The impact of SolarWinds Hack

SolarWinds Orion is an enterprise network management software suite that includes performance and application monitoring and network configuration management along with several different types of analysing tools. SolarWinds Hack, aka Solorigate and Sunburst, has been considered by some as the largest and most sophisticated cyberattack so far. The attackers exploited business software firm SolarWinds' Orion product to send malware to about 18,000 customers. This type of attacks commonly known as supply chain, value-chain or third-party cyberattacks. FireEye (tracking code UNC2452) detected this activity at multiple entities worldwide. The victims include government, consulting, technology, telecom and extractive entities in North America, Europe, Asia and the Middle East. They anticipate there are additional victims in other countries and verticals.

What exactly happened:

According to SolarWinds, SUNBURST attack exploited a vulnerability within their Orion® Platform software builds for versions 2019.4 HF 5, 2020.2 unpatched, and 2020.2 HF 1, which, if present and activated, could potentially allow an attacker to compromise the server on which the Orion Platform products run. SUNBURST attack disrupts a standard process resulting a compromised system can be manipulated to attack subsequent users of the software. Based on their investigations, it appeared that the code was intended to be used for targeted attacks as its exploitation requires manual intervention.

SUNBURST backdoor attack was followed by the SUPERNOVA malware that consisted of two components. The first was a malicious, unsigned webshell.dll "app_web_logoimagehandler.ashx.b6031896.dll" specifically written to be used on the Orion Platform. The second is the exploitation of a vulnerability in the Orion Platform to enable deployment of the malicious code.

It was also alleged by https://threatpost.com/ that malicious code added to an Orion software update may have gone undetected by antivirus software and other security tools on host systems thanks in part to guidance from SolarWinds itself. In a support advisory SolarWinds has advised its products may not work properly unless their file directories are exempted from antivirus scans and group policy object restrictions.

SolarWinds has not verified the identity of the attacker. Based on ongoing investigations SolarWinds believe that the SUNBURST vulnerability was inserted within the Orion Platform products and existed in updates released between March and June 2020 as a result of a compromise of the Orion software build system and was not present in the source code repository of the Orion Platform products. SolarWinds states that latest updates were designed to remedy this vulnerability in all supported versions of the Orion Platform.

Key Learning announced by the victims:

According to Microsoft, their key learning from the Solorigate is ; embracing a Zero Trust mindset and protecting privileged credentials. SolarWinds President and CEO Sudhakar Ramakrishna, in a recent talk conveyed the steps SolarWinds is taking for safer SolarWinds and customer community as; "Further secure our internal environment, Enhance our product development environment, Ensure the security and integrity of our software". Alex Stamos who leads the security team at SolarWinds details what you can learn from the attack are; "Learn to audit your cloud trust relationships, Learn to build for code integrity, Learn to centralize your monitoring to accelerate detection and speed response, Learn to document network dependencies to better control access, Learn to enhance permission rules and risk-based authentication"

Bridging the gaps in Enterprise Information Security Management and Compliance

Anyone who reads above Key Learnings may wonder, "Didn't you know about these already?" It is well documented and discussed that the weakest link in enterprise security might lie with partners and suppliers in the supply chain. Global Enterprises such as SolarWinds naturally attracts sophisticated and well-funded actors that are capable of advanced techniques and patience and be able to operate below the radar (aka advanced persistent threats), as it will be a huge return on their resources invested.

SolarWinds hack has proven again that despite existing security strategies many enterprises are struggling to cover the whole security echo system of the enterprise. So, what are the gaps in today's enterprise security echo systems and approaches that governing bodies and policy makers could fill in.

Should security be a responsibility of just the Enterprises? Is it time to bring in international compulsory protocols on product development, architectural design, situational awareness, and agility of response to threats, to be explored on?

Deepthi Ratnayake MBCS,
Senior Lecturer in Computer Science (Cyber Security & Networks)
University of Hertfordshire,
d.ratnayake@herts.ac.uk

Date manuscript accepted 24th Mar 2021.