Drexel Hamilton

A Service-Disabled Veteran Owned & Operated Business

Outside the Wire
Mass Cyber-Attack 2020

Photo Illustration/Shutterstock

As seen in the news lately, there is a bit of a stir going on within the issue of Cyber Security due to the massive SolarWinds hack that happened in 2020. More details are being discovered about the attack each day. Due to the complexity of computer networks and digital workspace, it is likely that the true extent of the situation will not be known for months.

Brief Description

It is now estimated that sometime around October of 2019, state sponsored Russian hackers residing in the U.S., breached their way into SolarWinds. SolarWinds is an IT management and remote monitoring company that services hundreds of U.S. companies and government agencies.

This data breach was discovered by one of SolarWinds' client companies, FireEye, which is a cybersecurity company that actively seeks out cyber-attacks and vulnerabilities. However, the discovery was not made for months, which means that alleged hackers had open-door access to many of our national defense networks and companies for much of last year. FireEye technicians discovered the breach after their own networks alerted them that an attempted breach was made on their servers. After looking through over 50,000 lines of SolarWinds' source code, FireEye discovered a back door for access that was created with malware. As soon as the discovery was made, they contacted SolarWinds and law enforcement.

Because SolarWinds is a remote IT management company, their internal networks have access to the networks of their client companies. For hackers, this is a goldmine entrance that enables them to access hundreds of additional networks. Some of the government agencies that were affected include the Departments of Homeland Security, Agriculture and Commerce, U.S. Treasury Department, and the Department of Energy. Private institutions that were affected by the SolarWinds hack included tech companies, a hospital, and a university. There is a possibility that there are many more, but the complete extent of the damage has yet to be revealed.

In response to the notification by FireEye and law enforcement, SolarWinds immediately deactivated its Orion platform. This platform was their largest and most popular IT monitoring and maintenance program. Since the discovery, SolarWinds has so far estimated that over 18,000 individuals had installed the compromised platform, and this number continues to grow as technicians learn more about the attack. At this stage, all of the individual companies that were breached are conducting their own internal assessments.

Who is SolarWinds?

SolarWinds is an IT management and monitoring provider for corporations and government agencies around the world and has become a dominant player in the industry since it was founded in 1999.

Source: SolarWinds APM

While their name is not as popular as a household name such as Microsoft or Norton, their remote services have been growing for decades, and they have a large market share of the computer IT industry. To bring it down to the individual perspective, they are one of the largest IT companies, whose clients can call and have them "remote in" to fix issues on a computer. Their platforms also provide for monitoring of business computer systems for employees of companies and government agencies.

The company has been in chaos since the discovery of the hack. They have been alerting customer accounts that an "outside nation-state" had found its way into their Orion platform via a "backdoor" and that the situation is still developing. In mid-December, the company took down a web page from its site which marketed their business with some of their well-known customers like the White House, Pentagon, Secret Service, McDonald's restaurant chain, Smithsonian museums, and others.

The Orion Platform product accounts for roughly half of the company's total revenue, which totaled $753.9m over the first nine months of 2020. Since news of the hack, the stock price of SolarWinds (NYSE: SWI) has decreased almost 40%.

Breakdown of the Hack

The type of hack that was made on SolarWinds is called a R.A.T., which stands for Remote Access Trojan. The hackers somehow got into SolarWinds's network, and investigation findings indicate that this may have been from the theft of an administrative password. Once granted access, hackers embedded lines of code which gave them more continued access via a "back-door". This is crucial because the SolarWinds network is an important part of the supply chain for cyber infrastructure across thousands of companies and government institutions.

The embedded code that hackers placed was unknowingly included in an ordinary software update. Users installed the update as a regular occurrence for their software maintenance. Once all the users of Orion downloaded the update, it gave additional access to hackers to obtain information and additional passwords. The hackers made a mistake when they attempted to steal information from FireEye, which is a sophisticated cybersecurity company. FireEye has specialized cyber tools and software, which makes them a great target for hackers. The company had protection protocols in place, such as something called a "honeypot", which is a decoy file that contains data that looks like something important but is actually false (such as an empty file named "Company Passwords"). This honeypot file essentially has a cyber "pressure sensor" and shoots red flags to administrators and technicians when the file is activated. In essence, the hackers were caught because they got too greedy.

Photo Illustration by Fidelis Cybersecurity: A "Honeypot"

What can we do about it?

The internet domain industry is not adequately protected, but that is not to say that the problem cannot be fixed. All industries will continue to experience hacks, and a strong cyber defense will become critical.

From a macro perspective, there needs to be laws aimed at deterrence. As we have noted in the past, the U.S. government lacks a comprehensive cyber deterrence strategy. There is the possibility of retributions on nation-states that launch or sponsor cyber-attacks against the U.S. specifically in the form of sanctions or through diplomatic actions. Actions must be implemented that would effectively raise the cost of performing an attack, so that the perpetrators would be forced to ask themselves beforehand, "is this really worth it?".
Things like sanctions, embargos, penalties, and U.S. responses "in-kind" could be enacted to hit the enemy in their wallets. Stricter punishments should be put in place and publicly known for those who wish to tamper with cybersecurity. Finally, the United States could enable or institute a national supply-chain hardening system so that there are more controls over vendors and suppliers of cybersecurity products.
Legislation could require vendors of security software for private companies and the DOD to prove that their networks are heavily secured.

On a micro level, there are many things that individuals and companies can do to strengthen their security. First, there should be increased due diligence on an organization's internal network security. Too often people lose passwords, do not use strong passwords, and are victims of phishing scams. Social engineering remains the biggest threat. This is a problem that requires training and education of the workforce. There is no easy technical solution.

For those businesses who are bringing in third-party cybersecurity consultants and software providers such as SolarWinds, it is important to focus on supply chain risk. Every vendor needs to provide assurance and guarantees that their efforts are clean and completely secured. When signing contracts with cybersecurity or IT providers, liability should be assumed by the consultant. If their software is compromised by a hacker, they are responsible for damages and loss from theft. Within the cybersecurity industry, a lot of the problem comes from individual developers. Even a 1-character error written in source code can provide a hacker with free, easy access to a computer network. This risk can be mitigated by putting in greater effort with checking the background and experience of hired tech firms.

Conclusion:

Cyber-attacks are becoming more common as reliance on digital infrastructure grows. Companies and organizations can remain on top of these threats by continuously monitoring and trying to improve their cyber defenses. Understanding the latest technologies and developments in the space is important. We believe that Artificial Intelligence will do a lot to improve cyber security. These AI tools can be used to monitor networks more efficiently than a human being. AI tools can spot anomalies and alert network administrators as they happen. This market will continue to grow as the need becomes more apparent.

Photo Illustration/InformationAge

Turton, W. & Mehrotra, K. (2020, December 14). *FireEye Discovered SolarWinds Breach While Probing Own Hack*. Bloomberg. Retrieved from https://www.bloomberg.com/news/articles/2020-12-15/fireeye-stumbled-across-solarwinds-breach-while-probing-own-hack