RQ11174687 - Suspicious File Downloaded from High Risk Categorized Site

SUMMARY

On Apr 15, 2022 at 4:21:57 AM EDT Splunk technology queries Palo Alto Firewall logs to produce a triggered alert warning of a presumed 'Suspicious File Downloaded from High Risk Categorized Site' in regards to web traffic following the malicious web request at a https://downloads.solarwinds.com/solarwinds/CatalogResources/Core/2019.4/2019.4.5220.20574 SolarWinds domain.
Primarily searching upon the 10.220.20.176 source IP and category ‘Malware’ outlined three malicious files whos transferrence is traceable between the 10.220.20.176(src_ip), 104.126.72.165 (dst_ip), 172.217.8.78 (dst_ip) addresses, from a time period spanning April 14, 2022 5:10:37 PM EDT to April 15, 2022 4:00:23 AM EDT. The downloaded malicious files were namely *superRiskySite.com/thisisnotmalware.exe*, *SolarWinds-Core-v2019.4.5220-Hotfix4.msp*, and *SolarWinds-Core-v2019.4.5220-Hotfix5.msp*.

A quick VirusTotal examination on both of the two alerted file hash artifacts “*3395856ce81f2b7382dee72602f798b642f14141*”(hash of SolarWinds-Core-v2019.4.5220-Hotfix4.msp) and “*3395856ce81f2b7382dee72602f798b642f14140*” (hash of SolarWinds-Core-v2019.4.5220-Hotfix5.msp) returns inconclusive results for the first, and malicious results for the latter (Hotfix5.msp). Specifically, performing a VirusTotal URL detective scan on the *SolarWinds-Core-v2019.4.5220-Hotfix5.msp* file returns malicious results that link the file to SUNBURST. Leveraging OSINT sources such as MalwarebytesLabs and Mandiant, information surfaces demarcating SUNBURST (CVE-2020-14005) as a supply chain attack that uses a trojanized backdoor to communicate via HTTP to third-party servers.

All analyzed file downloads are bound to the same source IP 10.220.20.176 which suggests this IP as the main target of exploitation. Analyzing destination addresses of the traffic coming from this source IP leads to discovery of an external public address 172.217.8.78, from which originates a high-risk unknown process 'superRiskySite.com/thisisnotmalware.exe’. Given this evidence, source IP 10.220.20.176 can be assumed to be involved in malicious C2 traffic between both internal and global (external) hosts. Lastly, VirusTotal scans upon the *thisisnotmalware.exe* process and the aforementioned SolarWinds-Core-v2019.4.5220-Hotfix4.msp return inconclusive results regarding the nature of these two files. Despite this, the Palo Alto WAF performs an action of ‘allowed’ for all malicious files.

GENERAL INFORMATION

Source IP:

- 10.220.20.176

Destination host:
- 104.126.72.165

Destination IP:
- 104.126.72.165

Destination port:
- 80 (HTTP)

Malware/Signature/Threat Name:
- SolarWinds-Core-v2019.4.5220-Hotfix5.msp

Exploit details (Vulnerable versions, fixes, etc.):
- Exploitation achieved by CVE-2020-14005 (SUNBURST)

Action:
- Allowed

Event Time/Date:
- April 14, 2022 5:10:37 PM EDT to April 15, 2022 4:00:23 AM EDT

Log Source:
- pan:threat

ANALYSIS

During the analysis phase of this incident, central pivot artifacts comprised of *src_ip, action, cat*, and *url*. Additionally, numerous 'message-contains' filters were performed to identify all events assigned classifications of 'high-risk', and 'malware'.

Analysis began with pivoting on the *src_IP* 10.220.20.176 to reveal outbound communications from the 104.126.72.165 host.

Pivoting off of the *3395856ce81f2b7382dee72602f798b642f14141* (SolarWinds-Core-v2019.4.5220-Hotfix4.msp) and *3395856ce81f2b7382dee72602f798b642f14140* (SolarWinds-Core-v2019.4.5220-Hotfix5.msp) hashes engaged file hash lookups using VirusTotal.

Pivoting off of the located https://downloads.solarwinds.com/solarwinds/CatalogResources/Core/2019.4/2019.4.5220.205

74/SolarWinds-Core-v2019.4.5220-Hotfix5.msp url allowed verification of malicious file download using VirusTotal.

Further, pivoting off the *cat* (cat: 'Malware') field allows identification of the 10.220.23.189 src_ip which is involved in a marked malicious download *SolarWinds-Core-v2019.4.5220-Hotfix4.msp.* Additionally, this pivot reveals src_ip:10.220.20.176's communication with an external private address 172.217.8.78 to download *thisisnotmalware.exe.*

RECOMMENDATION

The predominant malicious URL SolarWinds-Core-v2019.4.5220-Hotfix5.msp signifies the presence of a threat campaign premised on the SUNBURST backdoor exploit. Source IP 10.220.20.176 acts as a coordinator of malicious C2 traffic. To remediate this incident, continuous monitoring of the SolarWinds domain should be enacted, as well as education on the susceptibility of this domain to the CVE-2020-14005 vulnerability. Lastly, all internal hosts labeled as unessential to business function should be blacklisted from access of the aforementioned Solarwinds domain, until SolarWinds can release a remediating update/patch to the domain status