Radware Cybersecurity Alert

SolarWinds Orion Supply Chain Attack
FireEye Hack Update

Dec 15, 2020

SolarWinds Orion Supply Chain Attack

FireEye published their analysis of what turned out to be a global intrusion campaign, a supply chain attack "trojanizing" SolarWinds Orion software updates performed by an advanced and sophisticated threat actor and that distributes a backdoor dubbed SUNBURST.

The SolarWinds supply chain attack affects 18,000 organizations across the globe. According to **Forbes**, SolarWinds is a major contractor for the U.S. government, with regular customers including CISA, U.S. Cyber Command, the Department of Defense, the Federal Bureau of Investigation, the Department of Homeland Security, and many others. The SolarWinds security breach **has already been linked** to hacks at U.S. security firm FireEye, the U.S. Treasury Department, and the U.S. Department of Commerce's National Telecommunications and Information Administration (NTIA).

"The SolarWinds Orion platform hack is slowly turning out to be one of the most significant hacks in recent years."

ZDNET

What Is A Supply Chain Attack?

A supply chain attack is a cyberattack that seeks to damage an organization by targeting less secured elements in the supply network. In 2013, Target, a US retailer, was hit by a data breach that saw 40 million customer credit and debit card information leaked when malware was introduced into their point of sale system in over 1,800 stores. It is believed, although not officially confirmed, that cybercriminals infiltrated into Target's network using credentials stolen from Fazio Mechanical Services, a Pennsylvania-based provider of HVAC systems.

During the spring of 2017, a Ukrainian accounting software firm had its servers seized by the Ukrainian police. The firm was unwittingly helping to spread the notorious NotPetya malware via a malicious update to its accounting software, M.E.Doc. Hackers seemed to have breached the company's computer systems and compromised the software update.

"Trojanized Orion"

On Sunday, SolarWinds published a press release admitting to a breach by a sophisticated actor who found a way to inject malicious code in SolarWinds' Orion IT monitoring and management software. The malicious code got distributed to many government and high-profile organizations through SolarWinds' website as part of software update packages. The digitally signed SolarWindows.Orion.Core.BusinessLayer.dll plugin module contained backdoor code hiding in plain sight by using fake variable names and tying into legitimate components and gets loaded and invoked by the Orion software framework. The malicious plugin module is tracked as **SUNBURST** by FireEye and **Solorigate** by Microsoft.

Radware Cybersecurity Alert

SolarWinds Orion Supply Chain Attack
FireEye Hack Update

Dec 15, 2020

1. Threat actor breaches SolarWinds
2. Threat actor hides backdoor in Orion plugin module
3. SolarWinds publishes update package with backdoor
4. SolarWinds customer downloads and installs Orion update
5. Orion executes and loads backdoored plugin
6. Backdoor initiates contact with C2 and receives commands and exfiltrates data

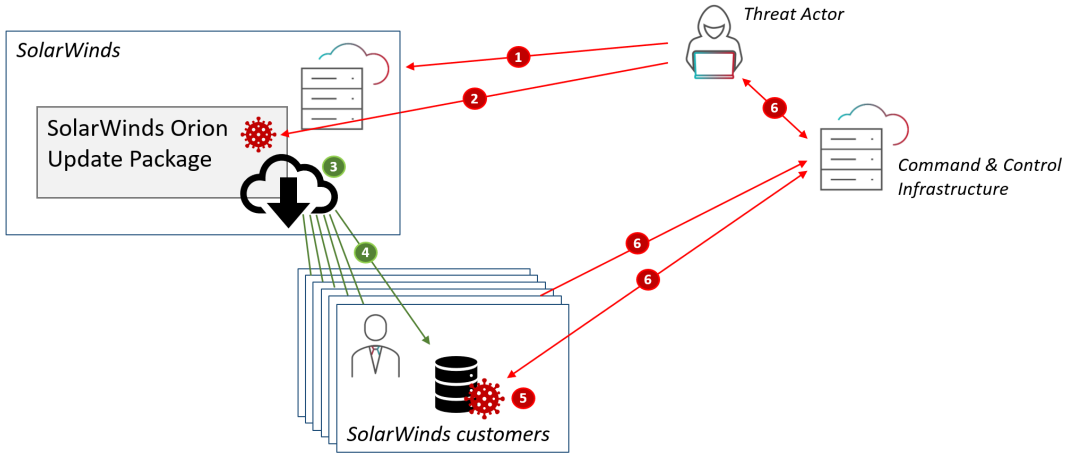

Figure 1: Supply chain attack on SolarWinds' Orion update package resulting in backdoor installation

The malicious code was distributed part of update version 2019.4 through 2020.2.1. that were released between March and June, 2020. According to the **in-depth analysis by FireEye**, after an initial dormant period of up to two weeks, the backdoor code retrieves and executes commands that allow it to transfer files, execute files, profile the system, reboot the machine and disable system services. The malware masquerades network traffic as the Orion Improvement Program (OIP) protocol and stores reconnaissance results within legitimate plugin configuration files allowing it to blend in with legitimate SolarWinds activity. The backdoor uses multiple obfuscated blocklists to identify forensic and anti-virus tools running as processes, services and drivers. The backdoor determines its command and control server using a Domain Generation Algorithm (DGA) which allows it to randomly generate one of many C2 hostnames making it more robust against detection and blocklisting. Command and control traffic is concealed through stenography in what looks like benign code exchange for .NET assemblies.

An Advanced, Sophisticated Threat Actor

The use of advanced techniques to deploy a light malware to accomplish the mission and avoid detection through obfuscation and stenography points to a highly sophisticated threat actor. FireEye is tracking the threat group with a neutral codename UNC2452, although sources speaking with the Washington Post linked the intrusion to APT29, also known as Cozy Bear, and indicating a Russian hacker group believed to

have working relations with the Russian Foreign Intelligence Service. Kremlin spokesman Dmitry Peskov **told reporters** Monday that Russia had "nothing to do with" the hacking.

Who Got Compromised?

SolarWinds confirmed 18,000 Orion customers could be compromised. **Reuters reported** however that the attackers appear to have focused only on a small number of high-value targets, leaving most Orion customers unaffected. **ZDNet** mentions several IT administrators reported that they found signs of the malware-laced Orion update on their systems, but they did not find signs of second-stage payloads, typically used by the attackers to escalate access to other systems and internal customer networks.

What Does It Mean?

Even if the attackers focused on a small number of high-value targets, how does one define high-value? Any organization using the SolarWinds Orion software platform and that installed updates for the platform between March and June 2020 is backdoored and potentially breached. Updating to the latest Orion software will remove the backdoor, but without forensic analysis it is not possible to exclude the possibility that other malware was loaded or user accounts created that allow the malicious actors access to the victim's network and systems even after cleaning and mitigating the original threat.

Mitigation Recommendations

SolarWinds recommends all customers immediately upgrade to Orion Platform release 2020.2.1 HF 1, which is currently available via the SolarWinds Customer Portal. In addition, SolarWinds has released additional mitigation and hardening instructions **here**. In addition, FireEye published IOCs and countermeasures **here**. More technical details regarding the actor's tactics, techniques and procedures (TTPs) were **published** by FireEye.

EFFECTIVE DDOS PROTECTION ESSENTIALS

- **Hybrid DDoS Protection** - On-premise and cloud DDoS protection for real-time DDoS attack prevention that also addresses high volume attacks and protects from pipe saturation
- **Behavioral-Based Detection** - Quickly and accurately identify and block anomalies while allowing legitimate traffic through
- **Real-Time Signature Creation** - Promptly protect from unknown threats and zero-day attacks
- **A Cyber-Security Emergency Response Plan** - A dedicated emergency team of experts who have experience with Internet of Things security and handling IoT outbreaks
- **Intelligence on Active Threat Actors** – high fidelity, correlated and analyzed date for preemptive protection against currently active known attackers.

For further **network and application protection** measures, Radware urges companies to inspect and patch their network in order to defend against risks and threats.

EFFECTIVE WEB APPLICATION SECURITY ESSENTIALS

- **Full OWASP Top-10** coverage against defacements, injections, etc.
- **Low false positive rate** – using negative and positive security models for maximum accuracy
- **Auto policy generation** capabilities for the widest coverage with the lowest operational effort
- **Bot protection and device fingerprinting** capabilities to overcome dynamic IP attacks and achieving improved bot detection and blocking
- **Securing APIs** by filtering paths, understanding XML and JSON schemas for enforcement, and activity tracking mechanisms to trace bots and guard internal resources
- **Flexible deployment options** - on-premise, out-of-path, virtual or cloud-based

LEARN MORE AT DDOS WARRIORS

To know more about today's attack vector landscape, understand the business impact of cyberattacks or learn more about emerging attack types and tools visit **DDoSWarriors.com**. Created by Radware's **Emergency Response Team (ERT),** it is the ultimate resource for everything security professionals need to know about DDoS attacks and cybersecurity.