CYSE 280 - Windows Systems Management and Security

Professor Malik A. Gladden

Homework 2

Short Answer Questions (short answers should generally be at least three to four sentences in length. However, it is important to be as concise as possible when responding.) or you may choose to **Upload a Two-Minute Audio or Video recording** to answer the following questions.

Listen to “Episode #54: NotPetya of the DarkNet Diaries podcast which can be found at https://darknetdiaries.com/episode/54/

Based on the podcast, answer the following questions.

1. What were the primary tools and techniques used in the NotPetya cyber-attack, and why were they particularly effective?

According to the podcast, the attackers wanted to create a worm starting with Mimikatz. Mimikatz can take the clear text stored and display it to anyone. According to Jack, Mimikatz can see the username and password of anyone who has sat down at the device since it was rebooted. The attackers also used another tool called EternalBlue which was posted on the internet by a mysterious group called Shadow Brokers. Once Mimikatz found its way into the system, it could get the usernames and passwords, try to log into the neighbor devices, and gather the usernames stored on those devices as well. If they could not log in with the usernames and passwords, EternalBlue would see if the system did not have a patch and then exploit it.

2. How did the attackers ensure that the NotPetya worm primarily targeted Ukraine, and what was the initial infection vector?

It was expressed early in the podcast that the goal was for the worm to take out as many devices as it could. The offenders wanted to take out all of Ukraine's network no matter the business. The intention was not for it to spread worldwide and stay in Ukraine, but that was not the case. The attack spread to the US, Russia, Copenhagen, and many others.

3. What were the broader global consequences of the NotPetya attack, and which major companies were impacted?

A better question could be which companies were not affected. While the attack was meant to stay local, the computer attacks do not know boundaries and borders as pointed out. The first affected was the Linkos Group, but also a formal national bank of Ukraine called Oschadbank. Some others mentioned to have been affected were FedEx, Merck, Saint-Gobain, Reckitt Benckiser, Mondelez, Rosneft, EVRAZ, etc. The largest company affected was Maersk which is the largest shipping company in the world. Any organization that coordinated with that company had the MeDoc software then was affected.

4. Why was the NotPetya attack ultimately classified as an act of cyber-war, and what evidence pointed to Russian involvement?

Due to the damages being estimated to have cost over ten billion dollars, this was labeled the largest cyber-attack to have ever occurred. A Slovakian cyber-security firm ESET looked through the records of the attack and analyzed it finding evidential ties to Sandworm. Nine months after a statement was released by the White House stating it was the worst cyber-attack in history and that the Russian military was behind the attack. There are still questions on whether Russia was the attacker, but with other countries stating similar releases that has limited Andy's doubt.

Resources:

NotPetya – Darknet Diaries. (n.d.). https://darknetdiaries.com/transcript/54/