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

There are many tools that the Russians used, to spread their worm virus, one of them being, Mimikatz. Mimikatz is a open source tool that was created by French researcher Benjamin Delpy, that passes through windows computers, main security program called Lsass.exe, and extracts the username and the passwords of users in clear text, through the windows Lsass memory, and it can be used to pass hashes and tokens. The second tool that was used in this attack, was a ransomware, that was a modified version of Petya. this tool would affect the master boot record and ask the system to reboot, and upon rebooting it would encrypt the file system, so the system is completely shut, until the individual targeted, where to pay a ransomware to free the system. third tool that was used in this cyber-attack, was eternal blue, which was a tool that was created by the NSA and was leaked by a group called the shadow brokers. Eternal blue was a tool that was used to exploit, the windows function called server message block, which essentially allowed computers to share information amongst one another. Eternal Blue could effectively run code remotely on every computer running Windows that was vulnerable, anywhere in the globe by taking advantage of the SMB vulnerability.

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

The goals of this attack was to destroy as many computers as possible, that were on Ukrainian servers. This included all businesses, government agencies, and even individual citizens that were targeted by this worm ransomware, to have their computers destroyed. Furthermore, the Russians wanted to contain this cyber-attack, to only be in Ukraine.

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

on this date, the group of Russian hackers, were able to exploit the update server, of Medoc's, which was Ukraine's main software that was used for filing taxes, and where able to upload their own malware, which caused everyone around the world who had Medoc's installed, to develop the worm virus of Notpetya. Once the seed was planted, the virus had spread quickly effecting thousands of Ukraine computers, by using tactics such as, grabbing the usernames and passwords and trying to log into other neighboring computers, and using eternal blue for computers they didn't have a password for, and upon this step the computers were encrypted and rebooted. Furthermore, the computers, where down at banks, in which nobody could withdraw or even deposit their money, and over 300 Ukrainian businesses were affected, by this cyber-attack. This was a major disaster for Ukrainian citizens, in which they were not able to withdraw money, to purchase subway tickets, or even go to the grocery store to shop for home essentials, and airports and hospitals were also affected. This lethal ransomware also knocked down around 17 ports, that were all around the world, owned by Maersk's, which caused many trucks and cargo ships, to be on standby for delivering their goods.

4: What Companies were affected by this NotPetya Attack?

There were many major companies, that were affected by this cyber-attack, that were outside of the borders of Ukraine, that used the software tool medocs. This included companies such as FedEx, which is one of Americas largest shipping companies, Maersk, which is the world's

largest shipping firm, Merck, the New Jersey-based pharmaceutical company, Saint-Gobain, one of Frances largest construction firms, Reckitt Benckiser, which is a UK manufacturing firm, and Mondelez, which is the food company that owns Nabisco and Cadbury.