Clarence Kimbrell Jr.

CYSE 280 – Windows Systems Management and Security
Professor Malik A. Gladden
Homework 2

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

Based on the podcast, answer the following questions.

1. What tools did the hackers use in this podcast?

The hackers in this podcast used a tool called Mimikatz. Which was a worm that self-replicated onto other computers to take them offline permanently. This program uses an executable file that stores usernames and passwords in clear text in the memory. This was later used to send that information off without the user having any indication of it doing so. The creators of the program continued to improve it and still a hassle for Windows to fix. There was another tool called Eternal Blue which is arguably the strongest tool of the three that were used.

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

The goal of the cyberattack was to have a worm infect as many computers as possible and destroy them. The overall goal was to permanently destroy as many computers in the country as possible. This would encrypt everything on a computer so it was inaccessible unless you had the decryption key. Then is called ransomware and the hackers in this incident used a ransomware program called Petya. This program and the work were used at the same time to infect and destroy as many computers as possible.

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

On June 27th, 2017, the hackers that attacked Ukraine used software that was used by nearly everyone in the country. They infected the software with the worm, blue enteral, and Petya. This created a country-wide attack that was only concentrated in Ukraine. MeDoc was a tax software that allowed people to do their taxes with this program. This was the host of the attack which targeted Ukrainian individuals.

4. What Companies were affected by this NotPetya Attack?

One major company that was affected by the attacks was a family-run software business called Linkos Group. Within minutes banks and government buildings around Ukraine were taken down and encrypted. Another huge company that was hit by this attack was Oschadbank which was the former national bank of Ukraine. This locked 90% of its computers and demanded large sums of Bitcoin to unlock them. Or just destroy the computer internally. Investigators figured out

that even if the sum of bitcoin was paid you were never getting the files back or access to the computers. Some reports suggest that more than 300 hundred companies were affected by this single attack. This even spread across the world infecting US-based companies like Merck and FedEx.