Homework #9

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

- The attackers used tools like Mimikatz to grab clear text credentials from Windows systems, and EternalBlue (an exploit leaked from the NSA) to propagate rapidly across networks. They built a worm style malware that didn't just lock files for ransom but destroyed systems, making it far more destructive. The techniques were effective because they combined credential theft, unpatched exploit, plus self replication, meaning even well-protected machines were quickly compromised if they had those weaknesses. Finally, the attack masked itself as ransomware but its real goal was destruction, so traditional defenses and response strategies were less effective.

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

- The attackers hijacked the update mechanism of a widely used Ukrainian accounting software called MeDoc. That allowed them to push the malware through a trusted channel in Ukraine, ensuring many Ukrainian organizations received the malicious update. While the worm quickly spread globally, the design and timing indicated Ukraine was the primary target. By using a software update mechanism for an application heavily used in Ukraine, the initial infection vector was trusted software update compromise.

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

- Although Ukraine was the target, the worm spread worldwide and ended up costing billions of dollars in damages. Major companies impacted included Maersk (a global shipping firm), Merck (a major pharmaceutical company), and FedEx among others. The attack disrupted shipping, manufacturing, financial services and many critical operations across multiple countries. It demonstrated how a cyber attack intended for one country can ripple globally, damaging supply chains and business continuity.

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

- The scale, intent and destructive nature of the attack helped classify it as cyber war: it targeted a country's infrastructure, caused mass disruption, and used nation-state level resources. Forensic investigations by firms like ESET linked the malware to the Russian military hacker group known as Sandworm Team, which had carried out previous attacks against Ukraine. Further, governments (including the "Five Eyes" intelligence alliance) publicly attributed the attack to Russia's military intelligence agency. The combination of strategic targeting, state backed actor linking and massive impact justified calling it cyber-war rather than a typical cyber crime.