The Top 5 Cyberattacks To Critical Infrastructure

Introduction

When one thinks of a Cyberattack, the images of causing damage to Web Servers, Databases, and Servers all come to mind. In these kinds of threat vectors, the main goal is to steal the proverbial Crown Jewels of a company, which are the Personal Identifiable Information (PII) datasets of both employees and customers. Ultimately, these are sold on the Dark Web, where a rather nice profit can be gained.

But Cyberattacks can reach other realms as well, other than just the digital kinds. These include attacks to Critical Infrastructure, in an attempt disable them for long periods of time, in effort to cause as much havoc as possible. In this regard, Critical Infrastructure includes such avenues as the Water Supply, Oil and Gas Lines, Nuclear Facilities, the National Electric Grid, and even the Food Distribution Channels.

Believe it or not, these kinds of targets are fairly easy to penetrate into for the Cyberattacker, because these systems are rather old by nature, and thus, possess legacy security systems which have not been upgraded in a very long time. In this series of articles, we focus we do a deeper dive into this.

The Most Well-Known Attacks

1) Attacks on the Power Grids in the Ukraine:

   This occurred in December 2015. The electric grid still made use of the traditional Supervisory Control and Data Acquisition (SCADA) system, which was not upgraded for the longest time. This Cyberattack impacted about 230,000 residents in that area and were without power for a few hours. Although this threat variant was short lived, it further illustrates the grave weaknesses of the Critical Infrastructure. For example, the traditional Spear Phishing Email was used to launch the threat vector, and in fact just a year later, the same of Email was used to attack an electrical substation near Kiev, causing major blackouts for a long period of time.

2) Attack on the Water Supply lines in New York:

   The target this time was the Rye Brook Water Dam. Although the actual Infrastructure was small in comparison, the lasting repercussions were magnanimous. The primary reason for this is that this was one of the first instances in which in a which a nation state actor was actually blamed, and all fingers pointed towards Iran. The most surprising facet of this Cyberattack was that it occurred in 2013 but was not reported to law enforcement agencies until 2013. Even more striking is that the Malicious Threat Actors were able to gain access to the command center of these facilities by using just an ordinary dial up modem.

3) Impacts to the ACH System:

   Although the global financial system may not directly fit into the classical definition of a Critical Infrastructure, the impacts felt by ay Cyberattack can be just as great. In this threat variant, it was the SWIFT Global Messaging system that was the primary target. This is used by banks and other money institutions in which to provide details about the electronic movement of money which includes ACH, Wire Transfers, etc. This is a heavily used system worldwide, as almost 34 million electronic transfers make use of this particular infrastructure (SOURCE: 1). The Lazarus Cyberattack group, originating from North Korea, were able to gain a foothold into the banks by

using hijacked SWIFT login username and password combinations. This attack has been deemed to be one of the first of its kind on the international banking sector.

4) Damages to Nuclear Facilities:

   Probably one of the well known Cyberattacks on this kind of infrastructure was upon the Wolf Creek Nuclear Operating Corporation, which is located in Kansas. In this instance, Spear Phishing Emails were leveraged against key personnel working at these facilities, who had specific control and access to the controls at this Nuclear Facility. Although the extent of the damage has been kept classified, this situation demonstrates clearly just how vulnerable the US based Nuclear Facilities are. For example, if a Cyberattacker were to gain access into one, they could move in a lateral fashion to other Nuclear Power Plants, causing damage in a cascading style, with the same or even greater effects of that of a Thermo Nuclear War.

5) Attack on the Water Supply:

   The most well-known attack just happened recently, in Oldsmar Florida. Although the details of this Cyberattack are still coming light, it has been suspected that the hacker was able to gain control by making use of a Remote Access tool, such as Team Viewer. But there were other grave weaknesses as in the infrastructure as well, such as a very outdated Operating System (OS) and very poor password enforcement (such as not creating long and complex ones and rotating them out on a frequent basis). In this instance, the goal of the Cyberattacker was not just to cause damage to the Water Supply system, but to even gravely affect the health of the residents that drank the water, by poisoning it with a chemical based lye. Luckily, an employee was able to quickly notice what was going on and immediately reversed the settings that were out into motion by the Cyberattacker. However, is it still not known yet whether this hack occurred outside US soil, or from within. If it is the latter, then this will raise even more alarm bells that domestic based Cyberattackers are just as much of a grave threat as the nation state actors to our Critical Infrastructure.

Conclusions

While this article has provided a sampling of the kinds of Cyberattacks that have happened, it illustrates one clear fact which is the most alarming of all: Through just a basic threat variant, such as that of Phishing Emails, catastrophic damage to Critical Infrastructure can happen simultaneously, with the impacts being far deadlier than that of 9/11.

Sources

1) https://www.investopedia.com/articles/personal-finance/050515/how-swift-system-works.asp#:~:text=SWIFT%20is%20a%20vast%20messaging,per%20day%20through%20the%20network.
2) https://www.cbronline.com/cybersecurity/top-5-infrastructure-hacks/
3) https://www.wfla.com/news/pinellas-county/federal-cybersecurity-advisory-offers-new-details-on-oldsmar-water-supply-cyberattack/