CISA Identifies SUPERNOVA Malware During Incident Response

cisa.gov/news-events/analysis-reports/ar21-112a

Analysis Report

Last Revised

April 29, 2021

Alert Code

AR21-112A

From at least March 2020 through February 2021, the threat actor connected to the entity via the entity's Pulse Secure VPN appliance (*External Remote Services* [T1133]). The threat actor connected via the U.S.-based residential IP addresses listed below, which allowed them to masquerade as teleworking employees. (**Note:** these IP addresses belong to routers that are all similar models; based on this activity, CISA suspects that these routers were likely exploited by the threat actor.)

- `207.89.9[.]153`
- `24.140.28[.]90`
- `24.117.18[.]111`

The threat actor authenticated to the VPN appliance through several user accounts (*Valid Accounts* [T1078]), none of which had multi-factor authentication (MFA) enabled. (CISA does not know how the threat actor initially obtained these credentials.) Once authenticated to the VPN appliance, the threat actor initiated a VPN connection to the environment (*External Remote Services* [T1133]). The media access control (MAC) address of the threat actor's machine as recorded in the VPN appliance logs indicates use of a virtual machine. The threat actor then moved laterally to the entity's SolarWinds Orion appliance (*Lateral Movement* [TA0008]) and established *Persistence* [TA0003] by using a PowerShell script (Command and Scripting Interpreter: *PowerShell* [T1059.001]) to decode (*Deobfuscate/Decode Files or Information* [T1140]) and install SUPERNOVA (*Ingress Tool Transfer* [T1105], Server *Software Component: Web Shell* [T1505.003]). The SUPERNOVA webshell allows a remote operator to dynamically inject C# source code into a web portal provided via the SolarWinds software suite. The injected code is compiled and directly executed in memory. For more information on SUPERNOVA, refer to MAR-10319053-1.v1 - SUPERNOVA.

The threat actor was able to dump credentials from the SolarWinds appliance via two methods (*Credential Access* [TA0006]).

- The threat actor used `Export-PfxCertificate` to gather cached credentials used by the SolarWinds appliance server and network monitoring (*Unsecured Credentials: Private Keys* [T1552.004]). The private key certificate must have been marked as exportable; either the threat actor was able to change or bypass that property prior, or the affected entity mistakenly marked the certificate exportable.
- The threat actor placed a copy of `procdump.exe` (*Ingress Tool Transfer* [T1105])—disguised as the entity's logging infrastructure, `splunklogger.exe` (*Masquerading: Rename System Utilities* [T1036.003])—on the SolarWinds Orion server. The threat actor used this tool and the system-level access to dump Local Security Authority Subsystem Service (LSASS) memory to obtain additional credentials (*OS Credential Dumping: LSASS Memory* [T1003.001]). Once the credentials were dumped, the threat actor placed them in the `c:\inetpub\SolarWinds\ja\license.txt` directory (*Data Staged: Local Data Staging* [T1074.001]), and the threat actor made a `GET` request to the entity's internet information services (IIS) server to *Exfiltrate* [TA0010] the file (*Exfiltration Over C2 Channel* [T1041]). The threat actor deleted the IIS logs for the date in question (*Indicator Removal on Host: Clear Windows Event Logs* [T1070.001]).

CISA believes the logs would have likely revealed the threat actor exploited CVE-2020-10148, an authentication bypass vulnerability in SolarWinds Orion Application Programming Interface (API) that allows a remote attacker to execute API commands.[2] CISA believes the threat actor leveraged CVE-2020-10148 to bypass the authentication to the SolarWinds appliance and then used SolarWinds Orion API `ExecuteExternalProgram()` to run commands with the same privileges the SolarWinds appliance was running (in this case `SYSTEM`). CISA had not observed the threat actor using privileged accounts prior to the credential dumps, and the account being used to connect to the SolarWinds appliance (via VPN) did not have sufficient privilege to access it. The PowerShell process that initiated the credential harvesting and installation of SUPERNOVA was a child process of the `solarwindsbusinesslayer.exe` process. Two `GET` requests were logged in the following day's log, with the internal Dynamic Host Configuration Protocol (DHCP) address given to the threat actor's machine by the VPN appliance minutes after the exploitation, suggesting the threat actor was interacting with the SolarWinds web application. (**Note:** although the threat actor likely exploited CVE-2020-10148, it could have also exploited another API authentication bypass or remote code execution (RCE) vulnerability.)

Several weeks later, the threat actor connected again via the VPN appliance and attempted to use credentials gained from the SolarWinds appliance. The threat actor connected to one machine via Server Message Block (SMB) (Transmission Control Protocol [TCP] port 445) and then attempted to login to an additional workstation (*Remote Services: SMB/Windows Admin Shares* [T1021.002]). No additional activity was observed during this session.

On another occasion, the threat actor connected to the environment via the VPN and used Windows Management Instrumentation (WMI) (*Windows Management Instrumentation* [T1047]) to remotely launch a tasklist to determine the process ID for the LSASS process (*Process Discovery* [T1057]). Then the threat actor, via WMI (*Windows Management Instrumentation* [T1047]), launched `procdump.exe`, which was disguised as `wininit.exe` (*Masquerading: Match Legitimate Name or Location* [T1036.005]). After this, the threat actor placed and ran `winrar`, which was also disguised as `wininit.exe` (*Masquerading: Match Legitimate Name or Location* [T1036.005]), to archive credentials (*Archive Collected Data: Archive via Utility* [T1560.001]) before *Exfiltration* [TA0010]. CISA observed the disguised `wininit.exe`commands on two separate machines—one server and one workstation. The commands executed were:

- `cmd /c tasklist /vc:\windows\temp\TS_85ET.tmp`
- `procdump.exe`:

  `cmd.exe c:\windows\temp\wininit.exe -accepteula -ma 992 c:\windows\temp\TS_9D3C.tmp`
- `winrar.exe`:

  `c:\windows\temp\wininit.exe a c:\windows\temp\googleupdate.tmp -hpJimJameJump c:\windows\temp\TS_9D3C.tmp.dmp` CISA also observed the threat actor perform *Discovery* [TA0007]. Specifically, the threat actor sent single Internet Control Message Protocol (ICMP) packets to other network infrastructure within the entity to determine if a communications path existed (*Remote System Discovery* [T1018]) and looked for files on the domain administrator's desktop as well as a ManageEngine server (*File and Directory Discovery* [T1083]).

Upon discovery of the incident, the affected entity performed incident response in accordance with its incident response plan, and CISA's engagement is ongoing. CISA encourages organizations to apply the recommendations provided in the Recommendations section. Organizations observing related activity should to enact their incident response plan.

Recommendations

CISA recommends all organizations implement the following practices to strengthen the security posture of their organization's systems.

- Check for instances of common executables executing with the hash of another process (e.g., `splunklogger.exe` with the hash of `procdump`).
- Implement MFA, especially for privileged accounts.
- Use separate administrative accounts on separate administration workstations.
- Implement Local Administrator Password Solution (LAPS).
- Implement the principle of least privilege on data access.

- Secure Remote Desktop Protocol (RDP) and other remote access solutions using MFA and "jump boxes" for access.
- Deploy and maintain endpoint defense tools on all endpoints.
- Ensure all software is up to date.

  If your organization has ever used SolarWinds Orion versions 2019.4 through 2020.2.1 HF1, refer to CISA's Emergency Directive ED 21-01, associated supplemental guidance, and CISA's Activity Alert AA20-352A for additional guidance prior to applying patches. Although ED 21-01 and associated guidance only apply to Federal Civilian Executive Branch agencies, CISA encourages non-federal entities to review them for recommendations on operating the SolarWinds Orion platform.
- Maintain up-to-date antivirus signatures and engines.
- Restrict users' ability (permissions) to install and run unwanted software applications. Do not add users to the local administrators' group unless required.
- Enforce a strong password policy and implement regular password changes.
- Enable a personal firewall on organization workstations that is configured to deny unsolicited connection requests.
- Disable unnecessary services on organization workstations and servers.

Summary

This Alert uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) framework. See the ATT&CK for Enterprise framework for all referenced threat actor techniques.

The Cybersecurity and Infrastructure Security Agency (CISA) recently responded to an advanced persistent threat (APT) actor's long-term compromise of an entity's enterprise network, which began in at least March 2020. The threat actor connected to the entity's network via a Pulse Secure virtual private network (VPN) appliance, moved laterally to its SolarWinds Orion server, installed malware referred to by security researchers as SUPERNOVA (a .NET webshell), and collected credentials. **(*Updated April 29, 2021*) Note:** at this time CISA cannot link this activity to exploitation of CVE-2021-22893 as addressed in AA21-110A. The entity has run the Ivanti Pulse Secure Connect Integrity Tool and found activity consistent with mismatched files. CISA is still investigating the root cause for the mismatched files.

SUPERNOVA is a malicious webshell backdoor that allows a remote operator to dynamically inject C# source code into a web portal to subsequently inject code. APT actors use SUPERNOVA to perform reconnaissance, conduct domain mapping, and steal sensitive information and credentials. (**Note:** for more information on SUPERNOVA, refer to Malware Analysis Report MAR-10319053-1.v1 - SUPERNOVA.) According to a SolarWinds advisory, SUPERNOVA is not embedded within the Orion platform as a supply chain attack; rather, an attacker places it directly on a system that hosts SolarWinds Orion, and it is designed to appear as part of the SolarWinds product.[1] CISA assesses this is a separate actor than the APT actor responsible for the SolarWinds supply chain compromise described in Alert AA20-352A: Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations. Organizations that find SUPERNOVA on their SolarWinds installations should treat this incident as a separate attack.

This report provides tactics, techniques, and procedures (TTPs) CISA observed during an incident response engagement. (**Note:** this threat actor targeted multiple entities in the same period; some information in this Analysis Report is informed by other related incident response engagements and CISA's public and private sector partners.) This APT actor has used opportunistic tradecraft, and much is still unknown about its TTPs.

For a downloadable copy of indicators of compromise (IOCs) associated with this malware, see AR21-112A.stix and Malware Analysis Report MAR-10319053-1.v1.stix.

References

[1] SolarWinds Security Advisory: SUNBURST and SUPERNOVA
[2] CERT/CC Vulnerability Note VU#843464: SolarWinds Orion API authentication bypass allows remote command execution

Revisions

April 22, 2021: Initial Version|April 29, 2021: Added New Note in Summary