SolarWinds Orion Supply-chain Attack

Compiled by ThaiCERT, a member of the Electronic Transactions Development Agency

Version 0.9 (17 December 2020)

TLP:WHITE

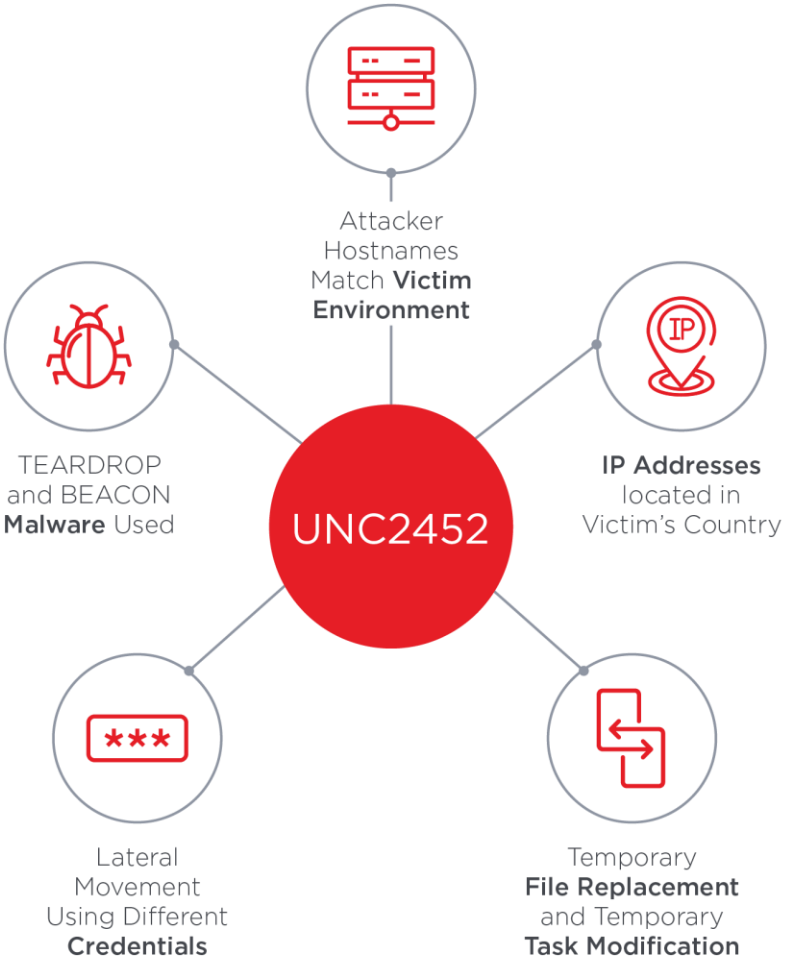
Attacker Hostnames Match Victim Environment
TEARDROP and BEACON Malware Used
UNC2452
IP Addresses located in Victim's Country
Lateral Movement Using Different Credentials
Temporary File Replacement and Temporary Task Modification

Figure 1: FireEye

Contents

Malware names

FireEye:	SUNBURST
Microsoft:	Solarigate

Management summary

Current situation:

- 18,000 customers have the malicious update installed (this may not necessarily mean all of those organizations have actually been breached).
- A patch (hotfix) has been made available by SolarWinds on 15 December.
- The malicious binaries are detected and removed by Microsoft Defender since 16 December.
- The main C2 infrastructure domain has been seized and sinkholed by Microsoft and the security industry and is now being used as a Killswitch for the malware.

Security organization FireEye was hit by a security breach in early December. Analyzing how the breach happened, they found it was done through a malicious software update of the SolarWinds Orion platform – i.e. a supply-chain attack[1].

Following the malicious infrastructure, they then found they were only one instance in a massive breach at many more organizations, many of which are government and military agencies.

SolarWinds is an IT (asset) management platform that is used by around 300,000 customers worldwide, of which around 425 of the Fortune 500, as well as many critical infrastructure organizations.

As for attribution, FireEye tracks this threat actor under the neutral name “UNC2452”. In the media, however, all sources point to a well-known APT called APT29/Cozy Bear, believed to be a Russian government sponsored group.

[1] <https://www.fireeye.com/blog/products-and-services/2020/12/global-intrusion-campaign-leverages-software-supply-chain-compromise.html>

Vulnerable systems

From SolarWinds' own advisory[2]:

SolarWinds® Orion® Platform software builds for versions 2019.4 HF 5, 2020.2 with no hotfix installed, and 2020.2 HF 1.

Prevention

- Patch your systems:
  - Orion Platform v2020.2 with no hotfix or 2020.2 HF 1: upgrade to Orion Platform version 2020.2.1 HF 2.
    The hotfix release 2020.2.1 HF 2 is now available in the SolarWinds Customer Portal at customerportal.solarwinds.com. We recommend that all customers update to release 2020.2.1 HF 2, as the 2020.2.1 HF 2 release both replaces the compromised component and provides several additional security enhancements.
  - Orion Platform v2019.4 HF 5: update to 2019.4 HF 6
- Analyze and possibly block access to the C2 servers as described in the various Malware analysis and advisories. Note that the various vendors report additional Indicators of Compromise, so please check all of them.

Recovery

- Microsoft published a blog "SolarWinds Post-Compromise Hunting with Azure Sentinel"[3]

[2] <https://www.solarwinds.com/securityadvisory>

[3] <https://techcommunity.microsoft.com/t5/azure-sentinel/solarwinds-post-compromise-hunting-with-azure-sentinel/ba-p/1995095>

References

US Government advisories

<https://us-cert.cisa.gov/ncas/current-activity/2020/12/13/active-exploitation-solarwinds-software>
<https://cyber.dhs.gov/ed/21-01/>

Malware analysis and advisories

<http://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html>
<https://www.fireeye.com/blog/products-and-services/2020/12/global-intrusion-campaign-leverages-software-supply-chain-compromise.html>
<https://github.com/fireeye/sunburst_countermeasures>
<https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/>
<https://blog.talosintelligence.com/2020/12/solarwinds-supplychain-coverage.html>
<https://blog.malwarebytes.com/threat-analysis/2020/12/advanced-cyber-attack-hits-private-and-public-sector-via-supply-chain-software-update/>
<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-solarwinds-supply-chain-attack>
<https://unit42.paloaltonetworks.com/fireeye-solarstorm-sunburst/>
<https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/sunburst-supply-chain-attack-solarwinds>
<https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/>
<https://www.picussecurity.com/resource/blog/ttps-used-in-the-solarwinds-breach>
<https://www.mcafee.com/blogs/other-blogs/mcafee-labs/sunburst-malware-and-solarwinds-supply-chain-compromise/>
<https://www.cadosecurity.com/post/responding-to-solarigate>
<https://blog.reversinglabs.com/blog/sunburst-the-next-level-of-stealth>
<https://github.com/RedDrip7/SunBurst_DGA_Decode>
<https://blog.cloudflare.com/solarwinds-orion-compromise-trend-data/>

Chain of events

Dec 13

<https://www.washingtonpost.com/national-security/russian-government-spies-are-behind-a-broad-hacking-campaign-that-has-breached-us-agencies-and-a-top-cyber-firm/2020/12/13/d5a53b88-3d7d-11eb-9453-fc36ba051781_story.html>
<https://www.nytimes.com/2020/12/13/us/politics/russian-hackers-us-government-treasury-commerce.html>
<https://www.wsj.com/articles/agencies-hacked-in-foreign-cyber-espionage-campaign-11607897866>
<https://www.cyberscoop.com/russian-hacking-treasury-commerce-fireeye/>
<https://www.theguardian.com/technology/2020/dec/13/us-treasury-hacked-group-backed-by-foreign-government-report>
<https://www.bankinfosecurity.com/us-commerce-treasury-hit-in-network-intrusions-a-15584>
<https://www.bankinfosecurity.com/hacked-us-commerce-treasury-departments-a-15584>
<https://apnews.com/article/technology-politics-national-security-hacking-e8a2e819f7cc6982f6a72f8c85209b72>
<https://www.nasdaq.com/articles/it-company-solarwinds-says-it-may-have-been-hit-in-highly-sophisticated-hack-2020-12-13>
<https://www.securityweek.com/us-investigating-computer-hacks-government-agencies>
<https://www.securityweek.com/us-government-confirms-cyberattack>
<https://thehackernews.com/2020/12/us-agencies-and-fireeye-were-hacked.html>
<https://www.databreaches.net/u-s-treasury-breached-by-hackers-backed-by-foreign-government-sources/>

Dec 14

<https://www.reuters.com/article/us-usa-cyber-amazon-com-exclsuive/exclusive-u-s-treasury-breached-by-hackers-backed-by-foreign-government-sources-idUSKBN28N0PG>
<https://www.theregister.com/2020/12/14/solarwinds_fireeye_cozybear/>
<https://www.zdnet.com/article/fireeye-confirms-solarwinds-supply-chain-attack/>
<https://krebsonsecurity.com/2020/12/u-s-treasury-commerce-depts-hacked-through-solarwinds-compromise/>
<https://www.bleepingcomputer.com/news/security/us-govt-fireeye-breached-after-solarwinds-supply-chain-attack/>
<https://www.cybereason.com/blog/the-solarwinds-supply-chain-attack-and-the-limits-of-cyber-hygiene>
<https://www.cyberscoop.com/solarwinds-supply-chain-treasury-commerce-espionage/>
<https://www.itnews.com.au/news/us-treasury-breached-by-hackers-558930>
<https://www.hackread.com/us-federal-agencies-hacked-russian-hackers/>

<https://www.bankinfosecurity.com/7-takeaways-supply-chain-attack-hits-solarwinds-customers-a-15585>
<https://abc7news.com/8753611/>
<https://isc.sans.edu/diary/rss/26884>
<https://securityaffairs.co/wordpress/112275/apt/solarwinds-supply-chain-attack.html>
<https://www.helpnetsecurity.com/2020/12/14/compromised-solarwinds-orion/>
<https://www.infosecurity-magazine.com/news/russian-hackers-data-supply/>
<https://www.riskiq.com/blog/external-threat-management/solarwinds-orion-hack/>
<https://www.securityweek.com/global-espionage-campaign-used-software-supply-chain-hack-compromise-targets-including-us-gov>
<https://www.theregister.com/2020/12/14/solarwinds_public_sector/>
<https://www.nytimes.com/2020/12/14/us/politics/russia-hack-nsa-homeland-security-pentagon.html>
<https://www.politico.com/news/2020/12/14/massively-disruptive-cyber-crisis-engulfs-multiple-agencies-445376>

SEC Filing: 18,000 out of 300,000 vulnerable customers

<http://d18rn0p25nwr6d.cloudfront.net/CIK-0001739942/57108215-4458-4dd8-a5bf-55bd5e34d451.pdf>
<https://www.zdnet.com/article/sec-filings-solarwinds-says-18000-customers-are-impacted-by-recent-hack/>
<https://www.darkreading.com/attacks-breaches/18000-organizations-possibly-compromised-in-massive-supply-chain-cyberattack-/d/d-id/1339716>
<https://www.itnews.com.au/news/solarwinds-says-fewer-than-18000-customers-compromised-558998>
<https://securityaffairs.co/wordpress/112294/hacking/solarwinds-sec-filing.html>
<https://www.securityweek.com/solarwinds-says-18000-customers-may-have-used-compromised-product>
<https://krebsonsecurity.com/2020/12/solarwinds-hack-could-affect-18k-customers/>
<https://www.infosecurity-magazine.com/news/solarwinds-our-office-365-emails/>
<https://thehackernews.com/2020/12/nearly-18000-solarwinds-customers.html>

15 Dec

<https://www.theregister.com/2020/12/15/solar_winds_update/>
<https://nypost.com/2020/12/15/russian-hackers-hit-dhs-dod-nih-state-department/>
<https://www.bankinfosecurity.com/blogs/target-selection-solarwinds-orion-big-fish-most-at-risk-p-2979>
<https://www.hackread.com/russian-hackers-hacked-homeland-security/>
<https://www.csoonline.com/article/3601508/solarwinds-supply-chain-attack-explained-why-organizations-were-not-prepared.html>
<https://www.cyberscoop.com/solarwinds-hack-dragos-ics-breach/>
<https://www.darkreading.com/attacks-breaches/concerns-run-high-as-more-details-of-solarwinds-hack-emerge/d/d-id/1339726>
<https://www.reuters.com/article/global-cyber-solarwinds/hackers-at-center-of-sprawling-spy-campaign-turned-solarwinds-dominance-against-it-idUSKBN28P2N8>
<https://www.infosecurity-magazine.com/news/dhs-cisa-ncsc-warnings/>
<https://arstechnica.com/information-technology/2020/12/solarwinds-hackers-have-a-clever-way-to-bypass-multi-factor-authentication/>
<https://www.schneier.com/blog/archives/2020/12/how-the-solarwinds-hackers-bypassed-duo-multi-factor-authentication.html>
<https://www.securityweek.com/group-behind-solarwinds-hack-bypassed-mfa-access-emails-us-think-tank>
<https://blog.sonicwall.com/en-us/2020/12/massive-supply-chain-attack-targets-solarwinds-orion-platform/>
<https://www.theverge.com/2020/12/15/22176053/solarwinds-hack-client-list-russia-orion-it-compromised>

Microsoft to quarantine compromised SolarWinds binaries tomorrow

<https://www.bleepingcomputer.com/news/security/microsoft-to-quarantine-compromised-solarwinds-binaries-tomorrow/>
<https://www.zdnet.com/article/microsoft-to-quarantine-solarwinds-apps-linked-to-recent-hack-starting-tomorrow/>
<https://www.infosecurity-magazine.com/news/microsoft-set-to-block-solarwinds/>

Microsoft and industry partners seize key domain used in SolarWinds hack

<https://www.zdnet.com/article/microsoft-and-industry-partners-seize-key-domain-used-in-solarwinds-hack/>
<https://securityaffairs.co/wordpress/112342/apt/microsoft-seized-c2-solarwinds-hack.html>

SolarWinds Issues Second Hotfix for Orion Platform Supply Chain Attack

<https://thehackernews.com/2020/12/solarwinds-issues-second-hotfix-for_15.html>
<https://www.securityweek.com/solarwinds-removes-customer-list-site-it-releases-second-hotfix>

Dec 16

<https://www.theregister.com/2020/12/16/solarwinds_github_password/>
<https://www.zdnet.com/article/solarwinds-said-no-other-products-were-compromised-in-recent-hack/>
<https://www.deepinstinct.com/2020/12/16/sunburst-trojan-what-you-need-to-know/>
<https://www.helpnetsecurity.com/2020/12/16/solarwinds-hackers-capabilities/>
<https://www.cyberscoop.com/solarwinds-white-house-national-security-council-emergency-meetings/>
<https://www.bankinfosecurity.com/solarwinds-hunt-to-figure-out-who-was-breached-a-15608>
<https://www.securityweek.com/hack-may-have-exposed-deep-us-secrets-damage-yet-unknown>
<https://securityintelligence.com/posts/update-widespread-supply-chain-compromise/>
<https://thehackernews.com/2020/12/new-evidence-suggests-solarwinds.html>
<https://www.linkedin.com/posts/karimhijazi_prevailionknows-cybersecurity-solarwinds-activity-6744862284868390912-BUb1/>
<https://www.nytimes.com/2020/12/16/opinion/fireeye-solarwinds-russia-hack.html>

Malicious Domain in SolarWinds Hack Turned into ‘Killswitch’

<https://krebsonsecurity.com/2020/12/malicious-domain-in-solarwinds-hack-turned-into-killswitch/>
<https://www.bleepingcomputer.com/news/security/fireeye-microsoft-create-kill-switch-for-solarwinds-backdoor/>
<https://www.cyberscoop.com/fireeye-microsoft-solar-winds-killswitch-hack/>
<https://www.darkreading.com/attacks-breaches/fireeye-identifies-killswitch-for-solarwinds-malware-as-victims-scramble-to-respond/d/d-id/1339746>
<https://securityaffairs.co/wordpress/112376/apt/solarwinds-backdoor-kill-switch.html>