Episode #77: Olympic Destroyer of the DarkNet Diaries podcast

Based on the podcast, answer the following questions

1. What immediate impact did the Olympic Destroyer malware have on the 2018 Winter Olympics' IT infrastructure?

The Olympic Destroyer malware took down a huge number of devices such as PCs, networks, etc. It also caused the visitors, competitors, and staffers to be unable to enter the stadium because the ticket booths were broken as well. In addition to this the wifi was down, which delayed media reporting of the opening ceremony. Worse of all, it wiped all of the domain controllers used, destroying the 2018 Winter Olympics' IT infrastructure.

2. What were some of the key challenges faced by the IT staff during the cyber-attack, and how did they respond?

The key challenges that the IT staff had to deal with were trying to evict the hacker, rebuild the domain controllers, and figuring out what the malware was. They responded by trying to rebuild the domain controllers, but the malware wiped all of them out again. So, they decided to get help from a South Korean security company to reboot all of the devices for the olympics. They made sure that the hackers were not able to get back into the systems, so that it didn't happen again.

3. Why was the attribution of the Olympic Destroyer attack so difficult, and what did investigators discover about its origin?

The attribution of the Olympic Destroyer attack was so difficult because the techniques used were not familiar to a specific country or hacker group. For example, there was Chinese code written in the malware but they couldn't rule out North Korea and Russia either since there was also evidence that they could've done it. The investigators discovered that it was called "winlogon.exe", normally this file is in the windows system but this time it was actually a malicious worm. They found out the domain of account-loginserve.com came from the Russia 2016 hacking incident, which pin-pointed it to them being the ones who did it.

4. What evidence pointed to Russia's involvement in the Olympic Destroyer attack, and how did researchers eventually confirm their responsibility?

One of the many pieces of evidence that pointed to Russia’s involvement in the Olympic Destroyer attack is that the Russian government denied that they did the attack before it even happened. Another piece of evidence is that Russia’s team was disqualified previously because they were caught “doping”. The domain from the infected word files was used in a previous attack by russian hackers. account-loginserve.com was the same domain used to target Ukraine’s LGBT activists groups and the 2016 Presidential election, leading them to conclude that the same Russian hacker group was responsible for the Olympic Destroyer malware.