**NotPetya Malware Analysis Project**

Daniel Cooper, Nicholas Halsell, Hamzah Khan, David Petit

**I: Overview**

In June 2017, Russian military intelligence launched what Wired magazine would later call “the most devastating cyber attack in history.” The primary target appeared to be the Ukrainian financial sector, but the malware spread around the world, causing massive disruption. In short order, the malware was dubbed NotPetya (because of similarities with the known ransomware Petya, the new malware was initially misidentified as Petya). NotPetya is a Windows-specific piece of malware that irreversibly encrypts a drive’s contents and is capable of autonomously spreading itself through a network. It presents as ransomware, but it is not - the attackers’ goal is disruption and destruction. To initiate the attack, the attackers compromised the update servers of a Ukrainian firm that owns a tax and accounting software, ME Docs, which is used by virtually every company that does business in Ukraine. The attackers then pushed out a fake ME Docs update, immediately infecting untold thousands of machines with NotPetya. The malware then spread itself across networks using EternalBlue, a zero-day exploit that had been stolen from the NSA and released by the Shadow Brokers, a hacking group thought to be linked to Russian intelligence. NotPetya also has an alternate propagation method in Mimikatz, which can be used to dump credentials out of RAM. Within hours of the fake ME Docs update going out, companies and governments around the world were in chaos, desperately trying to mitigate the spread of this particularly pernicious malware.

**II: Aftermath and Effects**

NotPetya caused more than ten billion dollars in damages, according to a White House assessment. To get a sense of the scale of the damage - a ransomware attack that paralyzed the government of Atlanta in March 2017 caused ten million dollars in damages. The worm WannaCry that spread a month before NotPetya cost between four and eight billion dollars.

During the attack, Maersk, a company responsible for nearly eight hundred seafaring vessels with tens of millions of tons of cargo, representing one-fifth of the world’s shipping capacity, was dead in the water. NotPetya hit at least four Ukrainian hospitals, two airports, and twenty-two banks. At least ten percent of all computers in the Ukraine were wiped.

The domain controllers, the servers that function as a detailed map of Maersk’s network and ruleset, were almost lost forever. After searching everywhere for the domain controllers, a copy was finally found in Ghana. Ghana, luckily for Maersk, had experienced a total blackout during the NotPetya attack. Without this copy, the company wouldn’t have been able to recover anything.

Recovery of the network of four thousand servers and forty-five thousand PC’s took ten days. It took two months for the full recovery. The company has since updated every security feature they had, which were lacking. Some servers were running on Windows 2000 at the time of the attack. Maersk lost between two hundred and three hundred million dollars, a figure that is considered low-balled by many.

One week after the NotPetya attack, a Ukranian SWAT team raided the headquarters of the Linkos Group and confiscated the patient zero servers for the attack. Cybersecurity experts still debate whether the attack was motivated by wiping away old evidence of espionage by the Russian government, an act of pure destruction, or as a warning to companies doing business with the Ukraine.

**III: NotPetya Technical Expose**

This is the summary of our analysis of NotPetya. The analysis was performed using both the static and dynamic results from Any.Run.

**Static Analysis**

This malware is an “.exe” file with a size of 3mb. The compilation date of NotPetya was June 17, 2017. Our analysis took place on December 4, 2019. This particular version of the malware seems to only have been involved in a single attack that took place on June 27, 2017, with the Ukraine economic sector being the target. The attack was halted the following day. With the exploits that NotPetya uses, I think that it could still be a threat to unpatched computers. At first glance, NotPetya appears to be a ransomware similar to Petya, but it is, in fact, a wiper virus.

**Initial Behavior**

The table below summarizes the initial activity generated by the sample upon upload to Any.Run.

|  |  |
| --- | --- |
| **Activity Type** | **Count** |
| HTTP Requests | **0** |
| DNS Requests | **0** |
| Connections | **1 UDP** |
| Files Changed | **882** |

**Dynamic Analysis**

The results below were generated by executing the malware sample on Any.Run’s hosted platform.

**Process Environment**

The malware runs all processes as “admin”. The analysis was run on a Windows 7 version 7601. There are a few indicators of suspicious activity, starting with the “.exe” file drop, followed by files being created in the program directory, and the “CMD.EXE” being pulled up to execute commands.

**Network Activity**

The malware sample only made a single UDP connection during the analysis.

The following table describes the servers that the sample communicated with.

|  |  |  |  |
| --- | --- | --- | --- |
| **Request Type** | **Target Domain** | **Target IP** | **Reputation** |
| UDP |  | 192.168.100.209 | Unknown |

**Filesystem Modifications**

NotPetya drops an executable file, then imports a number of “.dll” files into the program directory. These files seem to be what execute the encryption of the computer upon reboot.

**Summary**

NotPetya presents itself as ransomware like its predecessor Petya, however, it is really a wiper worm that works its way through a network encrypting computers and damaging the files beyond repair. The most prominent sign of malicious behavior is the task scheduler being pulled up and edited to reboot in 60 minutes. The malware imports a large number of binaries and “.dll” files to take care of the encryption and spread of the virus throughout a network.

**IV: Containment Strategy / Awareness Training**

Risk mitigation is multi-faceted when it comes to this destructive malware. NotPetya is *not* ransomware, even though it looks like it. Even though it demands ransom to restore files, NotPetya damages data beyond repair. NotPetya is also capable of spreading extremely quickly (within seconds) over a network. For this reason, the most effective measures are preventative instead of reactionary.

The SMB (Server Message Block protocol - a network communication protocol for providing shared access to files, printers, and serial ports between nodes on a network) flaw exploited by EternalBlue should be patched by MS17-010, developed by Microsoft. If this isn’t done, in the case of infection, NotPetya will be able to utilize EternalBlue alongside MimiKatz to proliferate autonomously across a network in a frighteningly short amount of time. When Maersk was infected in 2017, not all of their hardware was running the newest OSs - some servers were running versions of Windows that dated as far back to the year 2000. Having an operating system that is isn’t updated to protect against developing malware is a huge and inherent risk and liability for any firm or organization.

In the event of an outbreak, employees should be briefed on how to quickly respond to the situation. In this case, all employees, no matter what rank or position, should disconnect from the network immediately upon hearing or seeing news of an infection. IT staff should preemptively collaborate with management to design networks that prevent lateral spread of infections. For example, networks should be partitioned, privileges should be segmented, and local admins should not receive maximal privileges at all times. The company or organization’s IT staff and management should also run a robust anti-malware suite and strongly consider investing in two-factor authentication and password managers. Lastly, sensitive and important data should be backed up offline in the event of an outage or complete shutdown. Staff can run programs or regular scheduled cron backups and output the data to physical hard drives that should then be secured and maintained in a safe place in the event of an emergency that could potentially require building a network back from the ground up.

Employees should also be aware of the greater implications of malware like NotPetya. In the Maersk case study, most experts believe that the malware was an act of cyberwar sponsored by a nation-state (Russia) with the intent to cause raw damage to Ukraine. Although Ukraine was the target, the infection caused collateral damage all across the globe. Being aware of the kind of world we live in is hugely important for the management of any kind of firm to consider as they implement IT protocols and hiring practices.

**Sources**

<https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>

[https://securingtomorrow.mcafee.com/mcafee-labs/new-variant-petya-ransomware-spreading-like-wildfire/?\_ga=2.102556866.2128779380.1575468981-823521893.157546898](https://securingtomorrow.mcafee.com/mcafee-labs/new-variant-petya-ransomware-spreading-like-wildfire/?_ga=2.102556866.2128779380.1575468981-823521893.1575468981)

<https://www.csoonline.com/article/3233210/petya-ransomware-and-notpetya-malware-what-you-need-to-know-now.html>

<https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/petya.html>