Ukraine Power Grid Attack

Miles Anderson

Old Dominion University

CYSE 300: Introduction to Cybersecurity

Dr. Joseph Kovacic

January 21, 2024

Ukraine power companies experienced multiple blackouts on December 23rd, 2015 that affected a large number of people throughout the country ("Cyber-Attack", 2021). Although many may have thought this was a typical power outage, it was the work of a planned out cyber attack. Cyber attacks against critical infrastructure are particularly dangerous because they can severely impact how a community functions. Moreover, the lack of power for even 24 hours can easily cause financial loss and mass panic. In regards to the Ukraine Power Grid Attack, professionals discovered vulnerabilities that led to the presence of malware, several repercussions including the corruption of critical systems, and a newfound sense for cyber security practices to mitigate an attack like this in the future.

The cyber attack on the Ukraine Power Grid was more than an ordinary cyber crime. In truth, it was a coordinated attack against three power companies in the span of 30 minutes ("Cyber-Attack", 2021). Though these companies may have had some defenses in place, they left themselves vulnerable by being incapable of defending themselves against a synchronized attack. Consequently, power systems were all compromised at the same time, increasing the size of the blackout by drastic measures. In addition, each company was infected with BlackEnergy malware through spear phishing emails ("Cyber-Attack", 2021). Though the effects of the BlackEnergy Malware have not been fully identified, it is suspected that it was used as an entry point to infect and compromise the company's power systems ("Cyber-Attack", 2021).

The cyber criminals made use of the KillDisk malware to execute their attack by taking advantage of the system's master boot record ("Cyber-Attack", 2021). The KillDisk malware is a malicious software that deletes files and corrupts the master reboot record ('Cyber-Attack", 2021). The master reboot record left the companies extremely vulnerable. Once it was overwritten with the KillDisk malware, it rendered systems completely inoperable. The KillDisk

malware also infected itself within HMIs to cause further disruption and damage (“Cyber-Attack”, 2021).

Due to the power outages, nearly 225,000 customers were affected (“Cyber-Attack”, 2021). A blackout affecting this many people can have multiple repercussions. Blackouts can cause food spoilage and water contamination, as well as disrupt the operations of grocery stores and other businesses (“Power Outages”, 2023). In addition, this attack was conducted in December, so it is likely that citizens were left in freezing cold homes with no air conditioning whatsoever. Finally, backouts can disrupt communications and transportation, which can endanger the lives of individuals traveling by car or other vehicles (“Power Outages”, 2023).

There are multiple steps that could have been taken to mitigate a synchronized cyber attack such as this one. For example, plans and policies need to be in place in case the Industrial Control System (ICS) is compromised (‘Cyber-Attack”, 2021). Very limited remote access functionality should also be paired with strong multi-factor authentication to avoid unauthorized personnel from accessing systems. Finally, employees need to be wary of spear phishing emails that contain malware. They need to recognize the signs of a phishing attempt, such as receiving an email that contains an unknown link or downloadable software. If these phishing attempts were spotted and shut down, it’s likely that the cyber attack would never have happened.

The synchronized attack on the Ukraine Power Grid was a major threat that affected hundreds of thousands of individuals. Companies were targeted in the span of 30 minutes, had their systems compromised, and left approximately 225,00 people without power (“Cyber-Attack”, 2021). Attacks on critical infrastructure can have absolutely devastating consequences. To mitigate long lasting damages and financial loss, companies need to prioritize their defense policies, thoroughly train employees, and observe their systems with a keen eye.

Cybersecurity professionals will use this cyber attack as an example in order to better protect power systems and critical infrastructure across the globe.

References

Cyber-Attack Against Ukrainian Critical Infrastructure. (2021, July 20). Cybersecurity & Infrastructure Security Agency. https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01.

Power Outages. (2023, February 9). Ready. https://www.ready.gov/power-outages#:~:text=A%20power%20outage%20may%3A,food%20spoilage%20and%20water%20contamination.