**Human Security**

Shiva Sindhu Poloju

Department of Information Technology, Pittsburg State University

23SP-GRT-714-01: Network Admin Concepts

Dr. Derrel Fincher

April 24 th, 2023

**HUMAN SECURITY**

**POWER GRID CYBER ATTACK IN UKRAINE**

**Introduction:**

A successful cyber-attack which caused a significant impact to Ukraine’s critical energy structure on 23 December 2015. The temporary malfunction of power supply in three Western oblasts of Ukraine. The Russian hackers targeted a power distribution center outside Kyiv which is Ukraine's capital, a home to 3 million people.

**What led to the event of 23 December 2015:**

On December 23, 2015, and December 17, 2016, there were outages in Ukraine's capital city Kyiv. At the end of the shift, a worker lost control of his cursor, which triggered the circuit breakers. This caused the power substations to go offline. The fight continued and he found himself logged out of the system and his password was changed. By the end of this, the hackers had taken 20 substations offline and put more than 2.3lakh residence of Kyiv into darkness.

**Preparation for the attack:**

The preparation of attack took several days. It started with delivering malware via spear phishing emails with malicious attachments. They establish footholds to obtain credentials, and increased access to other parts of the network. Later investigations have revealed that the attack had been planned over months and the reason for weakness in the system that allowed the hackers to penetrate the systems was that remote VPN logins were linked to grid control networks and lack of two factor authentication. The supervisory control and data acquisition network that controlled the grid weren’t required to use two-factor authentication, which allowed the attackers to hijack their credentials and gain crucial access to system’s that controlled the breakers. Power was out for only 1 to 6 hours but months after that the systems were not fully operational because the hackers over road firmware on critical devices making them irresponsible to remote commands, the workers were controlling the circuit breakers manually. The initial intrusion was done through a spear phishing attack against the staff. A spear phishing campaign is an extremely targeted attack where the hackers get users to click on a link or a file depending on their profile for an instance. If they know that the user enjoys pet videos, they’ll send one of those to them. So, in this case there were infected word files that prompted the victims to enable macros through which a backdoor successfully enabled their computers. The phishing campaign had delivered emails to the workers at three of the companies with an infected word document attached. When workers clicked on the attachment, a popup displayed asking them to enable macros for the document. If they complied, a program called BlackEnergy3 variants of which have infected other systems. The method is notable because most intrusions these days exploit a coding mistake in a software program.

The hackers targeted the ups at the control centers. That means that not just the customers were in the dark, but the operators who were to get the systems back online were in the dark, during the reconnaissance phase, the attacker’s studies each of them carefully. Then, they wrote malicious firmware to replace the legitimate firmware on the ethernet converters at more than a dozen substation. They used the converts to process commands sent from the SCADA network to the substations control systems. Taking out the converters would prevent operators from spending remote commands to re-close breakers once a blackout occurred. They launched the telephone denial of service attack which means that customers couldn’t contact the helpline centers to report the power outage. After they had done this, they used a piece of malware called KillDisk to delete files from operator stations to make them inoperable as well. KillDisk deletes or overwrites data in essential system files, causing computers to crash. Because it also overwrites the master boot record, the infected computers could not reboot. They used KillDisk malware to rewrite master boot record of computers with zeros so they could not reboot. Some of the KillDisk components had to be set off manually, but in two cases the attackers used a logic bomb that launched KillDisk automatically around 90 minutes into the attack. So that it will be around 2 hours extra. Twelve months later when the hackers struck again, they were even more sophisticated instead of going after distribution centers, they went after Kyiv transmission centers. It carried 200 megawatts of more load than all the distribution centers attacked a year earlier, this time instead of using a mouse, the malware could send the commands directly to the grids equipment's using its control system protocols, this can quickly reconfigured to attack any PowerGrid, power came back within an hour or else it had been a much worse instead of nearly turning it off the malware could have destroyed critical grid equipment, Researches found the malware contained code designed to target electrical line and transformer.

**Response from utility:**

Future, the power utility, responded by going to manual control after the loss of their SCADA systems and engineers had to travel to the effective substations to close the breakers and power was restored.

**Conclusion:**

These cyberattacks provide a window into how sophisticated the nation-based hackers can be. A vast potential of damage can still occur without a single soldier stepping on the soil of the victim nation. Countries must work to establish proper defense for their cyberspace by using antivirus software's to protect against malwares, staying alert, avoiding clicking on suspicious links, using strong passwords, and training the staff.

**References:**

Cluley, Graham. (n.d.). The phishing swindle that conned $100 million out of google and facebook.<https://www.bitdefender.com/blog/hotforsecurity/the-phishing-swindle-that-conned-100-million-out-of-google-and-facebook/>

James, E.S., & Lee, T.B. (2015, January 20). The 2014 Sony hacks, explained. Vox. Retrieved April 4, 2023, from <https://www.vox.com/2015/1/20/18089084/sony-hack-north-korea>

Liang, G., Weller, S. R., Zhao, J., Luo, F., & Dong, Z. Y. (2017). The 2015 Ukraine Blackout: Implications for false data injection attacks. *IEEE Transactions on Power Systems*, *32*(4), 3317–3318. <https://doi.org/10.1109/tpwrs.2016.2631891>

Whitehead, D. E., Owens, K., Gammel, D., & Smith, J. (2017). Ukraine cyber-induced power outage: Analysis and practical mitigation strategies. *2017 70th Annual Conference for Protective Relay Engineers (CPRE)*. [https://doi.org/10.1109/cpre.2017.8090056](https://doi.org/10.1109/cpre.2017.8090056%20)