Dennis Hargro Jr

Cybersecurity Fundamentals CS462

16th April, 2023

Ukrainian State Nuclear Power Company Attack

The early days of computer hacking can be remembered as teenage hobbyists looking to have fun messing with each other's systems, playing pranks or improving the quality of their internet experience beyond the developer’s terms and conditions. As the modern computer and the core devices that operate the internet became more advanced and more intertwined with the daily transactions of life, the more dangerous the concept of hacking became. Hacking went from a mischievous prank to the weapon of cyber destruction we know today. The dangers on the internet are no longer just trolls and pranksters, but hackers who will attack for money, fame, or political gain. “Cyber attacks happen once every 39 seconds”(Boskamp,2023). The world of cyber security is always at war and requires the sharpest minds to respond and advance the field’s strategies. With the Cyber security field being more of a cat and mouse game, there are attacks that slip through. In this discussion I will detail a cyber attack not for fame nor for money but what could be considered an act of terrorism. We will look at the Ukrainian Nuclear power plant enterprise Energoatom that was attacked by Russian hackers in the Fall of 2022.

Ukraine, only having been recognized as an independent country since 1991 after declaring independence from the Soviet Union that August, is home to roughly 50 million residents (Worldometer.info). The split from the Soviet Union and pushing for democracy did not come without tensions from the surrounding communist regimes. Appointing Leonid Kravchuk as the first President of the now independent country, questions rose as to how a population of that size would find the resources to survive; energy being a major concern.

In modern day Ukraine, over %50 of the country's energy is produced by nuclear power plants (world-nuclear.org, 2023). The Ukrainian nuclear power enterprise, Energoatom, manages four major plants: Rivne, Khmelnytskyi, South-Ukraine and Zaporizhzhya. Combined for a total of 15 nuclear reactors powering Ukraine. Not only has the growth of Nuclear energy plants brought a clean, zero emissions resource to the people of Ukraine, but a sense of independence as it moves away from relying on gasoline imports from Russia and other surrounding countries. After the Chernobyl incident during the Soviet Union 1986, Nuclear safety concerns were at the forefront of the Global Nuclear Industry policies. However, redesigning power plant construction and giving proper safety training on machine operation would not be the only vulnerabilities the Ukrainian enterprise would need to defend themselves from.

Tensions with Russia and Ukraine have always been a concern since the official separation in 1991. Leaving Russia less powerful, the country had to find a way to sustain itself through multiple economic collapses as the separation had left the country also low on resources. Russia had found itself back on its feet in modern day even during the global coronavirus pandemic, but after President Putin's decision to station Russian soldiers on the border of Ukraine, tensions grew worse and led to the Russian invasion; war had broken out on the borders of Ukraine. The question in the minds of foreign spectators and those who thought Russia-Ukraine still had a family-like bond was, "why"? Possible motives detailed by Jonathan Masters' *Council on Foreign Relations* article details that some Russian individuals did not see Ukraine eye-to-eye; "After the Soviet collapse, many Russian politicians viewed the divorce with Ukraine as a mistake of history and a threat to Russia's standing as a great power. Losing a permanent hold on Ukraine, and letting it fall into the Western orbit, would be seen by many as a major blow to Russia's international prestige" (Masters, 2023). This mindset in groups of Russia individuals would result in terrorist attacks on Ukraine well before the invasion had occurred.

Ukraine, not being a stranger to cyber attacks from Russia, suffered an attack that threatened the safety of their nuclear energy resource. The Russian People's Cyber Army, detailed in Antoniuk's *The Record* article on the matter, is a public Russian hacking community of over 8,000 volunteers analogous to Ukraine's public IT Army of 230,000 members (Antoniuk, 2023). The two groups would go back and forth causing denial of service attacks on the other country. One denial of service attack I am pointing out occurred the August before the invasion of Ukraine by Russia on Ukraine's Nuclear power enterprise Energoatom. The Russian public hacker group, People's Cyber Army, flooded the Energoatom website using over 7 million bots in a botnet attack on the company. "It used a flood of garbage web traffic and web page requests… the attack was part of a Russian psyops campaign to create fear of a nuclear disaster and terrorize Europeans"(Antoniuk,2022). Chronicle article by Michael Right could imply that one of the activist group's motive was to hasten the capture of the power plants, "The cyberattack occurs as tensions rise over the country's southern Zaporizhzhia power facility, which Russian forces took control of in March just after invading their pro-EU neighbor"(Right, 2022).

A Botnet attack in summary is an army of infected devices connected to the internet used in unison to carry out large scale flooding and spamming attacks to deny the service of a target's system or fish for account information. In this case, the Russian cyber army volunteers would command over 7 million users using malware infected devices to flood the connection to the Energoatom webpage; the amount of users would cause too much congestion for the site to handle. The enterprise's website was disrupted for three hours until the Russia cyber army moved on to terrorize other Ukrainian industry pages. There isn't much detail as to how the attack was directed; however, you could imply that the number of known members of the activist group compared to the number of bots used in the attack could indicate that the cyber army had to infect over 7 million unsuspecting systems to conduct this attack. So not only was Energoatom's site not equipped to handle such congestion, but innocent users lacking the appropriate security to prevent hackers from exploiting their systems were potentially a part of this attack whether they were aware or not.

The People's Cyber Army's method of attack may seem trivial in comparison to the official Russian military hacker group "Sandworm" (or unit 74455) that was able to knock out Ukraine's power grid back in 2015 detailed by the Council on Foreign Relations' site, "In December 2015, a threat actor compromised power distribution companies in western Ukraine, causing a power outage for more than 230,000 residents. Several control centers were targeted by suspected Russian hackers, who were able to siphon operator credentials and gain access to the power grid for the Ivano-Frankivsk region. The power outage lasted as long as six hours in some areas"(crf.org). The country's power grid would again be targeted in 2016. It would seem that Ukraine became a target for not only the Russian military, but also its radical civilians; exploiting any vulnerability they can find in Ukraine's infrastructures.

Despite not causing irreversible damage to the Ukrainian nuclear industry, the botnet attack leaves an implication of just how veristalie and dangerous cyber space is to the well being of a nation. It is not just the damage that an attack can cause, but the fact that knowledgeable civilians are capable and were willing to use the internet as a weapon against a country that they did not agree with. This was not the only attack the nuclear industry faced from Russian

Hactivists. The Institute for Economics and Peace states, “Ukraine has been the target of many cyberattacks over the past years. In 2020, the number of attacks was close to 400,000.2 Past high profile attacks in the Ukraine include NotPetya, CrushOverride, Cyclop Blink” (IEP, 2022). For a country that already suffered from the tragedy of the Chernobyl incident, to have a foreign enemy gain control of any part of the nuclear infrastructure is a terrifying thought.

Trend micro’s web article *Lessons Learn From the Russian Cyber Warfare Attacks* puts into perspective how effective Russian hacking tactics are in causing divides in a government and its people by spreading misinformation, airing propaganda and cutting off resources or communication. “..hacking government websites, spreading misinformation on social media, and installing malware to steal data — are taking on a bigger role in physical conflicts. In a world where people and critical infrastructures are hyper-connected, malicious hackers have an abundance of targets” (Trend micro,2022).

The internet is no longer in its infancy and the bad actors on the internet are not just pranksters looking for fun, but criminals threatening a vital part of civilian life. The harmful potential of hacking has reached a global level. Weaponizing cyberspace as a means to carry out acts of terrorism to and from the civilian level puts entire nations in danger.With the rise of political extremism, this is just one attack of many that could be the precursor to a dark age of the internet.

Citations

Boskamp, E. (2023, March 1). *30 important cybersecurity statistics [2023]: Data, trends and more*. Zippia. Retrieved April 14, 2023, from https://www.zippia.com/advice/cybersecurity-statistics/#:~:text=Cyber%20attacks%20happen%20once%20every,websites%20are%20hacked%20each%20day.

Wikimedia Foundation. (2023, March 28). *Nuclear power in Ukraine*. Wikipedia. Retrieved April 16, 2023, from https://en.wikipedia.org/wiki/Nuclear_power_in_Ukraine

Ukraine population (live). Worldometer. (n.d.). Retrieved April 16, 2023, from https://www.worldometers.info/world-population/ukraine-population/

Right, M. (2022, August 17). *Russian hackers accused of attacking Ukraine nuclear operator's website*. Chronicle.ng. Retrieved April 16, 2023, from https://www.chronicle.ng/2022/08/russia-accused-of-attacking-ukraine/

Says:, P. J., says:, S. S., Says:, C., says:, D. L., & Says:, D. (2018, March 16). *Ukraine's push for Independence*. Association for Diplomatic Studies and Training. Retrieved April 16, 2023, from https://adst.org/2014/03/ukraines-push-for-independence/

Encyclopædia Britannica, inc. (n.d.). *The second Putin presidency*. Encyclopædia Britannica. Retrieved April 16, 2023, from https://www.britannica.com/place/Russia/The-second-Putin-presidency

Ukraine population (live). Worldometer. (n.d.). Retrieved April 16, 2023, from https://www.worldometers.info/world-population/ukraine-population/

Peace Research, presentations & Resources Free to download. Vision of Humanity. (2023, March 14). Retrieved April 16, 2023, from https://www.visionofhumanity.org/resources/

Nuclear Power in Ukraine. Nuclear Power in Ukraine | Ukrainian Nuclear Energy - World Nuclear Association. (n.d.). Retrieved April 16, 2023, from https://world-nuclear.org/information-library/country-profiles/countries-t-z/ukraine.aspx#:~:text=In%20February%202022%2C%20Russia%20launched,about%20half%20of%20its%20electricity.

Council on Foreign Relations. (n.d.). *Ukraine: Conflict at the Crossroads of Europe and Russia*. Council on Foreign Relations. Retrieved April 16, 2023, from https://www.cfr.org/backgrounder/ukraine-conflict-crossroads-europe-and-russia#:~:text=Ukraine%20became%20a%20battleground%20in,annexed%20the%20territory%20of%20another.

03, B. T. M. A., Authors, Center, T. M. C. I. S. O. R., Trend Micro, Center, C. I. S. O. R., Us, C., & Subscribe. (2022, August 3). *Lessons from the Russian Cyber Warfare attacks*. Trend

Micro. Retrieved April 16, 2023, from https://www.trendmicro.com/en_us/ciso/22/h/russian-cyber-warfare-attacks.html