SEQURETEK

Timeline Perspective of the SolarStorm Supply-Chain Attack

OVERVIEW

On Dec. 13, the cyber community observed one of the most significant cybersecurity events of our time, impacting both commercial and government organizations worldwide.

The event was a supply-chain attack on SolarWinds Orion software conducted by suspected nation-state operators that is being tracked as SolarStorm. This event can be traced back to an attack successfully prevented earlier this year.

KNOWLEDGE BASE REGISTER

- Version Control

Issue Date	Version	Prepared by	Approved by
28th Dec 2020	v 1.0	Sameer Prabhu	Cdr. Subhash Dutta

OVERVIEW

- On 13th Dec. 2020, the cyber community observed one of the most significant cybersecurity events of our time, impacting both commercial and government organizations around the world.
- The event was a supply-chain attack on SolarWinds Orion software conducted by suspected nation-state operators that is being tracked as SolarStorm.
- This event can be traced back to an attack successfully prevented earlier this year.
- While this is not the first software supply-chain compromise, it may be the most notable, as the attacker was trying to gain widespread, persistent access to a number of critical networks.
- Given the importance of the event, Palo Alto Networks published a timeline of the attack based on extensive research into the information available.
- This invaluable information to cybersecurity professionals in the industry will help in responding to this attack, as well as to other researchers piecing together the event details.
- While the information available is being traced together, there is no complete knowledge of when the planning and execution of this campaign began.
- However, evidence suggests that SolarStorm command and control (C2) infrastructure was set up as early as August 2019.

TECHNICAL DETAILS

- The first modified SolarWinds software was released in October 2019, and the earliest related Cobalt Strike payload identified was generated using Cobalt Strike 4.0, which was built in December 2019.
- It is unclear when SolarStorm first compromised the SolarWinds software supply chain or the method by which they accomplished this task.
- Additionally, multiple reports indicate that SolarStorm employed additional initial access vectors beyond the compromised SolarWinds software. Reports tracking these have not confirmed other techniques used to obtain initial access to networks at this time.
- Of course, an adversary with the capability to execute this campaign could have used many additional means to accomplish their goal.
- Analysis of the SolarWinds software revealed code modification as early as October 2019, although the first weaponized software updates, denoted as SUNBURST malware, were not released until approximately March 2020.

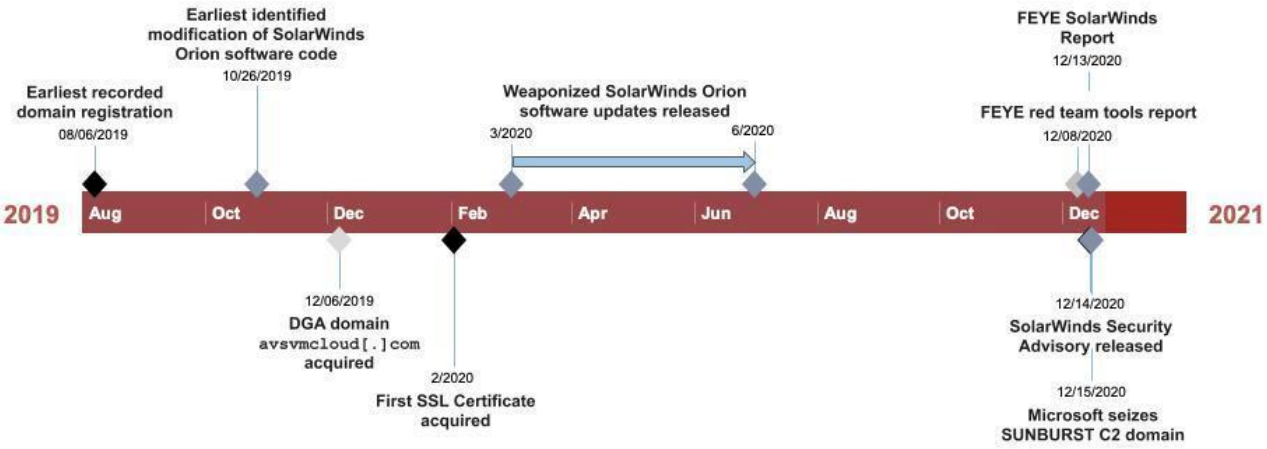

Figure 1: SolarStorm Visual Timeline (source: Palo Alto)

- Two samples of the modified SolarWinds software have appeared as early as October 2019.
- The majority of the infrastructure observed in this campaign was acquired between December 2019 and March 2020; however, at least one domain, incomeupdate[.]com, noted in Cobalt Strike BEACON activity, was registered in August 2019.
- SSL certificates for many of the associated domains were acquired by SolarStorm operators between February and April 2020, with at least one certificate extending to July.
- The extensive infrastructure build-out throughout this timeline helps to visualize the persistence of the operation from initial targeting to completion of the objective. SolarStorm threat actors are highly skilled and thorough in their operational handling.
- A review of DNS Security logs for requests to avsvmcloud[.]com, the domain used with a domain generation algorithm (DGA) in this activity for better understanding the timing around when organizations installed the malicious SUNBURST update revealed start in April, shortly after SolarStorm distributed the malicious update.
- It also displayed a slowly rise with a peak in July and then a trail off.
- Microsoft and industry partners seized control of this domain on Dec. 15. They used it to send a form of "killswitch" command, instructing SUNBURST to terminate itself and prevent further execution.

- During analysis of the information available, related activity involving TEARDROP malware that was used to execute a customized Cobalt Strike BEACON was identified. The sample contained a beacon request to the previously unreported domain mobilnweb[.]com.
- While some of these domains have a registration date earlier than the dates depicted, the dates shown are the domain modification dates believed to be when the actors acquired control over the domain. The variation in registration date vs. the time of acquisition by SolarStorm provides an added sense of legitimacy for the domains in use.

Domain	Assessed Actor Controlled Date	Registrar
incomeupdate[.]com	8/6/19	NameCheap
zupertech[.]com	10/10/19	NameSilo
avsvmcloud[.]com	12/6/2019	GoDaddy
mobilnweb[.]com	12/19/19	NameCheap
highdatabase[.]com	12/26/19	NameSilo
solartrackingsystem[.]net	1/7/20	NameSilo
webcodez[.]com	1/15/20	NameCheap
panhardware[.]com	1/18/20	NameSilo
websitetheme[.]com	1/27/20	NameSilo
thedoccloud[.]com	2/5/20	NameSilo
seobundlekit[.]com	2/6/20	NameCheap
freescanonline[.]com	2/10/20	NameCheap
deftsecurity[.]com	2/12/20	NameSilo
virtualwebdata[.]com	2/13/20	NameSilo
digitalcollege[.]org	3/5/20	NameCheap
databasegalore[.]com	3/12/20	NameCheap
zupertech[.]com	3/15/20	NameSilo
lcomputers[.]com	6/22/20	NameSilo

Table 1. SolarStorm Domain acquisition timeline (source: Palo Alto)

- The SSL certificates observed in connection with SolarStorm infrastructure were issued by Sectigo RSA Domain Validation Secure Server CA.

Domain	SSL Certificates SHA-1	Dates Valid
websitetheme[.]com	66576709A11544229E83B9B4724FAD485DF143AD	2/3/20 – 2/2/21
thedoccloud[.]com	849296C5F8A28C3DA2ABE79B82F99A99B40F62CE	2/6/20 – 2/5/21
seobundlekit[.]com	E7F2EC0D868D84A331F2805DA0D989AD06B825A1	2/6/20 – 2/5/21
freescanonline[.]com	8296028C0EE55235A2C8BE8C65E10BF1EA9CE84F	2/11/20 – 2/10/21
solartrackingsystem[.]net	91B9991C10B1DB51ECAA1E097B160880F0169E0C	2/12/20 – 2/11/21
virtualwebdata[.]com	AB93A66C401BE78A4098608D8186A13B27DB8E8D	2/13/20 – 2/13/21
deftsecurity[.]com	12D986A7F4A7D2F80AAF0883EC3231DB3E368480	2/13/20 – 2/12/21
digitalcollege[.]org	FDB879A2CE7E2CDA26BEC8B37D2B9EC235FADE44	3/5/20 – 3/5/21
databasegalore[.]com	D400021536D712CBE55CEAB7680E9868EB70DE4A	3/12/20 – 3/12/21
mobilnweb[.]com	2C2CE936DD512B70F6C3DE7C0F64F361319E9690	4/3/20 – 4/3/21
panhardware[.]com	AF6268F675ED810D804745970927E36D12AC9B0A	4/10/20 – 4/10/21
incomeupdate[.]com	B654148983439E28802166449A8F413B9C995547	4/14/20 – 4/14/21
highdatabase[.]com	35AEFF24DFA2F3E9250FC874C4E6C9F27C87C40A	4/16/20 – 4/17/21
zupertech[.]com	B80B01AE313C106F70502142F2B2BCFFC7E15ABD	5/13/20 – 5/13/21
lcomputers[.]com	7F9EC0C7F7A23E565BF067509FBEF0CBF94DFBA6	6/23/20 – 6/24/21
webcodez[.]com	2667DB3592AC3955E409DE83F4B88FB2046386EB	7/8/20 – 7/8/21

Table 2. SSL certificates associated with SolarStorm domain activity

- There have been reports indicating additional techniques and tools used with this incident.
  - VMware: VMware has been associated with SolarStorm attack in two ways.
    - An advisory released by NSA earlier this month about CVE-2020-4006, a command injection vulnerability, states that Russian state-sponsored actors were actively exploiting the vulnerability and suggesting US Government agencies patch immediately.
    - The vulnerability exists in five VMware software products focused on identity and access management.
    - Exploitation allows attackers to deploy a webshell on the system and gain access to protected data.
    - This vulnerability can only be exploited by someone who has already authenticated to the system and indicates that when leveraged, it likely is used to gain additional access once the attacker is already inside the networks.
    - Second, VMware stated they have SolarWinds Orion systems in their environment, but they have not seen any evidence of exploitation. However, there has been no indication that VMware's software was used as an infection vector or a TTP utilized within the SolarStorm attack.
  - Microsoft / SAML: Microsoft published multiple reports on activity related to this attack campaign, including a summary of the backdoor implanted into SolarWinds Orion (referred to by Microsoft as Solorigate), as well as guidance for their customers on protecting themselves. They have publicly stated they are working with more than 40 companies who have been targeted in this attack.
    - One specific component of the attack that Microsoft has discussed in detail is what they have observed in compromised networks with regard to identity infrastructure. Specifically, the attackers have exfiltrated SAML token signing certificates that allow them to forge tokens and access any resources trusted by those certificates. Microsoft has observed these forged tokens presented to the Microsoft cloud on behalf of their customers.
    - The impact of a compromise of these certificates implies the attacker gained the highest level of privileges inside the network and used them to establish long-term access to the network.
  - SUPERNOVA Webshell: FireEye's initial report on the SolarWinds compromise included indicators for a webshell they call SUPERNOVA. Since publication, FireEye has removed those indicators as they no longer believe they were used as a result of the SolarWinds

software compromise. This webshell may not be related, but it is still vital to defend against it.

- MFA Bypass: The SAML token-forging attack allows an attacker to evade multi-factor authentication systems, as in that case, the authentication system itself is compromised.
  - A recently published security risk report about a threat group named Dark Halo has now been connected to SolarStorm. The report describes that the attacker targeted the "integration secret key" used to connect Cisco's Duo Multi-Factor Authentication (MFA) solution to an Outlook Web Access server. With that key, they were able to pre-compute the token codes necessary for authentication.
  - Once again, similar to the SAML token-forging attack, this MFA bypass requires a significant compromise of the systems used to authenticate users and would have been performed post-compromise to extend the attacker's access to the network.
- Other Initial Access Vectors: On Dec. 19, CISA updated their alert on the threat to include this note:
  - "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 Security Assertion Markup Language (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. CISA will update this Alert as new information becomes available."

PREVENTIVE AND CORRECTIVE DEFENCE ACTIONS

- Employ content scanning and filtering on the organization mail servers. Inbound e-mails should be scanned for known threats and should block any attachment types that could pose a threat.
- Update your Operating system and software to latest version.
- Ensure anti-virus and anti-malware solutions are set to automatically update and regular scans are conducted.
- Do not trust emails from untrusted source.
- Do not open links and attachments from untrusted sources.
- Back-up data, store it outside of network connection.
- Use strong password and change it at regular interval. Use multi-factor authentication.

- Implement strict access control and auditing in your environment at operating system and network layers.
- Deploy a FIPS validated Hardware Security Module (HSM) to store on-premises token signing certificate private keys (aggressively updated HSM, makes it very difficult for actors who have compromised the system to steal the private keys and use them outside of the network)
- Ensure core privileged cloud administrative users, groups, and roles are not impacted by data synchronized from on premises environments.
- The cloud administrative roles should not authenticate with SAML SSO, but instead rely on cloud-only authentication.
- We recommend at minimum utilizing Windows Authentication, or implementing a SAML v2 based solution, if you cannot integrate Windows or SAML-based authentication.