

By Jordan Lemite, Justin Prosser, Rick Neal, Yahya Forihat

**Table Of Contents:**

Overview of NotPetya: (Page 3-4)

Technical Analysis: (Page 4-5)

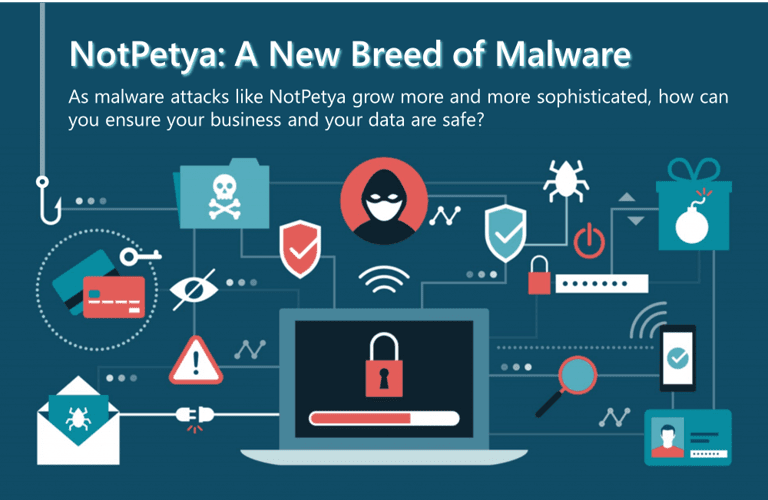
Containment strategy: (Page 5-6)

Awareness Training: (Page 6-7)

References: (Page 8)

Overview of NotPetya:

NotPetya was named after a vicious malware known as Petya. When NotPetya struck its victims, the world thought it was Petya but soon realized it was not. The sheer brutality of the malware dealt more damage to companies than Petya did so they started calling it “NotPetya”. This attack was performed by the Russian military. The Russians struck on June 27th, 2017. They aimed the malware at Maersk, an international shipping giant, hospitals, grocery stores, and even companies like Cadbury, a chocolate company in Australia. NotPetya was aimed at Ukraine, but still managed to affect countries all around the world. Being that this was a targeted attack, only 16,500 machines felt the wrath of the malware. However, people everywhere were affected by it.



NotPetya was thought to be ransomware similar to its eponym, Petya. However, it simply masqueraded itself as such, but was actually a different type of malware called wiperware. Instead of just encrypting a computer’s files until the ransom is paid, NotPetya does something slightly more vicious. Shown in the diagram above, Notpetya starts through a phishing attack, next it begins encryption and asks for you to pay $300 in bitcoin for your files. The rest of the diagram does not seem to be a happy ending where you get the decryption key and rejoice with your files. Even if the ransom was payed, you could not retrieve your files. Wiperware encrypts the entire hard drive for good and deletes all information immediately. This attack cost everyone involved an estimate of $300 billion combined. Due to a mass installation of patches, Notpetya is not as dangerous as it once was. However, there are still many systems that are old and vulnerable to attacks like these.

Technical Analysis:

In order to understand how NotPetya works we need to analyze it from a purely technical perspective. NotPetya was mostly installed by using Spearphishing (using a .doc or a .txt file) and through a Russian backdoor left in the M.E.Doc Servers. Using the backdoor Notpetya was able to install the software onto the targeted computers that ran M.E.Doc Software. It would prompt the user to update the software causing NotPetya to install. From that point the software is designed to run a modified version of Mimikatz in order to comb the database for higher credentials it can then use to install itself. In order to propagate it uses a combination of the credentials and eternal blue to spread from computer to computer. Once NotPetya is able to install it starts rundll32.exe like so: "C:\Windows\System32\rundll32.exe" "C:\Users\admin\AppData\Local\Temp\027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745.exe", #1 . (any.run, 2019) The purpose of this command it is replace the entire directory that Notpetya is installing into with new files that will corrupt your system information. Then it will launch cmd.exe like so /c schtasks /Create /SC once /TN "" /TR "C:\Windows\system32\shutdown.exe /r /f" /ST 01:34 . (any.run, 2019) Essentially in Command line that command is telling schtask.exe (schedule tasks) to schedule a force reboot of the system at 01:34 am local time to install the software properly. Then reason why it is so late is that less people are likely to notice and it unifies what time all the machines will get infected thus affecting the response time. Once the malware is installed your computer pops up with a message asking you to pay a ransom and you lose all your data. NotPetya focused mostly the Ukraine and was launched by Russian Hackers.

Containment Strategy:

**Scope**

NotPetya Malware aims to obtain user credentials in order to propagate itself using Mimikatz tools. It spreads from one device to another using three vulnerabilities: the EternalBlue, Microsoft Office CVE-2017-0199, and an FTP vulnerability on Me. Doc’s server [4]. Instead of holding people information like ransomwares it actually wipes their information. The malware targeted windows computer in 2017, a month after WannaCry ransomware was launched. Maersk is an example of a large company that was attacked by NotPetya, Maersk is the largest shipping company in the world and transport 20% of world trade making them a huge part of our infrastructure. When Maersk got attacked by NotPetya, all of their IT systems paralyzed. They were unable to process credit cards, cargo that is unable to be logged, and entering or exiting ports. They suffered a loss between 250 and 300 million, 49,000 laptops destroyed, 1,200 applications instantly inaccessible, and 1,000 destroyed. They stayed without IT for 10 days and have to overcome with human resilience.

**Solution**

NotPetya spread via phishing or spam emails, so the best way to protect yourself from this malware is to make sure you check an emails content for legitimacy [3]. Moreover, a complete backup of your information is the most important procedure. don’t pay the ransom, you will lose your money because nothing guarantee that you will get your information back. Another important thing is to ensure that your system is fully patched according to the latest security updates. Back to our example, Maersk had to rebuild their entire infrastructure. Within 10 days they were able to have 4,000 servers, 45,000 new PCs, and restore 2,500 applications.

Awareness Training:

It is important to realize that that sometimes the most secure password or the best employee training in the world will not save your data [6], as evidenced in the case of the Maersk NotPetya infection which was distributed through a backdoor, in an automatic update to the MeDoc accounting software [7], and spread within 7 minutes. That said, there are some best practices to consider when developing awareness training. The first is to know that awareness is more than being vigilant before some bad cyber thing is happening. It is being aware that some bad cyber thing IS going to happen, before it actually happens. What you do with that awareness should define your posture. For instance, often service continuity plans and service resumption plans are combined. The danger there, is that you assume you will be able to continue service without planning for what action to take in the event of having NO technology at all [7], not even phones to use. Were you aware of that? Maersk wasn’t, unfortunately [7].

Awareness training is now much more than training people not to click email or web links. [6] It is now the intuitive combination of prevention, identification and quick, cogent, aggressive response.

Awareness considerations include:

Be aware that bad things are going to happen

Train users to spot and report phishing lures. [5]

Maintain a thorough vulnerability management program. [5]

Patch serious vulnerabilities promptly when they are announced. [5]

Make use of basic security controls, e.g., DMARC, spam filters, etc. [5]

Have a service resumption plan. [7]

Have a business continuity plan. [7]

Perform regular, encrypted backups [6] and store them off site, requiring physical methods of retrieving the tapes.

Provide on-going technical training for IT staff.

# References

*any.run*. (2019, 12 13). Retrieved from Anyrun: https://app.any.run/tasks/3551ebae-486f-462a-9f0f-9850d8f30e21

Carrazana, L. (2019, 12 19). *The Economics of Cybersecurity and Cyberwarfare: A Case Study*. Retrieved from austrianstudentconference: http://austrianstudentconference.com/wp-content/uploads/2019/02/ASSC-2019-Lorenzo-Carrazana.pdf

computer weekly. (2019, 12 18). *industry wide lessons*. Retrieved from Computer weekly: https://www.computerweekly.com/news/252464773/NotPetya-offers-industry-wide-lessons-says-Maersks-tech-chief

isbuz. (2019, 12 18). *notpetya most destructive cyber attack*. Retrieved from isbuzz: https://www.informationsecuritybuzz.com/expert-comments/notpetya-two-years-on-from-the-most-destructive-and-costly-cyber-attack-in-history/

lastline. (2019, 12 19). *notpetya ransomware attack*. Retrieved from lastline: https://www.lastline.com/blog/notpetya-ransomware-attack/

mcafee. (2019, 12 18). *Petya*. Retrieved from Mcafee: https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/petya.html

medium. (2019, 12 18). *learning from not petya*. Retrieved from medium: https://medium.com/cyr3con/learning-from-notpetya-43f2fea8994c

mitre. (2019, 12 19). *not petya*. Retrieved from mitre: https://attack.mitre.org/software/S0368/

pei. (2019, 12 18). *modern malware*. Retrieved from pei: https://www.pei.com/modern-malware-notpetya/

phishlabs. (2019, 12 18). *ransonware evolved*. Retrieved from phishlabs: https://info.phishlabs.com/blog/wannacry-notpetya-ransomware-evolved-in-2017

tripwire. (2019, 12 19). *timeline of a ransomware*. Retrieved from tripwire: https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/notpetya-timeline-of-a-ransomworm/

wired. (2019, 12 18). *Notpetya*. Retrieved from wired: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

zdnet. (2019, 12 19). *how many victims are there really*. Retrieved from zdnet: https://www.zdnet.com/article/petya-ransomware-attack-how-many-victims-are-there-really/