Darknet Diaries: The NotPetya Attack

Carl Lochstampfor Jr.

Department of Cybersecurity, Old Dominion University,

CYSE 280 - Windows Systems Management and Security, Professor Malik A. Gladden

May 26, 2025

Assignment: Homework 2

Listen to "Episode #54: NotPetya of the DarkNet Diaries podcast which can be found at https://darknetdiaries.com/episode/54Links to an external site.

Based on the podcast, answer the following questions:

1. What tools did the hackers use in this podcast?
2. We know Ukraine was the target, but what was the goal of this Cyberattack?
3. What events happened on Tuesday, June 27th, 2017?
4. What Companies were affected by this NotPetya Attack?

<u>Darknet Diaries:</u> The NotPetya Attack

What tools did the hackers use in this podcast?

The hackers used four tools and methods for the (Not)Petya cyberattack in June 2017: a worm with ransomware, Mimikatz, and EternalBlue (Rhysider, 2019). A Worm is a standalone, self-replicating program (like a virus) that spreads and infects many other computers and networks without the need for user interaction or consent, usually disrupting a network's normal traffic while infecting the assets of the computers within the network(s). Second, Ransomware is a type of malicious software designed to block access to a computer system or its data/assets by encrypting it until the victim pays a ransom to the attacker with a 'promise' to decrypt the victim's assets. The infection includes the master reboot record, allowing the virus to instruct the machine to reboot immediately, and upon rebooting, the virus will encrypt that file system. The encryption prevents access for its original users and thereby rendering the system unusable and indirectly "destroyed" unless the ransom is paid to the attackers to decrypt it.

Third, Mimikatz is an open-source tool to conduct vulnerability assessments in Microsoft Authentication protocols, particularly in how login credentials are stored in the memory (sometimes in plaintext) by extracting the usernames and passwords or even their hashes or tokens to gain unauthorized access to the target's computer and network. Lastly, EternalBlue is a software exploit developed by the U.S. National Security Agency (NSA), which was later leaked by the Shadow Brokers hacking group in April 2017. It targets a vulnerability in Microsoft Windows Server Message Block (SMB) protocol that allows computers to share data between themselves, specifically versions 1.0 to 3.0. Attackers remotely execute arbitrary code without authentication, passing by any/all login credentials to gain direct access to workstations and networks.

We know Ukraine was the target, but what was the goal of this Cyberattack?

The goal of Russia's state-sponsored NotPetya cyberattack was to permanently shut down and render Ukraine's cyber infrastructure unusable/useless, providing a gateway or path to occupy and grab more land using Russian troops physically. The attack was the climax of a series of attacks against Ukraine over many decades (since World War II). There is a long-standing history of bloody conflict between Russia and Ukraine, with Russia declaring sovereignty over Ukraine and laying claim to territory within Ukraine, particularly Crimea and its surrounding area. Thus, the NotPetya cyberattacks primary purpose was to use a worm posing as ransomware to cause mayhem and destruction on Ukraine's cyber and physical infrastructure, advancing Russia's interest in seizing control over more of Ukraine's overall infrastructure and land.

What events happened on Tuesday, June 27th, 2017?

To better understand the dangerous purpose, events, and consequences of the June 27th, 2017 cyberattack, we need to understand *how* Mimikatz and EternalBlue work together (Rhysider, 2019). First, hackers will attempt to transport a Worm onto a target system and infect it. Next, the hackers will run Mimikatz to search for and steal any/all stored usernames, passwords, and other login credentials (i.e., hashes and tokens) that have logged into that computer. With those login credentials, the Worm will use them to spread and infect other neighboring computers within that network. The Worm will continue this expansion, scooping up all login credentials along its path that are associated with each computer its infected and using it to 'jump' to more external networks and computers. Eventually, the Worm passes data/assets onto the hacker. However, in the case of the NotPetya attack, the hackers went one step further by running ransomware with a twist.

However, what if Mimikatz cannot find or access any login credentials at the front end of the attack within a target's computer or network? The hackers can then use EternalBlue to see if the Windows system is patched and attempt to exploit any/all vulnerabilities without user interaction. EternalBlue will send a uniquely crafted packet to a vulnerable system to gain privileged access to the target's kernel-level access, allowing the attacker to execute remote code like malicious software. Therefore, the attacker will run Mimikatz after EternalBlue's assistance and infect computers with the Worm and Ransomware by stealing the targets' login credentials.

In the NotPetya attack, hackers targeted as many Ukrainian government institutions, businesses, and citizens as possible to render them useless and to effectively shutdown Ukraine's entire cyber and physical infrastructure forcing everyone to operate within the 'dark.' The cyberattack effectively 'destroyed' the targeted computers and networks by infecting a well-known and used tax-filing software called MeDoc (Rhysider, 2019). Using MeDoc as an instrument of destruction, the hackers targeted a small business called Linkos Group, which uses the MeDoc. The hackers hijacked and infiltrated MeDoc to take control of its servers and push out their malware to Ukrainians, seeking only to target Ukrainians and not the rest of the world. However, the malicious software traveled beyond the country's borders to completely shut down many other government and business computers and networks.

What Companies were affected by this NotPetya Attack?

Malicious software negatively impacts many government institutions, businesses, and citizens. First, within Ukraine, banks like Oschadbank experienced simultaneous full-day nationwide system shutdowns and lockouts among employees and customers. The post office, hospitals, utility companies, and many other financial institutions in Ukraine were negatively impacted, too. One researcher estimated that more than three hundred companies were brought down by the virus, potentially costing over ten billion dollars globally and taking days if not weeks or months for governments and companies to fully recover. Second, the virus moved beyond the Ukrainian border and infected numerous multinational companies, preventing them from conducting transactions and even sending out basic communications to employees through email or VoIP. Some multinational companies infected and/or negatively impacted by the virus include FedEx, Maersk, Merck, Sait-Gobain, and Reckitt Benckiser. The virus impacted almost every type of business industry in the global economy, ranging from finance, logistics and transportation, medical services and pharmaceuticals, manufacturing, and foreign government networks like the U.S., U.K., France, and Germany.

References

Jack, Rhysider (Host). (2019, October 8). NotPetya (No. 54) [Audio podcast episode]. In DarkNet Diaries. https://darknetdiaries.com/episode/54