Module 3

And

Episode # 77: Olympic Destroyer

Carl Lochstampfor Jr.

Department of Cybersecurity, Old Dominion University,

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

June 12, 2025

Short Answer Questions: Short answers should typically be three to four sentences long. It is crucial to be concise while providing a thorough response. Alternatively, you have the option to upload a two-minute audio or video recording to answer the questions.

Listen to "Episode #77: Olympic Destroyer of the DarkNet Diaries podcast which can be found at https://darknetdiaries.com/episode/77/Links to an external site.

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.

AhnLab (a South Korean cybersecurity firm) and the Olympics IT staff worked to mitigate the Olympic Destroyer malware. The malware wiped domain controllers, rendering much of the network unusable. The process to defeat the malware likely involved several key steps:

- **Identification and Containment:** they focused on identifying the malware by monitoring its behavior, which included stealing passwords and spreading across the network to delete boot configurations and disable Windows services. The malware was a Worm and was later revealed to have been installed through a series of clicked links and downloaded malware files through phishing emails. Throughout the night and early morning of the incident, they worked to isolate infected systems to prevent further spread.
- **Analysis and Reverse Engineering:** The company analyzed the malware's components, which resembled those of previous attacks such as NotPetya and Bad Rabbit, to understand its propagation methods and destructive payload. With the help of other IT researchers and professionals, they examined various components, including metadata and rich headers, forged but identical digital signatures, and delivery mechanisms. They eventually discovered the source of the malware called winlogon.exe: it is also the name of a real and critical process within Windows. The virus was hiding in 'broad daylight' for an extended period before the Olympic cyberattack, mirroring a Logic Bomb event.
- **Restoration of Systems:** The team focused on restoring the wiped domain controllers. The team implemented a series of temporary solutions to ensure the Olympic Opening Ceremony concluded and all visitors and athletes could safely exit the venue and return to their accommodations. Afterward, the team frantically rebuilt the network infrastructure, restored backups, and redeployed clean systems to regain control of the Olympics' digital environment.
- **Collaboration and Response:** AhnLab and the Olympic IT staff worked with other security firms to deploy technical countermeasures, including updating antivirus signatures and network security patches, to block the malware's remote access capabilities. For example, during the fight against the malware, someone uploaded the malware to VirusTotal, a premium website that can tell you more information about the malware. The information is open to other premium members, and multiple threat research companies have begun analyzing it to assist the Olympic IT staff and AhnLab (i.e., Cisco).

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

The group responsible for the Olympic Destroyer attack was Sandworm, a Russian state-sponsored hacking group linked to the GRU (Russia's military intelligence agency). The motive for the attack was likely geopolitical retaliation, but it remains somewhat of a mystery to this day. IT professionals and authorities viewed the attack as a targeted response against the International Olympic Committee and its ban on Russian athletes competing under their national flag at the 2018 Winter Olympics. Russia and its athletes were banned because of the state-sponsored doping scandal among their athletes. The cyberattack targeted and disrupted the Olympics' operations, attempting to manipulate athletes' scores in real-time, embarrassing South Korea (a U.S. ally) and demonstrating Russia's cyber capabilities. The malware's destructive nature targeted critical infrastructure, closely following the pattern of Sandworm's history of disruptive, politically motivated, and strategically focused cyberattacks. It was later discovered and released to the public that Sandstorm was responsible for other cyberattacks, such as NotPetya and the 2016 U.S. Presidential Election.

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

The Threat Intelligence Team, which named the worm "Olympic Destroyer," was Talos, Cisco's cybersecurity research group. Talos analyzed the malware during the attack and coined the term based on its targeting of the Pyeongchang Winter Olympics.

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

Sandworm targeted the domain controllers of the Olympics's digital infrastructure in Pyeongchang, South Korea. These servers are critical for managing network authentication and access, and the malware repeatedly wiped them, rendering much of the network unusable. By targeting the domain controllers, Sandworm sought to disrupt the core operations of the Olympic network, including ticketing, broadcasting, and other critical services.