Overview of Recent Sunburst Targeted Attacks

trendmicro.com/en_us/research/20/l/overview-of-recent-sunburst-targeted-attacks.html

December 15, 2020

Cyber Threats

Various sources have recently disclosed a sophisticated attack that hit organizations via the supply chain via a compromised network monitoring program. This post discusses what the Sunburst backdoor is and what you can do now to mitigate this threat.

By: Trend Micro December 15, 2020 Read time: (words)

Update on 12/29/2020 2:40 PM PST: Information on Supernova added

Update on 1/22/2021 4:56 PM PST: Trend Micro's Zero-Day Initiative (ZDI) provided technical analysis of recently patched vulnerabilities in the SolarWinds Orion Platform. CVE-2020-14005, one of these vulnerabilities, has been linked to the recent SUNBURST cyberattack on SolarWinds. These vulnerabilities, when combined, could allow an unauthenticated attacker to execute arbitrary code as Administrator on an affected system.

Various sources have recently disclosed a sophisticated attack that hit organizations via the supply chain. This was carried out via a compromised version of a network monitoring application called SolarWinds Orion. The attackers used the access provided by this application to plant a backdoor known as Sunburst onto affected machines. This backdoor provided the attacker with complete access to the targeted organization's network.

What is Sunburst?

Sunburst is a sophisticated backdoor that provides an attacker nearly complete control over an affected system. It has several peculiarities in its behavior, however.

Before it runs, it checks that the process name hash and a registry key have been set to specific values. It will also only run if the execution time is twelve or more days after the system was first infected; it will also only run on systems that have been attached to a domain. This specific set of circumstances makes analysis by researchers more difficult, but it also limits the scope of its victims to some degree.

It connects back to its command-and-control server via various domains, which take the following format:

> *{random strings}.appsync-api.{subdomain}.avsvmcloud.com*

The subdomain is one of the following strings:

- eu-west-1
- eu-west-2
- us-east-1
- us-east-2

Once in a system, it can both gather information about the affected system and execute various commands. The gathered information includes:

- Domain name
- Network interfaces
- Running processes/services

- Installed drivers

This gathered information is used either to generate a user ID for the affected machine, or to check against blocklists - if certain drivers, processes, or services are found on the machine, the backdoor will cease to function.

The commands that can be executed include:

- Registry operations (read, write, and delete registry keys/entries)
- File operations (read, write, and delete files)
- Run/stop processes
- Reboot the system

What is Supernova?

Supernova, one of the malicious components associated with the attack, is a .NET web shell backdoor that presents itself as a legitimate SolarWinds web service handler. It is a second-stage payload in the attack. Once running, it inspects and responds to HTTP requests with appropriate HTTP query strings, cookies, and HTML form values. It can also execute web shell commands via a specific HTTP request format.

Who is affected?

It is believed that Sunburst was delivered via a trojanized version of the Orion network monitoring application. According to SEC filings by SolarWinds, threat actors inserted the malicious code into otherwise legitimate code, which means anyone who downloaded the software was potentially at risk. This was done as part of the build process; the source code repository was not affected.

According to the SolarWinds SEC filing, this trojanized version was downloaded by under 18,000 customers from March to June of 2020. Once this malicious code is present in a system, it runs the behavior described in the first part of this post. Multiple organizations, including US government agencies, have reported that they were affected by this campaign.

Solutions

In a security advisory, SolarWinds advised all of their affected customers to immediately update their software to versions that do not contain the malicious code. The advisory also lists the appropriate products and their versions. Our article titled ***Managing Risk While Your ITSM Is Down*** includes suggestions on how to manage network monitoring and other IT systems management (ITSM) solutions.

In addition to this, the US Department of Homeland Security, in a directive to US government agencies, ordered that systems with the said software be taken offline and not reconnected to networks until they have been rebuilt. The directive treats agencies to treat said machines as compromised, with credentials used by said machines to be changed as well. Organizations that use SolarWinds Orion within their network may consider similar steps.

The malicious files associated with this attack are already detected by the appropriate Trend Micro products as Backdoor.MSIL.SUNBURST.A and Trojan.MSIL.SUPERNOVA.A. In addition to this, the entirety of the domain *avsvmcloud.com* has been blocked.

If you believe that your organization may have been affected by this campaign, visit this page for the available Trend Micro solutions that can help detect and mitigate any risks from this campaign.

If you're a Trend Micro Apex One customer, check your product console for a notification to scan your environment for attack indicators of this campaign.

Indicators of Compromise

The following hashes are associated with this campaign and are detected by Trend Micro products:

SHA256	SHA1	Trend Micro
019085a76ba7126fff22770d71bd901c325fc68ac55aa743327984e89f4b0134	2f1a5a7411d015d01aaee4535835400191645023	Backdoor.M
c15abaf51e78ca56c0376522d699c978217bf041a3bd3c71d09193efa5717c71	75af292f34789a1c782ea36c7127bf6106f595e8	Trojan.MSIL
ce77d116a074dab7a22a0fd4f2c1ab475f16eec42e1ded3c0b0aa8211fe858d6	d130bd75645c2433f88ac03e73395fba172ef676	Backdoor.M
32519b85c0b422e4656de6e6c41878e95fd95026267daab4215ee59c107d6c77	76640508b1e7759e548771a5359eaed353bf1eec	Backdoor.M
d0d626deb3f9484e649294a8dfa814c5568f846d5aa02d4cdad5d041a29d5600	1b476f58ca366b54f34d714ffce3fd73cc30db1a	Backdoor.M

The following domain names are associated with this campaign and are also blocked:

- avsvmcloud[.]com
- databasegalore[.]com
- deftsecurity[.]com
- highdatabase[.]com
- incomeupdate[.]com

- panhardware[.]com
- thedoccloud[.]com
- zupertech[.]com