m (Ghafur, et al., 2019). This report will outline the mechanism and exploits WannaCry used infect NHS systems. It will also discuss the countermeasures and corrective measures that could have been taken and can be taken in the future.

II. WannaCry

Ransomware is used to extort money from its victims. The WannaCry ransomware does this by encrypting the files on a device and then demanding a Bitcoin ransom in order to decrypt the files. Initially, it was thought that WannaCry was spread through phishing. Phishing is the use of emails to spread infected links or attachments. However, it was later found that the malware is a computer worm that used the Microsoft Windows vulnerability EternalBlue and the tool DoublePulsar to spread (Data Protection Report, 2017).

EternalBlue, official name ms17-010, is an exploit that was developed by the United States National Security Agency (NSA). The exploits only affect the Microsoft Windows operating system (OS), it uses the CVE-2017-0144 vulnerability present in the Server Message Block (SMB) protocol. This vulnerability can allow for remote code execution meaning once an attacker has sent a malicious packet to the target they can use this exploit to remotely activate the code (Stier & Greve, 2019) (Rapid7, 2019).

DoublePulsar is a backdoor implant tool that provides an access channel for malware to be loaded on the target. EternalBlue uses this tool to spread across local networks undetected by attempting to connect to other targets using SMB over ports TCP 139 and TCP 445 (Kao, et al., 2018) (Lakhani , 2017).

Once the malware has successively embedded itself onto a device it executes the encryption process. The encryption technique used by WannaCry relies on a hybrid algorithm of Advanced Encryption Standard (AES) and Rivest–Shamir–Adleman (RSA) encryption. This hybrid allows for a high encryption speed rate while still being secure as encryption keys are stored in a remote command and control server (Akbanov, et al., 2019).

It is not clear how WannaCry initially gained access to NHS systems; however, it is obvious the systems that were infected were using outdated IT systems, including Windows XP, an OS that Microsoft stopped supporting in 2014. In fact, at the time of the NHS attack a MS17-010 patch had already been released by Microsoft, including unsupported OS, and it was discovered that none of the NHS organizations infected by WannaCry had applied the patch (William , 2018). This highlights the significance of keeping software up to date, most cyberattacks take advantage of known vulnerabilities in systems and WannaCry was no exception to this; it is likely the attack could have been entirely avoided if systems had been updated (Panda Security, 2019).

Another reason the WannaCry ransomware was able to spread so easily throughout the NHS is it's under preparedness to deal with Cyber Security attacks. It is reported in reviews of the WannaCry attack that the NHS had developed plans for responding to attacks; however, these plans had not been tested and were not clear. Therefore individual NHS organizations did not know who to report the incident too. This issue was further complicated by the belief that it was a Phishing attack causing many individual organizations to shut down their email systems as a precaution, causing communication issues (Department of Health, 2018). Clearly, an incident response (IR) plan for cyber security breaches should have been in place, an effective IR plan will minimize damage, protect data,

and help an organization recover from the incident as quickly as possible. There are 6 steps to an IR plan; these are Preparation, Identification, Containment, Eradication, Recovery and Lessons learned (Kral, 2011).

Preparation: Large organizations should have a well-trained computer emergency response team (CSIRT) in place; the NHS calls their team CareCERT. It is vital this team has the necessary access control and tools to deal with a cyber security incident, without this access it is likely that the CSIRT will be ineffective at mitigating damage. Clear guidelines and rules for incident handling should be defined for both the CSIRT and users of the systems. These guidelines must be highly visible to all users of the system so that it is clear what users should do during an incident including in what situations the CSIRT should be contacted and how to communicate with the CSIRT; with contingencies in place for internet inaccessibility (Kral, 2011).

Identification: Identifying ransomware once it is activated is easy. But preferably, malware should be detected before it is activated. One way of identifying malware is by using antivirus software and firewalls. Not only can this software identify viruses and malware, but it can also delete or quarantine the malicious files and programs. However, antiviruses and firewalls can only protect a device against the known viruses/malware, and they need updating very frequently or they will be completely ineffective. It is also debatable how effective this type of software is against ransomware, as with this type of malware it only needs to be executed successfully once for it to encrypt all files (Scaife, et al., 2017).

Since the initial outbreak of WannaCry research has been conducted into specific detection methods for WannaCry that can be used to determine if WannaCry is present on a system and the different stages of attack the malware has completed. "A Comprehensive Detection Approach of WannaCry: Principles, Rules and Experiments" provides a rule set called Comprehensive WannaCry Detection Rules (CWDR) which can accurately detect the whole process of WannaCry's attack. (Lu, et al., 2020).

Containment: Computer worms can infect large numbers of computers in a network extremely fast and don't require any human interaction to do so. One of the only techniques for containing WannaCry is to isolate network segments by removing them from both the local network and the internet. This method brings entire systems to a standstill but prevents the malware from infecting outside of the network segment (Kral, 2011).

Eradication: One of the most efficient ways of eradicating malware such as WannaCry is to identify the root cause and set up preparation against it. Because WannaCry was a worldwide incident the cause was quickly investigated by many organizations and as discussed earlier a patch released by Microsoft (William , 2018). As well as the discovery of a kill switch by a cybersecurity researcher, Marcus Hutchins, which temporally stopped the spread of the malware (Newman , 2017). This made the eradication of WannaCry from NHS systems simpler as it was unlikely systems would be reinfected.

Recovery: Even after WannaCry is eradicated from a system the encryption will still be present and even paying the ransom is not a guarantee of recovery (Baraniuk, 2017). This issue is made more challenging by the fact WannaCry tries to prevent common data recovery techniques by deleting backups and snapshots of files/volumes that Windows OS and Windows Server create called "Shadow Copy's" (Akbanov, et al., 2019). Organizations should create regular backups of data, this should be stored in a separate system so that it can be isolated immediately to prevent backups being infected (Scaife, et al., 2017).

Before restoring backups, it is vital to first ensure the threat is completely removed. Due to the size and demand for the NHS, it is unlikely a full verification could be performed before systems were brought back online. However, ongoing monitoring for some time after the incident can allow the CSIRT to step in at the first sign of recurrence.

Lessons learned: In order to learn from a cyber security incident it is vital to utilize documentation during and after the incident so that a review of everything that happened can be completed to establish what was effective and areas that need improvement. The NHS has published a lesson learned review of the attack. This details the entire attack and the steps they are taking to learn from it, including the creation and distribution of IR plans (William , 2018).

III. Conclusion

The WannaCry attack on the NHS was able to spread across systems and may have caused a large amount of damage. However, it is likely this incident could have been completely avoided if systems had been updated regularly so that the MS17-010 patch

could be applied. The attack could also have been mitigated if a detailed incident response (IR) plan had been created and tested so that a CSIRT could respond appropriately and quickly to control the situation.

IV. References

Akbanov, M., Vassilakis, V. G. & Logothetis, M. D., 2019. *WannaCry Ransomware: Analysis of Infection, Persistence, Recovery Prevention and Propagation Mechanisms,* s.l.: Journal of Telecomuncations and Infomation Technology.

Baraniuk, C., 2017. *Should you pay the WannaCry ransom?.* [Online]
Available at:
https://www.bbc.co.uk/news/technology-39920269

Bisson, D., 2020. *Amazon Web Services Mitigated a 2.3 Tbps DDoS Attack.* [Online]
Available at: https://www.tripwire.com/state-of-security/security-data-protection/amazon-web-services-mitigated-a-2-3-tbps-ddos-attack/

Chen, Q. & Bridges, R., 2017. *Automated Behavioral Analysis of MalwareA Case Study of WannaCry Ransomware.* s.l., 16th IEEE International Conference on Machine Learning and Applications.

Data Protection Report, 2017. *WannaCry Ransomware Attack Summary.* [Online]
Available at:
https://www.dataprotectionreport.com/2017/05/wannacry-ransomware-attack-summary/

Department of Health, 2018. *Investigation: WannaCry cyber attack and the NHS,* s.l.: Natinal Audit Office.

Ghafur, S., Kristensen, S., Honeyford, K. & et al., 2019. *A retrospective impact analysis of the WannaCry cyberattack on the NHS,* s.l.: Digital Medicine.

Kao, D.-Y., Hsiao, S.-C. & Tso, R., 2018. Analyzing WannaCry Ransomware Considering the Weapons and Exploits. *ICACT Transactions on Advanced Communications Technology,* 7(2), pp. 1098-1102.

Kral, P., 2011. *The Incident Handlers Handbook,* s.l.: SANS Institute.

Lakhani , A., 2017. *How does WannaCry spread?.* [Online]
Available at: https://www.fortinet.com/blog/threat-research/wannacry-faq#:~:text=WannaCry%20has%20multiple%20ways%20of,is%20to%20use%20the%20Backdoor.&text=Once%20the%20malware%20has%20successfully,TCP%20139%20and%20TCP%20445.

Lu, G. et al., 2020. *A Comprehensive Detection Approach of Wannacry: Principles, Rules and Experiments.* s.l., s.n.

Newman , L., 2017. *How an Accidental 'Kill Switch' Slowed Friday's Massive Ransomware Attack.* [Online]
Available at:
https://www.wired.com/2017/05/accidental-kill-switch-slowed-fridays-massive-ransomware-attack/

NHS, 2017. *CLDAP Used in DDoS Attacks.* [Online]
Available at: https://digital.nhs.uk/cyber-alerts/2017/cc-1333

Panda Security, 2019. *The importance of updating your systems and software.* [Online]
Available at:
https://www.pandasecurity.com/en/mediacenter/tips/the-importance-of-updating-systems-and-software/

Rapid7, 2019. *Microsoft CVE-2017-0144: Windows SMB Remote Code Execution Vulnerability.* [Online]
Available at:
https://www.rapid7.com/db/vulnerabilities/msft-cve-2017-0144/#:~:text=A%20remote%20code%20execution%20vulnerability,code%20on%20the%20target%20server.

Scaife, N., Traynor, P. & Butler, K., 2017. *Making Sense of the Ransomware Mess (and Planning a Sensible Path Forward),* s.l.: Financial Technology.

Shin, D., 2018. *How to Defend Against Amplified Reflection DDoS Attacks.* [Online]
Available at:

https://www.a10networks.com/blog/how-defend-against-amplified-reflection-ddos-attacks/

Stier, T. & Greve, J., 2019. *An analysis of WannaCry and EternalBlue.,* s.l.: University of Copenhagen.

William , S., 2018. *February 2018 Lessons learned review of the WannaCry Ransomware Cyber Attack,* s.l.: NHS.