**2015 Ukraine Power Grid Attack**

Nicholas Holdsworth

Department of Computing and Information Science, Mercyhurst University

CIS 402: Cyber Threat Intelligence

Dr. Polachek

December 12, 2024

**2015 Ukraine Power Grid Attack: The First of its Kind**

On December 23, 2015, the people of Ukraine suffered the first successful hacking attack on a power grid. Multiple power companies were targeted in this attack and an external hacking group named Sandworm Group was responsible for the attack. Since this attack was the first of its kind it sparked concern for other countries worldwide. It caused countries like the United States to evaluate their security processes and harden their infrastructure. Nobody wants to be the next country targeted by a power grid attack that could cause a mass panic. The methods of entry were elementary and could have been entirely prevented. This report goes into detail on the origins of the attack, the impact and severity of the attack, the threat actor, their motives, and what can be done in the future to prevent similar attacks.

**Attacks on Ukrainian Power Grid: The Real Impact**

Attacks on government agencies such as the power grid should not be taken lightly since the impact can be extremely costly. Worldwide panic can occur sending citizens into a flight or fight situation which can result in violent acts such as looting and murder. It is essential to get normal operations up and ready ASAP to prevent such chaos. During this attack, Ukraine was not the least bit prepared for the attack on its power grid. The attack lasted anywhere from one to six hours depending on location since multiple companies were targeted, not everyone experienced the same outages (Cybersecurity and Infrastructure Security Agency, 2016). An estimated total of 225,000 consumers were impacted during this attack which could have gotten out of control very quickly. The attack was coordinated and involved multiple attacks that hit various parts of Ukraine. The map below indicates locations of compromise.

A map of ukraine with red and black text

Description automatically generated

Figure 1: Map of Impacted Areas (Jackson School of International Studies, 2017)

The Ivano-Frankivsk region of Ukraine was impacted the hardest, this is where most of the consumers experienced power outages. Areas surrounding Ukraine’s capital, Kyiv, experienced some disruptions but nothing to the scale of Ivano-Frankivsk. Cybersecurity researchers acknowledge that the attacks were spread out around Ukraine because it further gave confidence to Russia that they could attack at such a scale. This newfound confidence is beneficial for future attacks against Ukraine.

**Doomed From the Start?**

Looking back after a cyber-attack it is clearer what needed to be done to prevent the attack in the first place. As stated, Ukraine was not prepared for the attack, it does not help that this attack was the first of its kind. Ukraine heavily relied on existing power supplies such methods include nuclear, coal plants, renewable energy sources, and even hydropower at a lower scale compared to the other. It is smart to have multiple sources but what is not smart is having all these sources collide at the distribution centers. These centers narrowed the scope of the attack and are the reason the attack succeeded.

Ukraine had poor sources of back-ups which added to their unpreparedness (Cybersecurity and Infrastructure Security Agency, 2016). Manual grid operations were used to restore power. This method is better than having no back-ups but the manual aspect of it requires time that the government might not have. For instance, let us say this attack was used to initiate armed combat. Manually starting the system would be impossible since the enemy would more than likely have armed guards protecting the site. The power needs to be turned on immediately and manual operation has proved to be inefficient.

**Sandworm Group**

Sandworm Group, the threat actor responsible for the attack, is a Russian-sponsored hacking group that aids in Russia’s hybrid warfare strategy. Sandworm Group acts as a way for Russia to attack both digitally and physically (MITRE, 2024). Hacking a country before invasion can provide intelligence on the weaknesses of the country. Experts say that the warning signs were obvious in predicting the 2022 invasion of Ukraine by Russian President Vladimir Putin.

Tensions between the two countries can be dated back to 2014 which was the beginning of the Russo-Ukrainian war where Russia occupied and built upon Crimea. Sandworm Group have done numerous attacks before the 2015 attack to evaluate capabilities. Various methods of attack are listed on MITRE some popular ones involve DDOS attempts on NATO allies before 2015. Some other methods include spearfishing attacks, network sniffers, and gaining root access to systems. Sandworm Group is an experienced threat actor who has numerous methods up their sleeves.

**Moments of Entry**

The attack was initiated using spear phishing tactics that targeted high-level positions at various companies. Attacks were synchronized and coordinated all of which happened 30 minutes of each other. Emails were sent containing malicious Microsoft Office attachments. When the user opens the attachment, malware named BlackEnergy is installed on the devices (Cybersecurity and Infrastructure Security Agency, 2016). BlackEnergy allowed the threat actor, Sandworm, to gain access to the network and give themselves root access. Once Sandworm was in the system, they knew exactly how to navigate and what to look for since they had been monitoring the system months prior to the attack.

            After Sandworm had a reliable footing in the network, they deployed Kill Switch malware to take control of Ukraine’s circuit breakers. Using this malware, they could turn off and on power. At this point, Sandworm had complete control over the power grid while Ukraine had to watch. Towards the end of the attack, KillDisk malware was deployed to cover up any evidence. Data was destroyed to make recovery more difficult. In the heat of the moment, Ukrainians had no idea what was happening or what to do.

            Systems that were taken for granted in 2024 were not used during the 2015 attack. Ukraine had poor monitoring systems and completely overlooked the initial intrusion (Jackson School of International Studies, 2017). Employees did not have to use multi-factor authentication to log into their accounts, which allowed Sandworm to sign in using employee credentials. Manual back-ups and data deletion made it time-consuming to gather lost information. Back-ups needed to be integrated better along with isolating the network to prevent worms from creating contemporary issues.

**Impact of Attack and Damages**

A cyber-attack can cause various problems and damage. The Ukraine power grid hack is no different. Starting off, Ukraine suffered a mass financial burden which included the remediation process. Funds were targeted at employee training and coverage to prevent future attacks. Systems needed to be replaced and upgraded with the most secure hardware and software.

            On to the intangible damages, Ukraine’s reputation was mocked since they let the attack happen in the first place. Ukraine seemed weaker than it had before the attack. Nation-states now knew Ukraine's weaknesses and how they could be used against them in the future. Attacks after the 2015 hack prove this statement since a similar power grid attack was performed just a year later (MITRE, 2024). Sandworm continued to hit Ukraine while they were weak. These back-to-back attacks only created more public fear, and it gave Russia the satisfaction that they succeeded.

**Lessons Learned**

As technology continues to advance so will the need for cyber security professions. Looking back on the 2015 Ukraine power grid hack there can be a lot of information to be learned. Starting, the need for multi-factor authentication was exposed because of this attack. Government sectors and any other business should be equipped with multi-factor, least privilege, and segregation of duties to prevent preventable attacks. White-listing software prevents threat actors from using their malicious software in networks. If Ukraine had done this prior to the attack Sandworm might have been detected and prevented the attack entirely. Preventing all unused ports is essential to preventing attacks. Open ports are like keeping a gate open with no lock. Bad actors can easily access your system. Mapping network perimeters is also essential. Organizations should know what is connected to what. This prevents attacks such as a worm and trojan horse from getting out of control. It also helps visualize the isolation of the attacker. Without a map, it might be difficult to track the paths of the hacker. Finally, awareness and employee training should be implemented to prevent phishing attacks. The weakest link of an organization is usually the employees. Training should consist of constant training and using real-world examples to explain what to look for.

**United States Point of View**

The 2015 Ukraine power grid attack proved that Russia is a superpower that needs to be watched. Russia does things such as hacking for their own personal gain and the United States needs to make sure that they are not targeted next. The United States observed the weaknesses in Ukraine’s infrastructure and learned from it by implementing safeguards to their existing infrastructure. The people of America are concerned that they are the next target.

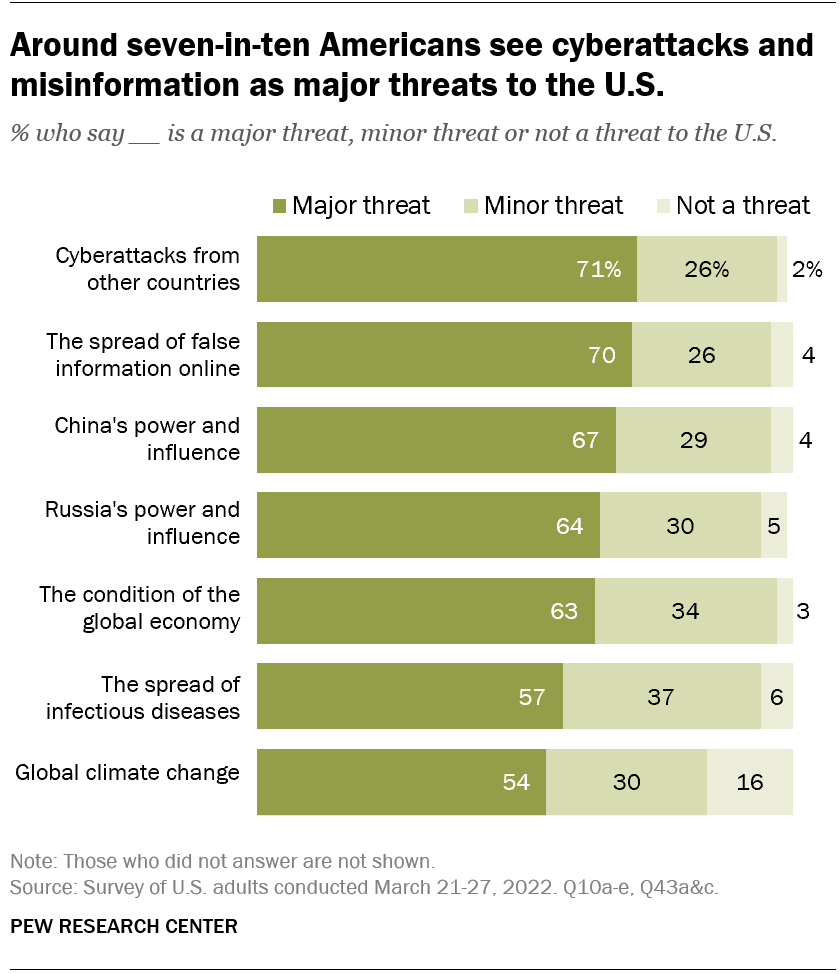


Figure 2: Pew Research Poll (Silver, L., 2022)

As one can tell from the poll Americans are genuinely concerned about the future of the world. With the war continuing in Ukraine, Putin is set on war and will not surrender. A staggering 71% of Americans see cyber-attacks from other countries as a major threat along with 64% acknowledging Russia’s power and influence. The first step in protecting ourselves is acknowledging the threat. Which we have already done.

References

Cybersecurity and Infrastructure Security Agency. (2016, February 25). *IR-ALERT-H-16-056-01: Cyber-attack against Ukrainian critical infrastructure*. CISA. <https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01>

International Society of Automation. (n.d.). *Top 10 differences between ICS and IT cybersecurity*. ISA blog. Retrieved December 11, 2024 from [https://blog.isa.org/top-10-differences-ics- cybersecurity](https://blog.isa.org/top-10-differences-ics-%09cybersecurity)

Jackson School of International Studies. (2017, October 11). *Cyberattack on critical infrastructure: Russia and the Ukrainian power grid attacks*. University of Washington. Retrieved December 10, 2024, from [https://jsis.washington.edu/news/cyberattack- critical- infrastructure-russia-ukrainian-power-grid-attacks/#\_ftn87](https://jsis.washington.edu/news/cyberattack-%09critical-%09infrastructure-russia-ukrainian-power-grid-attacks/#_ftn87)

MITRE. (n.d.). *Sandworm Team (C0028)*. MITRE ATT&CK®. Retrieved December 11, 2024 from <https://attack.mitre.org/campaigns/C0028/>

Silver, L. (2022, June 6). Americans see different global threats facing the country now than in March 2020. *Pew Research Center*. [https://www.pewresearch.org/short- reads/2022/06/06/americans-see-different-global-threats-facing-the-country-now-than-in- march-2020/](https://www.pewresearch.org/short-%09reads/2022/06/06/americans-see-different-global-threats-facing-the-country-now-than-in-%09march-2020/)