Kailyn Johnson

NotPetya: One Year Later

Abstract

Almost immediately following the WannaCry cyber-attack, the NotPetya malware affected countries and organisations around the globe that had strikingly similar repercussions and lessons to take away. This attack exemplified the chronic failings organisations and nation-states continue to have despite the blatant and ongoing threats cyberspace poses. With cyber threats remaining a critical issue for organisations, there is still a great deal organisations need to do to mitigate these for future resilience.

Introduction

Shortly after the global WannaCry ransomware incident occurred, another cyber incident infected a large number of machines in Ukraine that ended up spreading across the globe. This new attack transpired on June 27, 2017 until June 28, 2017, when many organisations and businesses were still working to recover in the aftermath of WannaCry which occurred May 12, 2017 until May 15, 2017. This attack targeted a majority of Ukrainian organisations, specifically Ukrainian infrastructure and other major companies, though international companies were also severely impacted.[1] Many attribute the attack to Russia, although the nation vehemently denies it was responsible despite recent evidence researchers have released that incriminate Russian state-sponsored threat actors.[2] This white paper will discuss how NotPetya worked, the consequences of the attack, and lessons that organisations can take away from this event that will benefit their own future cyber resilience..

Technical Analysis of the Malware

NotPetya was initially believed to originate from a previous version of a malware called Petya, which was seen in attacks on Windows-based systems in 2016[3]; however, the malware was determined to have similar binary code to the Petya variant, "GoldenEye."[4] The GoldenEye malware rewrote the computer's master-boot record, which prevented the infected machine from starting up properly.[5] The malware would then load a ransomware notification textbox on the infected machine where it would inform the

1 Matt Burgess, "What is the Petya ransomware spreading across Europe?," WIRED.co.uk, 2017, https://www.wired.co.uk/article/petya-malware-ransomware-attack-outbreak-june-2017 (Accessed June 24 2018); Roi Perez, "NotPetya Ransomware: Lessons Learned," InfoSecurity Magazine, 2017, https://www.infosecurity-magazine.com/magazine-features/notpetya-ransomware-lessons-learned/ (Accessed June 29 2018).
2 Simon Sharwood, "UK names Russia as source of NotPetya, USA follows suit," The Register, 2018, https://www.theregister.co.uk/2018/02/15/uk_names_russian_military_as_source_of_notpetya/ (Accessed August 10 2018).
3 "NotPetya Technical Analysis," LogRhythm Labs (2017).
4 Ibid.
5 Symantec Security Response Team, "Petya ransomware outbreak: Here's what you need to know," Symantec Security Response, 2017, https://www.symantec.com/blogs/threat-intelligence/petya-ransomware-wiper (Accessed June 24 2018).

user that their system is infected, and the system could only be fixed if a ransom was paid to the threat actors in Bitcoin.[6] As the name suggests, NotPetya is different compared to the Petya malware in a variety of ways. Notably, it was disguised to be ransomware but actually turned out to be a "wiper."[7]

The threat actors behind NotPetya used a compromised update for software MEDoc to initiate the attack. MEDoc was likely used as the initial attack vector because it was one of the few approved applications for Ukrainian organisations to pay corporate taxes which is required by Ukranian law for government entities and businesses to have.[9] Therefore, the malware could effectively impact a broad scope of targets that operated specifically within Ukraine. Threat actors somehow obtained the credentials of an administrator at MEDoc that allowed them to gain root privileges and modify the configuration of certain software update modules.[10] The compromised software update server evoked the "IsNewUpdate" function within the MEDoc application and established that a so-called legitimate software update was available for users.[11] This then installed the malicious software update containing the hidden backdoor termed "MeCom" onto the victim's machine.[12] Since every organisation in Ukraine had a unique registry legal entity identifier, known as an EDRPOU code, the threat actors could track specific organisations that had the MEDoc software containing the backdoor.[13] This backdoor is what allowed the NotPetya malware to then propagate inside an organisation's network.

The use of a third-party partner or provider with access to an organisation's system or data to initiate an attack[8] is known as a "supply-chain attack." It takes advantage of the fact that the outside party is trusted by an organisation, so threat actors can initiate an attack much more effectively through this method.

Once NotPetya infiltrated a machine via the infected MEDoc software update, it would overwrite and encrypt various sections of the physical hard drive and C: drive volume by obtaining direct read and write access to those drives, given it had the proper permissions which will be discussed later in this section.[14] It utilised one of two ways to propagate once it was in a network:

1. Use the same Server Message Block (SMB) exploits that WannaCry used, "EternalBlue" and "EternalRomance," to self-propagate.[15]

OR

2. Use collected account credentials from the first machine it infected that would allow the malware to spread within the network even if an organisation patched their operating systems.[16]

To harvest the administrator credentials, the malware would search for a file called "perfc.dat" on the infected machine, and if it was not found, the malware would continue running to then check for three different privileges.[17] These privileges would allow for the malware to operate in the way it was designed

6 Ibid.
7 Josh Fruhlinger, "Petya ransomware and NotPetya malware: What you need to know now," CSO Online, 2017, https://www.csoonline.com/article/3233210/ransomware/petya-ransomware-and-notpetya-malware-what-you-need-to-know-now.html (Accessed June 29 2018).
8 Maria Korolov, "What is a supply chain attack? Why you should be wary of third-party providers," CSO Online, 2018, https://www.csoonline.com/article/3191947/data-breach/what-is-a-supply-chain-attack-why-you-should-be-wary-of-third-party-providers.html (Accessed August 08 2018).
9 David Maynor, Aleksandar Nikolic, Matt Olney, and Yves Younan, "The MeDoc Connection," Cisco Talos, 2017, https://blog.talosintelligence.com/2017/07/the-medoc-connection.html (Accessed August 08 2018); GReAT: Global Research and Analysis Team, "Schroedinger's Pet(ya)," SecureList, 2017, https://securelist.com/schroedingers-petya/78870/ (Accessed June 29 2018); Andrew E. Kramer, "Ukraine Cyberattack Was Meant to Paralyze, not Profit, Evidence Shows," The New York Times, 2017, https://www.nytimes.com/2017/06/28/world/europe/ukraine-ransomware-cyberbomb-accountants-russia.html (Accessed August 30, 2018)
10 Ibid.
11 Anton Cherepanov, "Analysis of TeleBots' cunning backdoor," WeLiveSecurity, 2017, (Accessed August 08 2018).
12 Ibid.
13 Ibid.; Symantec Security Response Team, "Petya ransomware outbreak: Here's what you need to know," Symantec Security Response, 2017, https://www.symantec.com/blogs/threat-intelligence/petya-ransomware-wiper (Accessed June 24 2018).
14 "NotPetya Technical Analysis," LogRhythm Labs (2017).
15 Ibid.
16 Ibid.; Symantec Security Response Team, "Petya ransomware outbreak: Here's what you need to know," Symantec Security Response, 2017, https://www.symantec.com/blogs/threat-intelligence/petya-ransomware-wiper (Accessed June 24 2018); Josh Fruhlinger, "Petya ransomware and NotPetya malware: What you need to know now," CSO Online, 2017, https://www.csoonline.com/article/3233210/ransomware/petya-ransomware-and-notpetya-malware-what-you-need-to-know-now.html (Accessed June 29 2018).
17 "NotPetya Technical Analysis," LogRhythm Labs (2017).

to, although the third privilege the malware checks for is not necessary to obtain if the "EternalBlue" SMB exploit is unpatched in the infected machine. The three privileges, which act as functions within an operating system, are:

1. *SeShutdownPrivilege* which allows the administrator the ability to shut down a system. [18]
2. *SeDebugPrivilege* which allows for the malware to read and modify memory of processes from other owners.[19]
3. *SeTcbPrivilege* which processes part of the Trusted Computer/Computing Base and allows for higher privileged access to operating subsystems.[20] Again, this is only necessary for the malware to gain if the SMB vulnerability is not accessible.

Once the NotPetya malware obtained account credentials from the system via the aforementioned privileges, those privilege functions then directed the route of the malware code for the propagation (either through the SMB vulnerability or the SeTcbPrivilege function), encryption, and wiping process.[21] The malware was observed to have created a list of IP addresses to spread to within the Local Area Network (LAN) and a list of remote IP addresses by collecting credentials through the Windows Credential Manager, as well as executing a 32-bit or 64-bit credential dumper.[22] The malware then checked if specific antivirus software was installed, specifically Kaspersky, Norton Security, and Symantec.[23] NotPetya used the "ns.exe" or "ccsvchost.exe" processes to determine whether it would utilise the SMB exploits.[24] After analysis of the malware, it appeared that the SMB exploits were only utilised when Kaspersky antivirus software was installed on a machine because the SMBv1 payload was only found in the Kaspersky-specific malware code.[25]

To harvest and retrieve the administrative credentials, NotPetya would execute a temporary file with a random name that was in the "%TEMP%" directory to run the credential harvester depending on whether the system was 32-bit or 64-bit.[26] The harvesters used in this attack appeared to have been a modified version of a well-known credential harvester, "Mimikatz."[27] Finally, once the malware obtained some or all the privileges, it would then create a task to perform a shutdown of the machine. If the malware obtained all three privileges mentioned above, and the operating system was Windows Vista, 2007 or higher, the shutdown task would be configured to run under "SYSTEM" account.[28] If the malware did not obtain all three privileges or the operating system was an older version of Windows, the malware would use the built-in "AT" command to schedule a shutdown and reboot.[29]

Following the scheduled system shutdown and reboot, 65 types of files on the hard drive were subsequently encrypted (and wiped as victims would soon discover).

A ransom note was then displayed to the user.[30] The ransom note asked for $300 USD in Bitcoin to be sent to the email address *wowsmith123456@posteo.net* from the victim to receive the decryption key and retrieve their files back.[31] While the attackers ended up making approximately $6,000 USD in Bitcoin,

The files encrypted were: .3ds .7z .accdb .ai .asp .aspx .avhd .back .bak .c .cfg .conf .cpp .cs .ctl .dbf .disk .djvu .doc .docx .dwg .eml .fdb .gz .h .hdd .kdbx .mail .mdb .msg .nrg .ora .ost .ova .ovf .pdf .php .pmf .ppt .pptx .pst .pvi .py .pyc .rar .rtf .sln .sql .tar .vbox .vbs .vcb .vdi .vfd .vmc .vmdk .vmsd .vmx .vsdx .vsv .work .xls .xlsx .xvd .zip [33]

18 Ibid.
19 Ibid.
20 Ibid.
21 Ibid.
22 Symantec Security Response Team, "Petya ransomware outbreak: Here's what you need to know," Symantec Security Response, 2017, https://www.symantec.com/blogs/threat-intelligence/petya-ransomware-wiper (Accessed June 24 2018).
23 "NotPetya Technical Analysis," LogRhythm Labs (2017).
24 Symantec Security Response Team, "Petya ransomware outbreak: Here's what you need to know," Symantec Security Response, 2017, https://www.symantec.com/blogs/threat-intelligence/petya-ransomware-wiper (Accessed June 24 2018).
25 "NotPetya Technical Analysis," LogRhythm Labs (2017).
26 Ibid.
27 Ibid.
28 Ibid.
29 Ibid.
30 Symantec Security Response Team, "Petya ransomware outbreak: Here's what you need to know," Symantec Security Response, 2017, https://www.symantec.com/blogs/threat-intelligence/petya-ransomware-wiper (Accessed June 24 2018).
31 GReAT: Global Research and Analysis Team, "Schroedinger's Pet(ya)," SecureList, 2017, https://securelist.com/schroedingers-petya/78870/

the motives behind the attack appears to not have been financially-driven.[32]

The Aftermath and Consequences of the Attack

The attack is suspected to have been not financially driven due to the fact that NotPetya was uncovered to act as a wiper rather than ransomware.[34] In addition, a ransomware attack of this scale, infecting at least 16,000 machines and costing companies over $1.2 billion USD (approximately £850 million) in revenue, logically should have garnered more illicit profit than just $6,000 USD.[35] This specific malware was designed to use a CryptGenRandom function to randomly generate data in the computer.[36] This meant that instead of the final installation string in the code containing encrypted information used to restore the decryption key, it just contained random information.[37] Because of this, users, even if the ransom was paid, could not retrieve their files. This malware ultimately wiped out the information it encrypted.[38] This "flaw" in the NotPetya malware suggests, then, that the motive for the attack was to cause destruction and chaos.[39] Researchers discovered that approximately 70 to 80 percent of the victims in this attack were in Ukraine, with Ukrainian critical infrastructure, government offices, banks, and nuclear power plants being a large portion of the institutions affected.[40] Other major international institutions were also severely affected by NotPetya, such as shipping company Maersk, pharmaceutical company Merck, a FedEx-owned company, and even some Russian institutions.[41] Many of the organisations affected saw their Ukraine offices infected, which then spread to the rest of their networks.[42] An example of this can be found in the FedEx-owned company, TNT Express, that found their Kiev-based office infected with NotPetya, which then infected the rest of their organisation's network.[43] Interestingly, FedEx was also affected in the WannaCry attack, and while it is unknown how NotPetya infiltrated TNT Express' system, it could be posited that they had yet to patch their operating systems and did not ensure their third-party vendors did, as well. It is estimated that NotPetya cost busines-ses at least ten billion USD in damages, if not more.[44]

Suspected Russian Involvement

Following the attack, there was much speculation surrounding the possible perpetrators behind it. Many researchers suspected that Russia sponsored this specific attack. This was because the most substantial amount of affected victims were located within Ukraine due to the careful delivery method of the malware via the Ukrainian tax software, especially its financial, government, and energy sectors, and it was the eve of the Ukrainian national Constitution Day or their Independence Day following the fall of the Soviet

(Accessed June 29 2018)

32 Ibid.; Bradley Barth, "Key researchers reclassify NotPetya as a wiper, suspect destruction was true motive," SC Media US, 2017, https://www.scmagazine.com/key-researchers-reclassify-notpetya-as-a-wiper-suspect-destruction-was-true-motive/article/671940/ (Accessed June 26 2018).

33 Iain Thomson, "Everything you need to know about the Petya, er, NotPetya nasty trashing PCs worldwide," The Register, 2017, https://www.theregister.co.uk/2017/06/28/petya_notpetya_ransomware/?page=3 (Accessed June 22 2018).

34 Ibid.

35 Fred O'Connor, "NotPetya Still Roils Company's Finances, Costing Organizations $1.2 Billion in Revenue," CyberReason, 2017, https://www.cybereason.com/blog/notpetya-costs-companies-1.2-billion-in-revenue (Accessed July 05 2018).

36 Anton Ivanov and Orkhan Mamedov, "ExPetr/Petya/NotPetya is a Wiper, Not Ransomware," SecureList, 2017, https://securelist.com/expetrpetyanotpetya-is-a-wiper-not-ransomware/78902/ (Accessed June 23 2018).

37 Ibid.

38 Ibid.

39 Bradley Barth, "Key researchers reclassify NotPetya as a wiper, suspect destruction was true motive," SC Media US, 2017, https://www.scmagazine.com/key-researchers-reclassify-notpetya-as-a-wiper-suspect-destruction-was-true-motive/article/671940/ (Accessed June 26 2018).

40 Ibid.; Matt Burgess, "What is the Petya ransomware spreading across Europe?," WIRED.co.uk, 2017, https://www.wired.co.uk/article/petya-malware-ransomware-attack-outbreak-june-2017 (Accessed June 24 2018); Thomas Fox-Brewster, "Petya Or NotPetya: Why The Latest Ransomware Is Deadlier Than WannaCry," Forbes, 2017, https://www.forbes.com/sites/thomasbrewster/2017/06/27/petya-notpetya-ransomware-is-more-powerful-than-wannacry/#181b88bb532e (Accessed June 23 2018).

41 Matt Burgess, "What is the Petya ransomware spreading across Europe?," WIRED.co.uk, 2017, https://www.wired.co.uk/article/petya-malware-ransomware-attack-outbreak-june-2017 (Accessed June 24 2018).

42 Nicole Perlroth, Mark Scott and Sheera Frenkel, "Cyberattack Hits Ukraine Then Spreads Internationally," The New York Times, 2017, https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html (Accessed June 23 2018).

43 Eduard Kovacs, "NotPetya Attack Costs Big Companies Millions," SecurityWeek.com, 2018, https://www.securityweek.com/notpetya-attack-costs-big-companies-millions (Accessed June 25 2018).

44 Rich Tehrani, "NotPetya: World's First $10 Billion Malware," Apex Technology Services, 2017, https://www.apextechservices.com/topics/articles/435235-notpetya-worlds-first-10-billion-malware.htm (Accessed June 25 2018).

Union.[45] This indicated that this attack was planned and specifically intended to harm Ukraine. The UK in a statement declared that it was "almost certainly the Russian military behind the attack," which was also corroborated by the US Central Intelligence Agency (CIA), further stating the Kremlin was attempting to continually destabilise Ukraine after the annexation of Crimea in 2014.[46] Not only have the UK and US blamed Russia publicly, the US also implemented sanctions on Russia because of the NotPetya attack, amongst other reasons.[47] Despite this, Russia still denies that it was the perpetrator of NotPetya, as machines in Russia were also affected by the malware.[48] This, however, is rationalised that Russia unintentionally infected themselves because NotPetya was indiscriminate once it was inside a network and the nation has business ties within Ukraine so they inadvertently also ended up harming themselves. Thus, the malware propagated internationally from within the Ukraine which just also happened to then end up in their own systems. Whilst several nations such as the UK, US, Denmark, Lithuania, Estonia, Canada, Australia, New Zealand, Norway, Latvia, Sweden, and Finland have all declared Russia to be culpable, Russia still maintains their innocence. However, there still lacks clear physical evidence to accurately and definitively attribute this attack to any particular actor.

Lessons to Take Away from the Attack

Because NotPetya hit about a month after WannaCry, many organisations were still attempting to recover and revise their cyber security policies and practices. NotPetya highlighted many similar shortcomings within organisation's cyber security policies that WannaCry also exemplified. The attacks utilised the same SMB exploits to propagate in networks that could have both been avoided had organisations simply updated their systems, especially since some organisations were affected by both attacks because of this easy-to-fix vulnerability.[49]

There are some basic recommendations to help mitigate attacks like NotPetya:

1. Use threat intelligence to know what exploits are being used in the wild and work to patch or mitigate those vulnerabilities as efficiently as possible in your organisation.
2. Break up system networks so if a breach occurs, the infected subsystem can only spread the infection to a limited portion of the network.
3. Have an effective backup and recovery plan in place so paying ransoms is not necessary and doesn't reward attackers for holding your organisation hostage.
4. Delivery of regular awareness training regarding social engineering and what to do in case of ransomware attacks.[50]
5. Engage with penetration testing or red teams to regularly perform adversarial simulations against your systems and networks. This helps show flaws in defences ahead of actual breaches.

Basic cyber security practices like these are essential for organisations to create a cyber security foundation that can be further built upon.

NotPetya illustrated several different lessons that are crucial for organisations to recognise and address for lasting resilience against cyber threats. A critical lesson, especially from MEDoc's perspective, is the importance for software update codes to be digitally signed by the host organisation to allow for the code to be verified.[51]

45 "Russian military 'almost certainly' responsible for destructive 2017 cyber attack," National Cyber Security Centre, 2018, https://www.ncsc.gov.uk/news/russian-military-almost-certainly-responsible-destructive-2017-cyber-attack (Accessed August 10 2018); Bradley Barth, "Key researchers reclassify NotPetya as a wiper, suspect destruction was true motive," SC Media US, 2017, https://www.scmagazine.com/key-researchers-reclassify-notpetya-as-a-wiper-suspect-destruction-was-true-motive/article/671940/ (Accessed June 26 2018); Simon Sharwood, "UK names Russia as source of NotPetya, USA follows suit," The Register, 2018, https://www.theregister.co.uk/2018/02/15/uk_names_russian_military_as_source_of_notpetya/ (Accessed August 10 2018).

46 Simon Sharwood, "UK names Russia as source of NotPetya, USA follows suit," The Register, 2018, https://www.theregister.co.uk/2018/02/15/uk_names_russian_military_as_source_of_notpetya/ (Accessed August 10 2018).

47 Zack Whittaker, "US slaps new sanctions on Russia over NotPetya cyberattack, election meddling," ZDNet, 2018, https://www.zdnet.com/article/us-drops-sanctions-on-russia-over-notpetya-cyberattack-election-meddling/ (Accessed August 10 2018).

48 Danny Palmer, "A massive cyberattack is hitting organisations around the world," ZDNet, 2017, https://www.zdnet.com/article/a-massive-cyberattack-is-hitting-organisations-around-the-world/ (Accessed August 10 2018).

49 Rich Tehrani, "NotPetya: World's First $10 Billion Malware," Apex Technology Services, 2017, https://www.apextechservices.com/topics/articles/435235-notpetya-worlds-first-10-billion-malware.htm (Accessed June 25 2018).

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

51 David Cooper, Andrew Regenscheid, Murugiah Souppaya, Christopher Bean, Michael Boyle, Dorothy Cooley, and Michael Jenkins, "Security

This is will ensure the updates are genuinely from who they say they are from, and thus secure and safe to install. This means that organisations that create software for other companies and institutions need to protect the signing key for the code as well as have a secure process that signs the updates and certifies them to be legitimate.[52] Had MEDoc followed this process, threat actors would not have been able to easily access their software update's code, input their own malware into it, and then send off to the vendor's customers.

A particularly important point to note in the NotPetya attack surrounds the organisational policies and procedures that either were not in place or not enforced which contributed to the severity of the impact it had. A common theme found was that many organisations were ill-prepared to deal with an attack on the level of NotPetya and did not have cyber insurance or an appropriate internal equivalent, just in case they found themselves victim to such an attack.[53] Not having cyber insurance also meant that Ukrainian institutions and global organisations not only were without assistance to offset the costs related to the recovery process,[54] but also many lost millions of dollars in revenue that could not be mitigated.[55] The necessity of having cyber insurance has become more apparent to many companies, though not all make the effort to obtain it, or do not have an insurance plan that is proportionate to the amount the organisation could lose from damages. Organisations should utilise cyber insurance on top of current insurance plans, but compounded with insurance, organisations need to establish incident response plans for possible attacks that allocate funds specifically to cover losses from an attack, create recovery contracts and procedures, and have backups that are stored offline. It is imperative to plan for the worst and have strategies already in place so companies can address incidents immediately and effectively minimizing the extent of potential damage.

As seen with WannaCry and here with NotPetya, there is still a long way to go before organisations are resilient in cyberspace. This is due to their organisational policies, practices, and procedures not evolving at a comparable rate to the cyber threat landscape. Organisations need to be more pragmatic and immediate in developing solutions and proactive measures to counteract the current and future cyber threats; not being able to move as quickly as threat actors to address these problems does impede organisations' potential for success in the long-run. Being proactive in recognising who might target a company and, subsequently, how threat actors may target them will be extremely beneficial in combatting those threats to ensure security. Organisations need to learn how to adapt alongside the ever-changing threat landscape as to not fall too far behind cyber threat trends through quicker policy revisions and policy implementation procedures, as well as understand where their own specific vulnerabilities are whether that be employees falling victim to social engineering, inadequate IT infrastructure that does not have robust security, poor cyber security hygiene, or others. Engaging in these practices will better protect companies and their customers to ensure enduring success and cyber protection.

Considerations for Code Signing," National Institute of Standards and Technology (NIST) US Department of Commerce (2018).

52 Ibid.

53 Eduard Kovacs, "NotPetya Attack Costs Big Companies Millions," SecurityWeek.com, 2018, https://www.securityweek.com/notpetya-attack-costs-big-companies-millions (Accessed June 25 2018).

54 Kim Lindros and Ed Tittel, "What is cyber insurance and why you need it," CIO, 2016, https://www.cio.com/article/3065655/cyber-attacks-espionage/what-is-cyber-insurance-and-why-you-need-it.html (Accessed June 28 2018).

55 Fred O'Connor, "NotPetya Still Roils Company's Finances, Costing Organizations $1.2 Billion in Revenue," CyberReason, 2017, https://www.cybereason.com/blog/notpetya-costs-companies-1.2-billion-in-revenue (Accessed July 05 2018).