Risk Mitigation Consulting Inc.

Intelligence and Analysis Division

WHITE PAPER SERIES

2020 SolarWinds Hack: A Case Study of the Russian Cyber Threat

July 2021

INTENT

This white paper is designed to provide analysis of relevant, publicly available information on threat and hazard events/trends and their potential impacts to the interests of the United States, both at home and abroad. This product is not intended to be an all-encompassing assessment of the subject.

2020 SolarWinds Hack: A Case Study of the Russian Cyber Threat

Introduction

In recent years, the number of cyber-attacks and events has increased dramatically. In a world that continues to become more and more digitalized, cybersecurity has only become increasingly essential to ensure the safety of sensitive information and people. This paper intends to highlight the intent as well as an overview of Russia's cyber and espionage divisions. This paper does not, however, seek to highlight every cyber event carried out by Russia, but instead aspires to cover a single event, the SolarWinds cyber-attack of 2020, and the fallout that ensued. The SolarWinds attack was a major cyber-attack carried out by Russia's Foreign Intelligence Service (SVR). After going unnoticed for several months, Russia was able to obtain valuable intel from some of the United States most secure departments. This paper will serve as a guide through this attack as well as describe Russia's objectives when committing such attacks.

Russian Influence and Associated Cyber Threat Actors

Overview and Objectives

Russia has long been a challenger to the United States. With their growing espionage and cyber divisions, Russia has only become more of a risk to the security and operations of the United States. According to an unclassified report from the Director of National Intelligence, Russia's main target is critical infrastructure, supply chains, and many aspects considered critical to a country's economy.[1] By attacking such items, Russia is able to cripple an opposing country's economy, way of life, and operations that are essential to maintaining security and tranquility throughout a nation-state.

Although Russia utilizes normal intelligence gathering and boots on the ground spy work, they tend to lean more on cyber-attacks for many reasons. One, it is way faster to infiltrate a network digitally than it is to create a cover and gather the information by hand or for lack of better words, "walking through the front door". Two, using various hacking methods is vastly cheaper than sending an agent overseas and providing them with the resources needed for their mission. Cyber-attacks can be executed within minutes if done correctly and all someone needs are a computer and internet. Granted Russia's hackers are extremely skilled and trained in the art of digital warfare, but the idea is still the same. And the last reason that cyber-attacks are heavily used by Russia is the fact that they are easily deniable. If an agent is caught trying to infiltrate an organization, they can be easily traced back to the country that they were sent from. However, a hacker can bounce their location through several countries making it extremely difficult for the United States or anyone for that matter to trace their origin. And if they were to be caught, Russia can just as easily deny any relationship with them.

Hacker Groups and Methods

Russia is able to operate with such success and freedom due to the many state-sanctioned hacker groups such as APT 29, Fancy Bear, Cozy Bear, the Dukes, as well as a few other hacker groups that, while they aren't considered to be state-sanctioned, are continuously allowed to operate on Russian soil as long as they benefit Russia.

These hacker groups target the United States government and its private sectors in order to gain critical intelligence to further Russia's political agenda. They also hope to discover limitations and weaknesses hidden for the purpose of exploiting them for further access to the U.S. supply chain.

While Russia, or more specifically, these state-sanctioned hacker groups, is considered to be responsible for the SolarWinds attack that took place in 2020, and the main focus of this paper, there are still many state-tolerated hacker groups that have been responsible for more recent attacks such as the Continental Pipeline hack, and the JBS Meatpacking Hack. Although these hackers are not officially sponsored by Russia, Russia still acknowledges their existence and allows them to operate within their borders.[2] This allows Russia to deny responsibility for any cyber-attacks committed by these groups, but still have a mutual relationship with them. These groups primarily focus on smaller ransomware attacks for money and cryptocurrencies instead of full force cyberterrorism. On the other hand, state-sanctioned cyber groups like Cozy Bear, Fancy Bear, and Russia's SVR focus on the major supply chains of an adversary as well as government and private sector entities outside of the supply chain in search for valuable intelligence and sensitive information that can be weaponized and exploited.

The SolarWinds Hack of 2020

Event Overview

In early March 2020, Russian hackers breached a SolarWinds facility based in Texas. This breach, now known as the SolarWinds cyber-attack, allowed these hackers to upload malware onto the company's system and push the infected code onto their victims' computers via a routine software update. This software system, known as Orion, is a well-known program used by many throughout the information technology world, and according to a report by the SEC, SolarWinds claims there are approximately 33,000 active employees using the Orion system.[3] However, SolarWinds does not believe that all 33,000 employees downloaded the infected code and estimate the total number of infected devices to be around 18,000.[4] Although this number seems vastly less than the 33,000 employees originally reported by SolarWinds, the infected systems still include major fortune 500 companies, many important entities in the private sector, as well as several government agencies.

Like all computer programs, the Orion software needs routine updates to remain as secure and efficient as possible. Using this fact, hackers were able to exploit the software development process in order to carry out their attack. By uploading the malware to the SolarWinds software, and pushing it out to SolarWinds employees running the Orion system, these hackers created a back door into the computer of anyone who downloaded and installed this seemingly normal software update. Over the following months, thousands of Orion users downloaded the infected software and, unwillingly, gave the hackers access to their system. Of course, SolarWinds pushed out more software updates following the initial breached code, but they were unaware that their software had been tampered with in the first place. This is because in the initial breach, the hackers implemented a system that would alert them whenever SolarWinds was ready to begin writing a new software update. Typically, when writing new software an older version is used as a baseline. In this case, the baseline was perceived to be normal lines of code, and it was causing the SolarWinds development team to believe that everything was okay. Once the software was ready for release, the hacker's infected code would tell the system to swap the SolarWinds version of the code with the hacker's nearly identical but malicious one.[5] This process continued for nearly 9 months and was completely undetected by SolarWinds.

It wasn't until FireEye, a cybersecurity company out of California, recognized that their systems were compromised in December of 2020, that the initial SolarWinds attack was discovered. After countless investigations by SolarWinds and others it was determined that these attacks had been occurring over the span of several months. It was also discovered that the hackers had breached the SolarWinds systems before in October of 2019. This breach was a test run before the hacker's ultimate attack in March of 2020.

Following the discovery of the attack, the Biden administration put out a statement regarding an executive order imposing several sanctions against Russia. In addition to these sanctions, the White House also formally accused Russia's SVR, which includes groups APT 29, Cozy Bear, and the Dukes, as the perpetrator of this attack.[6]

Departments and Operations Affected

The SolarWinds cyber-attack affected a vast number of people from normal everyday employees, to the essential divisions of the private sector, and even a few government agencies and departments. Those affected include employees of several companies, most notably SolarWinds, Microsoft, Cisco, Intel, Deloitte, as well as government agencies such as parts of the Pentagon, the Department of Homeland Security, the State Department, the Department of Energy, the National Nuclear Security Administration, and the Treasury Department.

Once the attack had been discovered, the Cybersecurity and Infrastructure Security Agency (CISA) sent out a report ordering all government agencies to discover and destroy all instances of SolarWinds's Orion software running on their respected networks.[7] Although the hackers had been inside the Orion software for at least 9 months prior to this order, CISA was still able to prevent further damage from being done.

There is a lot of uncertainty regarding how deep this attack goes and what information was accessed. However, the main focus of the attack was espionage and information gathering and therefore, it can be inferred that personal and sensitive information was accessed. While many companies and departments reported signs of data breaches and malware, it is still hard to determine what information was accessed and stolen, if any.

Financial Fallout

With such a large-scale attack, financial fallout is a major concern. When it comes to damages, loss of data and personal information, and other minor effects from the attack, insurance alone can be extremely costly. Other financial concerns lie in increasing the funding to build better security systems and software, as well as improved training for employees. While employees are not to blame for the entirety of this attack, having the knowledge of what to do if something like this were to occur again is extremely important, and is a reason why many companies spend a massive amount of money on cyber-security trainings and programs.

Although the extent of the attack is not yet known, it is predicted that the total cost of the clean-up, including the costs from each government entity affected as well as the those affected in the private sector, is somewhere around $100 billion if not more.[8] SolarWinds spent between $18 million and $19 million in the first three months of 2021 alone in investigating the breach.[9] That is not including the cost of added security measures and software, increased funding to new employee cyber trainings, and compensation for those who feel they've been severely affected by this attack.

Future Security Concerns

As is well known, a large amount of personal information and sensitive information was accessed during the SolarWinds cyber-attack. This is obviously a major security concern going forward as these hackers could very easily use the personal information and access credentials obtained from the attack and use it to gain entry into further areas of the United States supply chain.

Another concern is the threat of having the personal information of U.S. citizens, military and government personnel be released onto the internet. Once on the internet, American adversaries can easily access it and do some serious harm to the American public. For example, in 2015, the Islamic State (IS) released the names and addresses of more than 1,400 U.S. military and government officials to the internet and urged their American followers to seek out violence.[10] While Russia is not likely to follow in the same footsteps as IS, other actions could be taken such as blackmailing someone discovered to be a liability to the U.S. or future espionage by using the personal information as a filter of sorts for a more specific attack against the U.S. Either way, the threat is still real, and should be a concern going forward.

Other threats include the idea that many of the hacked networks could still be unsecure or even modified for easier entry. Cyber-attacks can be extremely difficult to discover but they can be even more difficult to secure and defend against afterwards. Although the hackers have been flushed out of most networks, primarily government, it is impossible to be 100% sure that they have been flushed out of all of them. More backdoors could have been made, and unless another attack were to arise, it is impossible to know where they are located and how to destroy them.

Conclusion

All in all, the SolarWinds cyber-attack was one of the largest cyber-attacks against the United States in recent years. Not only will the effects of the attack still be felt years from the initial discovery, but the safety of the United States and cyberspace as a whole will be changed in a big way.

Russia gained a lot from this attack including valuable intelligence about the United States supply chain. Although the United States has responded heavily against Russia for this attack, it can be assumed that Russia will continue their attacks on the U.S. Russia thrives on suffocating a nation's economy and the added information obtained from this attack certainly helps.

On a broader note, while Russia may not have done much damage to the United States when it comes to infrastructure, they were still able to destroy the confidence that many people place on the security of the United States. Many people believe that the United States is impenetrable from threats from the outside world. However, as can be seen by the impacts of the SolarWinds attack, that is not the case. SolarWinds should be a major wake up call for high level corporations and government agencies. The threats of the cyber world are not to be taken lightly. Although they seem small, even the smallest of cyber events could turn into the biggest threat to national security.

[1] Office of the Director of National Intelligence (2021, April 9). Annual Threat Assessment of the U.S. Intelligence Community. Retrieved June 14, 2021, from https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf.

[2] Morris, L., &amp; Khurshudyan, I. (2021, June 12). Ransomware's suspected Russian roots point to a long detente between the Kremlin and hackers. The Washington Post. https://www.washingtonpost.com/world/europe/russia-ransomware-cyber-crime/2021/06/11/e159e486-c88f-11eb-8708-64991f2acf28_story.html.

[3] SolarWinds Corporation. (2020). Unites States Securities and Exchange Commission form 8-K. Retrieved from Securities and Exchange Commission website: https://www.sec.gov/ix?doc=/Archives/edgar/data/1739942/000162828020017451/swi-20201214.htm.

[4] Sanger, D. E., Perlroth, N., &amp; Schmitt, E. (2020, December 15). Scope of Russian Hacking Becomes Clear: Multiple U.S. Agencies Were Hit. The New York Times. https://www.nytimes.com/2020/12/14/us/politics/russia-hack-nsa-homeland-security-pentagon.html.

[5] Temple-Raston, D. (2021, April 16). A 'Worst Nightmare' Cyberattack: The Untold Story Of The SolarWinds Hack. NPR. https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack.

[6] The White House. (2021, April 15). FACT SHEET: Imposing Costs for Harmful Foreign Activities by the Russian Government. https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/.

[7] Boyd, A. (2021, April 14). CISA Orders Federal Agencies to Turn Off SolarWinds Products . Nextgov.com. https://www.nextgov.com/cybersecurity/2020/12/cisa-orders-federal-agencies-turn-solarwinds-products/170737/.

[8] Ratnam, G. (2021, January 11). Cleaning up SolarWinds hack may cost as much as $100 billion. Roll Call. https://www.rollcall.com/2021/01/11/cleaning-up-solarwinds-hack-may-cost-as-much-as-100-billion/.

[9] Satter, R. (2021, April 13). SolarWinds says dealing with hack fallout cost at least $18 million. Reuters. https://www.reuters.com/technology/solarwinds-says-dealing-with-hack-fallout-cost-least-18-million-2021-04-13/.

[10] Safi, M. (2015, August 13). Isis 'hacking division' releases details of 1,400 Americans and urges attacks. The Guardian. https://www.theguardian.com/world/2015/aug/13/isis-hacking-division-releases-details-of-1400-americans-and-urges-attacks.