Jasmyn Wilhelm 19 September 2024

CYSE 280 - Windows Systems Management and Security

Professor Malik A. Gladden

Homework 4

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 #77: Olympic Destroyer of the DarkNet Diaries podcast which can be found at https://darknetdiaries.com/episode/77/

Based on the podcast, answer the following questions.

1. **Explain the process used by the IT Staff with the help of AhnLab to defeat the Malware.**

Similar to a chess game, the IT staff spent many hours attempting to rebuild the system, but it would be wiped again as soon as it was built. The malware was found in a file labeled 'winlogon.exe', which is a legitimate process used in Windows, making it more difficult for the IT staff to detect.

With the help of AhnLab, the team was able to 'create a signature' to isolate the malware. After resetting the employee security passwords, they believe the worm was safely ejected and blocked from future access. The process of locating and cleansing the virus took approximately twelve hours. It was not until this occurred that the team could begin using the backups to rebuild the servers and restart all systems.

2. **What individual or group was responsible for the strike against the Olympic Operating Systems, and what was their motive?**

The false leads and sophistication of the attack made it difficult to pinpoint the legitimate offenders. Many signs showed 3 possible leaders behind the attack, such as China, North Korea, and Russia. It took many hours and individuals analyzing the malware after it was uploaded to VirusTotal to accurately narrow down a suspect. An analyst at FireEye, named Michael Matonis, was able to find this lead by going down many 'rabbit holes' showing connections to the 2016 US election tampering and many Ukrainian attacks. Russia is known to purposely attack Ukraine, and with a warning from the FBI in 2017 stating for users to beware of the domain used in both the US election tampering and the attack at the 2018 Olympics, it became clear Russia was behind the attack.

3. **What was the name of the Threat Intelligence Team that gave the worm the name "Olympic Destroyer?**

Many teams, including an individualized group, apart of the Cisco organization, named Cisco Talos, were one of those teams examining the malware file uploaded to VirusTotal. This group named the virus, what is now known as the 'Olympic Destroyer'. This type of attack had never been seen before on VirusTotal and therefore had no name, which added another layer of difficulty in identifying the hackers.

4. **What was the specific component that Sandworm was targeting at the Olympics?**

Two years after the 2018 Olympics took place, the FBI released a statement of six names involved in the event along with acknowledging their crimes with the 2018 Olympics and the 2016 Elections. The goal of this attack was to punish the Olympic team for disqualifying Russia due to faking drug tests and taking illegal substances to provide advantages in events. A specific target at the events was the timekeeping partners in charge of the 2018 Olympic events.

Resources

Olympic Destroyer – Darknet Diaries. (n.d.). https://darknetdiaries.com/transcript/77/