DAN OTIENO

CPE 449-01.

09/23/23.

ASSIGNMENT: The Untold Story of NotPetya, the Most Devastating Cyberattack in History.

1. How did NotPetya first gain a foot hold in organizations' computers?
    - Hackers infiltrated a Ukrainian company's update servers and exploited a hidden backdoor to inject NotPetya into their systems.
2. Why do EternalBlue and Mimikatz combined make virulent combination? How does this relate to vulnerability patch windows?
    - EternalBlue and Mimikatz combine virulently because they can both be used to develop malware that can pull passwords from the RAMs of unpatched machines and use them to infect machines that have been patched. This means that while some Windows machines had been patched, they could steal be breached using passwords grabbed from unpatched machines.
3. Who or what was the target of NotPetya?
    - NotPetya was released to target Ukraine as an act of Cyberwar.
4. What collateral damage occurred from NotPetya?
    - The Malware spread globally across a vast network of company servers with devastating speed. It affected major companies across several countries across different sectors, hospitals, resulting in global damages worth $10 billion.
5. In your estimation which had a greater cost, the damage that occurred to the intended target or the damage collateral damage?
    - The collateral damage was greater. Although the attack was intended to hit Ukraine, the resulting spread across multiple global networks and momentarily crippled the global economy, its also worth noting that this could've potentially cost human lives where hospital systems were hit.
6. What saved the Maersk domain controllers and why were they critical to recovery?
    - A single domain controller located in Ghana had survived the attack because it was offline (due to a power outage) when NotPetya struck. These controllers were critical because they mapped Maersk's entire network and defined all user system access permissions. If Maersk had been unable to recover the domain controllers, they wouldn't have recovered anything else, the entire company server structure would've been permanently wiped out.