verizon

Verizon Business Consulting Services
Cyber Security Consulting

Verizon Cybersecurity Solutions Intelligence Summary (INTSUM)

For the week ending 2020-12-18

Weekly Summary

The milestone attack abusing the SolarWinds Orion update process will probably eclipse WannaCry as the most costly cyberattack. The 18,000 SolarWinds customers exposed to the first stage Sunburst malware will be threat hunting to determine if they were among the priority targets for the attackers. Microsoft identified more than 40 customers that were "targeted more precisely and compromised through additional and sophisticated measures." Target-centric intelligence analysis of those companies is more useful than unsupported attribution assertions. 17,900+ companies have to search for evidence that was never present. Like WannaCry, SQL Slammer, Witty and Code Red, what we think we know at D+7 will be a fraction of what we have to learn in the coming weeks.

- *Prefaces/Tags:*

TTP: tactics, techniques and procedures	**YARA**: intelligence includes a YARA rule
SA: situational awareness	**KT:** Key takeaway(s)
IOC: network indicators of compromise (IP, FQDN, Snort IDs). Hash digests and registry keys are IOC; collections with only hashes or keys will not usually have the IOC preface. (**IOC links will be in bold**)	
(Gnnnn) (Group) **(Snnnn)** (Software) **(Tnnnn)** (Tactic/Technique) **MITRE ATT&CK ID# (beta)**	

Significant new threats

- *SolarWinds/Sunburst/Solorigate:* The cut-off of new intelligence and updated analysis for this INTSUM was 2300 UTC Saturday December 19th, 2020. This intelligence almost certainly will have changed significantly since this section was written.
- *Top intelligence:* **(TTP&IOC)**
  - Cybersecurity and Infrastructure Security Agency (CISA) AA20-352A | **"Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations."** CISA has revised this alert twice, most recently on the 19th key changes:
    - *CISA has evidence that **there are initial access vectors other than the SolarWinds Orion** platform. Specifically, we are investigating incidents in which activity indicating abuse of SAML tokens consistent with this adversary's behavior is present, yet where impacted SolarWinds instances have not been identified. CISA is working to confirm initial access vectors and identify any changes to the TTPs.* (**bold** emphasis by VTRAC)
    - *"Updated mitigation guidance, indicators of compromise table, and provided a **downloadable STIX file** of the IOCs."*
  - NSA | "Cybersecurity Advisory: (Full) Detecting Abuse of Authentication Mechanisms." Warning about two techniques hackers are using to escalate access from compromised local networks into cloud-based infrastructure. SolarWinds was only mentioned as one of 20 references on the penultimate page.
  - NSA | "Russian State-Sponsored Actors Exploiting Vulnerability in VMware Workspace ONE Access Using Compromised Credentials." The first reference in the NSA authentication advisory was to last week's advisory on VMWare attacks. *KrebsonSecurity* published "VMware Flaw a Vector in SolarWinds Breach?" connecting the dots between the VMWare vulnerability and the SolarWinds attacks.
  - Volexity | **"Dark Halo Leverages SolarWinds Compromise to Breach Organizations."** Volexity documented three incident response engagements with one USA-based think tank. They attributed them to an actor they labeled "Dark Halo." Only one of the three engagements involved SolarWinds and Sunburst malware. One of the other engagements may be the more

valuable intelligence as it involved a new security feature bypass of Duo multi-factor authentication. Lateral exploitation led to the beach of an Outlook Web Access server and compromise of Duo integration secret key allowing the attacker to pre-compute the Duo challenge/response. Duo was not mentioned in the NSA advisory.

- Microsoft | "A moment of reckoning: the need for a strong and global cybersecurity response." Microsoft President Brad Smith writing about "presidential goodness." He included some technical intelligence content: Microsoft found SolarWinds malware in their systems but no evidence of malicious activity; SolarWinds reported 18,000 customers exposed to SolarWinds malware, but Microsoft found only 40 were "compromised through additional and sophisticated measures." Kaspersky found 100 of their customers received the Trojanized DLL, but "none were interesting to the attackers to receive the 2nd stage of the attack." Graphics useful for briefings.
- Microsoft | **"Analyzing Solorigate, the compromised DLL file that started a sophisticated cyberattack."** While Microsoft's analysis is interesting, the threat hunting advice in the last ¼ of the post has not been previously reported.
- ReversingLabs | **"SunBurst: the next level of stealth."** Deep-dive malware analysis with insights into threat actor's strategy and evasion efforts. Measures for resisting supply-chain attacks.
- Sentinel Labs | "SolarWinds SUNBURST Backdoor: Inside the APT Campaign." Another malware analysis with post-compromise threat-hunting intelligence.
- McAfee | **"SUNBURST Malware and SolarWinds Supply Chain Compromise,"** and **"Additional Analysis into the SUNBURST Backdoor."**
- Kaspersky | **"Sunburst: connecting the dots in the DNS requests."** Examining the backdoor's DNS communications led researchers to companies that were flagged for further exploitation in the campaign. *KrebsonSecurity* published "Malicious Domain in SolarWinds Hack Turned into 'Killswitch,'" connecting the dots between DNS and SolarWinds response.
- Varonis | "SolarWinds SUNBURST Backdoor: Inside the Stealthy APT Campaign." Incident analysis suggesting cause of the initial breach: *"The prevailing theory, not yet confirmed by SolarWinds, is that the attackers used exposed FTP server credentials found on GitHub in 2018 to gain access to the company's software update infrastructure."*

Noteworthy attacks

- *Summary:* **(TTP&IOC&YARA)** Facebook | ***"Taking Action Against Hackers in Bangladesh and Vietnam."*** Cybersecurity researchers from Facebook linked the activities of a Vietnamese APT threat actor to an IT company in Ho Chi Minh City after the group was caught abusing its platform to hack into people's accounts and distribute malware. According to Facebook, APT32 created fictitious personas, posing as activists and business entities, and used romantic lures to reach out to their targets, ultimately tricking them into downloading rogue Android apps through Google Play Store that came with a wide range of permissions to allow broad surveillance of peoples' devices. |

Malicious code evolution

- *Summary:* **(TTP&IOC)** Sophos | **"Ransomware operators use SystemBC RAT as off-the-shelf Tor backdoor."** Researchers at Sophos detected hundreds of SystemBC deployments globally, including in recent Ryuk and Egregor ransomware attacks in combination with post-exploitation tools. In some cases, the backdoor was deployed after the attackers gained administrative credentials and moved deeper into a compromised network. SystemBC is a commodity RAT sold in Russian underground markets. **Proofpoint** was the source of our first SystemBC-related collection in August 2019. The researchers noted that SystemBC continues to evolve, with its most recent samples using the Tor anonymizing network to encrypt and hide the destination of C2 traffic.
- *Summary:* **(TTP&IOC)** Lookout | ***"New Spyware Used by Sextortionists to Blackmail iOS and Android Users."*** Researchers discovered Android and iOS spyware, they named "Goontact," targeting users in China, Korea, Japan, Thailand and Vietnam. The threat actor targets visitors of sites offering escort and similar services, and convinces them to install or sideload a purported secure messaging app. The ultimate goal of the campaign is believed to be extortion and blackmail. The Android version of the malicious app is capable of exfiltrating contacts, SMS messages, photos on external storage, location information, phone numbers, and more. The iOS version is only capable of stealing a victim's phone number and contact list, as well as communicating with C2 to display tailored messages to the user. The app was developed using enterprise certificates belonging to legitimate companies.