Kailyn Johnson

WannaCry: One Year Later

Abstract

Despite the massive impact the WannaCry ransomware attack had on businesses across the globe and the immediate changes to security practices following it, a year later businesses still have a reactive approach and struggle to implement comprehensive security policies that target employees and management. With cyber threats evolving so rapidly, businesses need to learn how to be quick on their toes and expedite the development and enforcement of cyber security policies to better prevent future breaches.

Introduction

The WannaCry malware outbreak that occurred in May 2017 was one of the most damaging attacks to happen globally, having infected over 300,000 computers in 150 different countries[1]. The attack began on Friday, May 12th, 2017 utilising the "EternalBlue" Microsoft Windows exploit that the cyber-oriented threat group, the Shadow Brokers, made public after stealing it from the United States' National Security Agency[2]. The first variant of WannaCry was stopped from infecting new machines when a security researcher inadvertently activated a kill-switch for the malware which stopped it from further spreading[3]. Other variants of WannaCry without the domain kill-switch appeared almost immediately after the first kill-switch halted the attack[4]. This specific attack using the WannaCry ransomware lasted until May 15th.

Technical Analysis of the Malware

WannaCry is a form of ransomware, which encrypts a variety of a user's files and then requests money in return for a decryption key. The ransom demands the payment be in the form of cryptocurrency, specifically Bitcoin, because anyone in the world could purchase Bitcoin, which allows for a larger pool of potential victims. If a victim paid out the ransom, in theory, the attackers would then give the victim a decryptor tool to unlock their files[5]. The initial ransom charged $300 USD in Bitcoin, which purportedly would increase to

1 "Foreign Office Minister Condemns North Korean Actor For Wannacry Attacks". 2018. GOV.UK. https://www.gov.uk/government/news/foreign-office-minister-condemns-north-korean-actor-for-wannacry-attacks
2 Symantec Security Response Team. "What You Need To Know About The Wannacry Ransomware". 2017. Symantec Security Response. https://www.symantec.com/blogs/threat-intelligence/wannacry-ransomware-attack
3 Vigliarolo, Brandon. 2017. "Wannacry: A Cheat Sheet For Professionals". Techrepublic. https://www.techrepublic.com/article/wannacry-the-smart-persons-guide/
4 Newman, Lily. 2018. "How An Accidental 'Kill Switch' Slowed Friday's Massive Ransomware Attack". WIRED. https://www.wired.com/2017/05/accidental-kill-switch-slowed-fridays-massive-ransomware-attack/
5 Global Research and Analysis Team. "Wannacry Ransomware Used In Widespread Attacks All Over The World". 2017. Securelist - Kaspersky Lab's Cyberthreat Research and Reports.

$600 USD if it was not paid within a certain timeframe[6]. Bitcoin is easily traceable compared to other forms of cryptocurrency, like Monero, which might lead threat actors to use those instead in future attacks. Because the ransom amount was so low compared to what it could have been, it was posited by many researchers that the end-goal of the attack was not financially-driven, but more likely, destruction and chaos were the intended outcomes. The ransomware changed the user's computer background to inform the victim that their files had been encrypted. An application window displayed the ransom instructions, and allowed for the note to be available in 28 different languages and provided a sort of "user manual" in English.[7]

Although the initial attack vector is unknown, the attack vector of how WannaCry self-propagates is well-researched and will be outlined in more detail in this section. WannaCry utilised a vulnerability within Windows Server Message Block (SMB) protocol[8]. The SMB protocol is used for, but not limited to, file sharing between Windows machines on Local Area Networks (LANs). The malware was observed using this protocol to spread within the infected networks because it does not require user interaction to further it[9]. Once WannaCry infected a machine, the malware would attempt to connect to the domain www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com."[10] If an IP address was returned and the malware performed a successful HTTP GET request to the domain, the malware would exit out and not run anything malicious[11]. By registering the domain and pointing it to a Web server, this check acted as a kill-switch for the malware. If the domain was not successfully accessed, the malware would run and encrypt the files on the machine whilst spreading within the network through the "EternalBlue" (CVE-2017-0143) SMB vulnerability.[12] During this process, the malware would load an embedded RSA public key into the machine creating a thread for moving and deleting files after they were encrypted.[13] This would then allow for the configuration of the Bitcoin wallet and the "Ooops, your important files are encrypted" alert to show up on the infected machine.[14]

Following the encryption process, the malware communicates with an Onion server accessed via Tor (The Onion Router) to register the infected machine and transfer the encryption key.[15]

Tor is a tool that allows users to connect to the Internet through virtual tunnels rather than direct connections, circumvents censorship, and anonymises access to the Internet, ensuring privacy.[16]

At this point, the malware is able to then communicate with the Tor server to check if a ransom is paid, by clicking the "Check Payment" button. The encrypted private RSA key is sent to the server, which is able to reply with the decrypted private RSA key, so the files can be unencrypted.[17] However, this system had no way for attackers to determine which machines had actually paid the ransom, so even individuals who did pay the ransom did not get their files back due to this flaw.[18]

The Aftermath and Consequences of the Attack

In the wake of the attack, it was disclosed that organisations like banks in Ukraine, FedEx, Spain's Telefonica, the Russian Ministry of Internal Affairs, a major German railway service, telecommunication

6 Ibid.
7 Ibid.
8 Vigliarolo, Brandon. 2017. "Wannacry: A Cheat Sheet For Professionals". Techrepublic. https://www.techrepublic.com/article/wannacry-the-smart-persons-guide/
9 Ibid.; Symantec Security Response Team. "What You Need To Know About The Wannacry Ransomware". 2017. Symantec Security Response. https://www.symantec.com/blogs/threat-intelligence/wannacry-ransomware-attack.
10 Berry, Alex, Josh Homan, and Randi Eitzman. 2017. "Wannacry Malware Profile". FireEye. https://www.fireeye.com/blog/threat-research/2017/05/wannacry-malware-profile.html
11 Ibid.
12 Ibid.
13 Ibid.
14 Ibid.
15 Ibid.
16 "Tor Project: Overview". 2018. Torproject.org. https://www.torproject.org/about/overview.html.en
17 Berry, Alex, Josh Homan, and Randi Eitzman. 2017. "Wannacry Malware Profile". FireEye. https://www.fireeye.com/blog/threat-research/2017/05/wannacry-malware-profile.html
18 Symantec Security Response Team. "What You Need To Know About The Wannacry Ransomware". 2017. Symantec Security Response. https://www.symantec.com/blogs/threat-intelligence/wannacry-ransomware-attack

companies, the UK's National Health Service (NHS) in England, universities, and many others were those affected by WannaCry. Many organisations that were affected did not publicly disclose the extent of the impact WannaCry had on them, but we can still create lessons learned from the attack, following an examination into how the NHS dealt with the aftermath of the attack as that has been made public.

80 trusts within the NHS England network and almost 600 General Practitioner (GP) practices were infected by WannaCry, causing major disruptions in daily services.[19] Between May 12 and May 18, over 19,000 appointments were cancelled according to the National Audit Office.[20] While the NHS had a plan for how to respond to certain incidents, it was never tested at a local level and there was not a plan in place for cyber-specific incidents.[21] When WannaCry hit, the NHS had no clear idea of who should lead the response to it and whom to communication with.[22] A common theme found across many organisations, though particularly apparent in the organisations affected by WannaCry, was that while they had security policies in place, many did not follow their own cyber security policies. The patches Microsoft released for the vulnerabilities exploited in this attack were not immediately applied; however, one explanation for the security patches not getting installed in a timely fashion might have been due to the possibility that they could break other applications and machines used by an organisation. On top of fixes not being implemented quickly, some organisations were also found to utilise unsupported software, like Windows XP, which Microsoft no longer issues updates or patches for.

Despite many organisations and individuals not getting their files back, the threat actors behind the WannaCry attack made approximately £108,953 ($144,653.52 USD) in Bitcoin.[23] Considering over 200,000 machines were infected in the attack, the financial profit the attackers made was comparatively low. This led to a variety of theories concerning the attribution and actual intention of the attack. Symantec and other security researchers have ascertained that the attack was most likely conducted to cause chaos rather than make a profit, and was likely conducted by a North Korean-linked Advanced Persistent Threat (APT) group, Lazarus group, because of similarities linking their Tactics, Techniques, and Procedures (TTPs)[24]. The NHS is supposed to come out with an estimate as to how much the attack cost the department after June 2018.[25] However, it has been determined that the government will allocate over £150 million ($199,150,350 USD) in the next three years to improve the NHS resilience to cyber threats with "£21 million ($27,881,049 USD) dedicated to address key vulnerabilities in major trauma centres and ambulance trusts" and £39 million ($51,779,091 USD) allocated to various NHS trusts to address their infrastructure shortcomings.[26] [27]

Lessons to Take Away from the Attack

WannaCry highlighted the lack of cyber security awareness within many organisations and their employees. A year following the attack, many researchers uncovered that various institutions still do not have proper cyber security awareness training for their employees and management.[28] This causes organisations to remain vulnerable to poor

19 Smart, William. Officer for Health and Social Care. 2018. "Lessons Learned Review of The Wannacry Ransomware Cyber Attack". London: The Crown.
20 National Audit Office. 2018. "Investigation: Wannacry Cyber Attack and the NHS". London: National Audit Office.
21 Ibid.
22 Ibid.
23 Gibbs, Samuel. 2018. "Wannacry: Hackers Withdraw £108,000 Of Bitcoin Ransom". The Guardian. https://www.theguardian.com/technology/2017/aug/03/wannacry-hackers-withdraw-108000-pounds-bitcoin-ransom
24 Symantec Security Response Team. 2017. "Wannacry: Ransomware Attacks Show Strong Links To Lazarus Group". Symantec Security Response.
https://www.symantec.com/connect/blogs/wannacry-ransomware-attacks-show-strong-links-lazarus-group
25 Donnelly, Caroline. 2018. "PAC Sets June 2018 Deadline For Department Of Health To Count NHS Cost Of Wannacry". Computer Weekly. https://www.computerweekly.com/news/252439314/PAC-sets-June-2018-deadline-for-Department-of-Health-to-count-NHS-cost-of-WannaCry; "Plans To Strengthen NHS Cyber Security Announced". 2018. GOV.uk. https://www.gov.uk/government/news/plans-to-strengthen-nhs-cyber-security-announced
26 Hall, Kat. 2018. "NHS Given A Lashing For Lack Of Action Plan One Year Since Wannacry". The Register. https://www.theregister.co.uk/2018/04/18/mps_slam_nhs_for_lack_of_action_plan_one_year_on_from_wannacry/
27 "Plans To Strengthen NHS Cyber Security Announced". 2018. GOV.uk. https://www.gov.uk/government/news/plans-to-strengthen-nhs-cyber-security-announced
28 Connolly, Lena Yuryna, Michael Lang, John Gathegi, Doug J. Tygar. 2017. "Organisational culture, procedural countermeasures, and employee security behaviour: A qualitative study". Information & Computer Security, Vol. 25 Issue: 2. pp.118-136; Kearney, W.D. and H.A. Kruger. 2016. 'Can perceptual differences account for enigmatic information security behaviour in an organisation?'. Computers &

cyber security hygiene such as not clicking links or downloads from unknown email addresses, going to suspicious websites, and sharing passwords with colleagues.[29] Many organisations continue to perpetuate an organisational culture that prioritises efficiency over security, and does not offer maintenance courses for security awareness which is extremely problematic given that threat actors continually evolve and refine their TTPs.[30] Therefore, organisations and employees need to stay up-to-date with the current threat trends such as: the increasing use of malicious applications in official download stores, more APT groups engaging in discrete state-sponsored attacks, and more sophisticated social engineering tactics. An example to exemplify the importance of staying up-to-date on these trends can be observed in threat actors beginning to switch to primarily utilising cryptominers to make an illicit profit over ransomware which was predominant in the recent past. Despite companies and organisations realising the cyber security practices need to be a priority to maintain security, many employees have admitted to "security fatigue."[31] "Security fatigue" is the threshold for when maintaining cyber security becomes too burdensome or difficult for users.[32] This threshold can also be applicable to employees and organisations becoming desensitised to the dangers and threats out in the wild, simply because they hear about it so often.[33]

There are many policies that were implemented in a variety of organisations in the wake of WannaCry such as security awareness training, better physically robust information security systems, consistent and immediate operating system patches, amongst others.[34] However, there is still a lot to be done to ensure that businesses and organisations have the best cyber security practices to prevent attacks and system infiltration. Despite the detrimental impact WannaCry had, another global ransomware campaign occurred shortly after, in June of 2017.

NotPetya occurred June 27 until June 28 2017, utilising the same SMB vulnerability to propagate through networks, and although the initial attack vector was different, it still affected prominent global businesses who still had not patched their systems. With data breaches and attacks still targeting businesses and successfully implementing malware, installing cryptominers, launching Distributed Denial-of-Service (DDoS) attacks, etc., businesses must begin creating and implementing more proactive policies, procedures, and countermeasures. It is essential to have a prescient and robust stance against cyber threats and threat actors in relation to cyber security policies. Threat actors are continuously developing sophisticated malware at a rapid pace, which does make it difficult to take an entirely proactive stance against threats; however, policies must recognise this while still attempting to provide adequate rules and regulations which are paramount to the future success of businesses in counteracting cyber threats, and maintaining security and resilience.

Good cyber security behaviours like immediately implementing critical patches to systems, utilising multi-factor authentication, having cold backup storage that is frequently updated, adequate CSIRT and SOC incident response procedures, and cyber security awareness training for employees are critical to reduce the likelihood an organisation has from being impacted by significant cyber attacks. It has been observed that organisations that utilise these practices and policies are at a considerably lower risk of being affected by threat actors. These practices effectively improve organisational security from a variety of fronts, and remain the best way that companies can improve their cyber resilience.

Security: 6

29 Ibid.; Pfleeger, Shari Lawrence, and Deanna D. Caputo. 2012. 'Leveraging Behavioral Science to Mitigate Cyber Security Risk'. Vol. 31

30 Ibid.

31 Connolly, Lena Yuryna, Michael Lang, John Gathegi, Doug J. Tygar. 2017. "Organisational Culture, Procedural Countermeasures, and Employee Security Behaviour: A qualitative study". Information & Computer Security, Vol. 25 Issue: 2. pp.118-136.

32 Ibid.

33 Ibid.

34 Connolly, Lena Yuryna, Michael Lang, John Gathegi, Doug J. Tygar. 2017. "Organisational culture, procedural countermeasures, and employee security behaviour: A qualitative study". Information & Computer Security, Vol. 25 Issue: 2. pp.118-136; Kearney, W.D. and H.A. Kruger. 2016. 'Can perceptual differences account for enigmatic information security behaviour in an organisation?'. Computers & Security: 6