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

- The Primary tools used in the NotPatya attack were EternalBlue & Mimikatz. These tools were effective because Mimikatz would read unencrypted files from the Lsas database and get them into computers that way. If Mimikatz didn't work then the worm would move onto EternalBlue. This would in turn allow the computer to be fully taken over through an exploit that disallowed the computer to communicate to itself internally. This exploit would give hackers full access to any computer that hasn't been recently updated.

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

- First, The hackers had to specifically choose a target that would help the spread of the worm. To make sure the worm was going to impact Ukraine they chose a small company named Linkos Group. On the 3rd floor, they had a server running the updates for tax software by Medoc. The hackers infiltrated the server to push malicious code to everyone who was running the tax software. This would mean essentially every citizen who actively files their taxes on that software and updates it at that time would get infected. In all, we can tell that the worm was targeting Ukraine because it targeted their tax software which would mainly only have Ukrainian citizens on it.

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

- The major border consequence of the worm was that borders mean nothing to a virtual worm. Any computer that had this software downloaded had been infected with the worm and subsequently had their computer shut down and then held for ransom. One major company affected by this worm was Merx Danish Company. They had one office with only one computer with Medoc installed on it. This led to one of the biggest shipping companies being shut down.

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

- The reason it was classified as a cyber-war is because it was used in a way to shut down an entire government. They declared the Ukrainian government dead and essentially killed off all of its governing sectors and parts of the main economy. They also

believe it to be an act of cyberwarfare because of the increased tensions between Russia and Ukraine. Some other evidence they have is that when Merx Danish Company was in talks with the hacker to get their systems back online they would only speak in Russian. Lastly, after a couple of days the “Five Eyes” Intelligence agency all at the same time confirmed and reprimanded Russia for the attack all at the same time.