SolarWinds

On December 8, 2020, an employee of the network security company FireEye received an alert that his password was fraudulently used to log in to the company's VPN and stolen the weapon arsenal used by FireEye to simulate cyber attacks. The months-long attack on SolarWinds has happened.

SolarWinds is the industry benchmark for network management software, and its customers cover all levels of government and major companies in the United States. As of December 20, 2020, in addition to the aforementioned Solarwinds and FireEye companies, the U.S. State Department, the Pentagon, the Department of Homeland Security (DHS), the Department of Commerce, the Department of Treasury, the Department of Justice, and the Bureau of Cybersecurity and Infrastructure are affected by the incident. (CISA), Centers for Disease Control and Prevention (CDC), National Institutes of Health (NIH), US Department of Commerce, National Telecommunications and Information Administration (NTIA), US Department of Energy (DOE), regulators of the National Nuclear Security Administration (NNSA) and other US government departments; Microsoft (Microsoft), Intel (Intel), Nvidia (Nvidia), Cisco (Cisco), VMWare, Deloitte (Deloitte) and other Fortune 500 institutions are listed. The investigation is still ongoing, but the Microsoft team issued an initial report on December 18. Hackers intruded into Solarwinds' software development process through unknown means, tampered with a DLL file, and added the official digital signature of "Solarwinds Worldwide, LLC". Unconsciously, the version of Solarwinds with more than 4000 lines of unknown code was hung up on the official website in the form of an upgrade package. There is speculation that the Russian spy bought Solarwinds staff to change the code. In August of this year, the FBI arrested a Russian spy who tried to bribe Tesla employees $1 million to install a backdoor on the company's computer. The backdoor program is very cautious and low-key. It runs on a thread different from the main program and does not interfere with the operation of the main program. The naming style of functions and variables in the code is consistent with the normal code. After the backdoor is loaded, it will first confirm that there is no anti-virus software in the operating environment. After that, the backdoor will contact the C2 server (command-and-control server, command, and control) controlled by the hacker. Using this as a springboard, hackers can compromise the entire network where the infected device is located.

It is foreseeable that with the deepening of the investigation, the scope and severity of the SolarWinds supply chain attack will further expand. According to past experience, it is almost impossible to find all the victims and completely prevent hackers from accessing the compromised network. Even if it can be done, it will be difficult. Just like treating a cancer patient, unless you can kill all cancer cells when it has not spread in the early stage, even if the condition is remission, you must be cautious and trembling in the following days, always worrying about recurrence. In addition, the attacker may still use the Trojan horses planted before to carry out secret attacks, continue to obtain information, and even lurch until a certain key node in the future concentrates again, causing greater damage.

In June 2020, network security service provider BlueVoyant launched a survey, and the results showed that 80% of surveyed companies had experienced data breaches due to attacks on their suppliers. A survey conducted by Accenture in 2019 showed that 40% of surveyed companies had data breaches due to suppliers. ESG and Crowstrike's supply chain security report released in 2019 showed that 90% of companies are "not prepared" to respond to supply chain cyber-attacks.

Work Cited:

“Unauthorized Access of FireEye Red Team Tools” FireEye, https://www.fireeye.com/blog/threat-research/2020/12/unauthorized-access-of-fireeye-red-team-tools.html

David E. Sanger, Nicole Perlroth and Eric Schmitt, “Scope of Russian Hacking Becomes Clear: Multiple U.S. Agencies Were Hit”, NYTime, https://www.nytimes.com/2020/12/14/us/politics/russia-hack-nsa-homeland-security-pentagon.html

NATASHA BERTRAND and ERIC WOLFF, “Nuclear weapons agency breached amid massive cyber onslaught”, Politico, https://www.politico.com/news/2020/12/17/nuclear-agency-hacked-officials-inform-congress-447855

Christopher Bing, “Suspected Russian hackers spied on U.S. Treasury emails - sources”, Reuters, https://www.reuters.com/article/us-usa-cyber-treasury-exclsuive/suspected-russian-hackers-spied-on-u-s-treasury-emails-sources-idUSKBN28N0PG

Ellen Nakashima and Craig Timberg, “DHS, State and NIH join list of federal agencies — now five — hacked in major Russian cyberespionage campaign”

https://www.washingtonpost.com/national-security/dhs-is-third-federal-agency-hacked-in-major-russian-cyberespionage-campaign/2020/12/14/41f8fc98-3e3c-11eb-8bc0-ae155bee4aff_story.html

Catalin Cimpanu, “Microsoft says it identified 40+ victims of the SolarWinds hack”, Zero Day,

https://www.zdnet.com/article/microsoft-says-it-identified-40-victims-of-the-solarwinds-hack/

Ian King and Kartikay Mehrotra, “Cisco Latest Victim of Russian Cyber-Attack Using SolarWinds”

https://www.bloomberg.com/news/articles/2020-12-18/cisco-latest-victim-of-russian-cyber-attack-using-solarwinds

“Analyzing Solorigate, the compromised DLL file that started a sophisticated cyberattack, and how Microsoft Defender helps protect customers”, Microsoft,

https://www.microsoft.com/security/blog/2020/12/18/analyzing-solorigate-the-compromised-dll-file-that-started-a-sophisticated-cyberattack-and-how-microsoft-defender-helps-protect/

Dan Goodin, “Russian tourist offered employee $1 million to cripple Tesla with malware”,

https://arstechnica.com/information-technology/2020/08/russian-tourist-offered-employee-1-million-to-cripple-tesla-with-malware/

Brian Fung, “Why the US government hack is literally keeping security experts awake at night”, CNN, https://www.cnn.com/2020/12/16/tech/solarwinds-orion-hack-explained/index.html

About me

In reports on multiple media platforms, the Sunburst attack has been described as the "most serious" supply chain attack in history, and the impact may continue in 2021. What other effects might Sunburst cause? By the end of 2021, will Sunburst still be the "most in history"? At this moment, I cannot give an answer. What I can do is better protect my personal data information on the Internet.

1. If you throw away the express package, you must smear and dispose of personal information such as your name and phone number;

2. Do not fill in the form online, especially important personal information, unless you have to provide it, use fake identity information;

3. It is possible to use authorized login, including authorized login by various social tools;

4. Delete important ID photos when they are used up, try not to keep them in the mobile phone or network disk;

5. Use mobile phone data as much as possible, and use public WIFI with caution. In addition, you need to use mobile WIFI The connection is set to manual, confirm that it is a safe and reliable WIFI and then connect and use;

6. Don’t arbitrarily discard the mobile phone number, especially the mobile phone number associated with important services. You must cancel the association one by one before discarding the number, otherwise, it is very likely to bring economic Loss;

7. Reduce the free disclosure of private information about yourself and family members on social media;

8. All kinds of important accounts that are not used, promptly cancel and deal with the binding of various accounts such as names and phone numbers.

9. Do not click to browse unknown websites, Do not download applications from unknown sources at will, which can effectively avoid computer or mobile phone poisoning;

10. Do not disclose your location, family members, and other information on social media to avoid social worker fraud by others;

Work Cited:

Sai Kit Chu, “Top 10 Safe Computing Tips for Employees”, Business 2 Community, https://www.business2community.com/cybersecurity/top-10-safe-computing-tips-for-employees-02382586

“The risks of public Wi-Fi”, Norton, https://us.norton.com/internetsecurity-privacy-risks-of-public-wi-fi.html