Threat Hunt Deep Dives: SolarWinds' Supply-Chain Compromise (Solorigate / SUNBURST Backdoor)

cyborgsecurity.com/cyborg_labs/threat-hunt-deep-dives-solarwinds-supply-chain-compromise-solorigate-sunburst-backdoor/

December 15, 2020

On December 13th 2020, it was unveiled by FireEye that SolarWinds has been impacted by a sophisticated supply chain compromise affecting their SolarWinds Orion software. A malicious backdoor was found to be present in the compromised software that FireEye has dubbed the SUNBURST backdoor. The impact of this compromise has been severe, SolarWinds boasts over 300,000+ customers world-wide and supplies its software to high-profile customers such as the majority of the Fortune 500, all five branches of the U.S. military, and many U.S. government agencies. The SolarWinds Orion software is an IT Management and Network Management System (NMS) which typically have access to key network infrastructure including network appliances, servers, and workstations making it a highly desirable target for attackers.

FireEye, the U.S. Department of the Treasury, and the U.S. Department of Commerce have all been compromised by this attack. The nature of the supply chain compromise, high-level profile of the attacks, and the malicious actors extreme attention to detail regarding operational security during post-exploitation have led to many reports regarding these attacks as conducted by a nation-state threat actor. Various, highly-regarded sources have attributed this attack to APT29 (aka Cozy Bear) which is believed to be associated with the Russian Foreign Intelligence Service (SVR).

IOCs

Domains:
avsvmcloud[.]com
deftsecurity[.]com
digitalcollege[.]org
freescanonline[.]com
globalnetworkissues[.]com
kubecloud[.]com
lcomputers[.]com
seobundlekit[.]com
solartrackingsystem[.]net
thedoccloud[.]com
virtualwebdata[.]com
webcodez[.]com

IPs:
3.16.81[.]254
3.87.182[.]149
3.87.182[.]149
13.57.184[.]217
13.59.205[.]66
18.217.225[.]111
18.220.219[.]143
34.219.234[.]134
54.193.127[.]66
54.215.192[.]52
196.203.11[.]89

SHA256 Hashes:
019085a76ba7126fff22770d71bd901c325fc68ac55aa743327984e89f4b0134
32519685c0b422e4656de6e6c41878e95fd95026267daab4215ee59c107d6c77
a25cadd48d70f6ea0c4a241d99c5241269e6faccb4054e62d16784640f8e53bc
ad1b2b89e60707a20e9eb1ca480bc3410ead40643b386d624c5d21b47c02917c
c09040d35630d75dfef0f804f320f8b3d16a481071076918e9b236a321c1ea77
ce77d116a074dab7a22a0fd4f2c1ab475f16eec42e1ded3c0b0aa8211fe858d6
d0d626deb3f9484e649294a8dfa814c5568f846d5aa02d4cdad5d041a29d5600
d3c6785e18fba3749fb785bc313cf8346182f532c59172b69adfb31b96a5d0af
dab758bf98d9b36fa057a66cd0284737abf89857b73ca89280267ee7caf62f3b
eb6fab5a2964c5817fb239a7a5079cabca0a00464fb3e07155f28b0a57a2c0ed

If you haven't already, watch *Threat Hunt Deep Dives Episode 2: Application Shimming!*