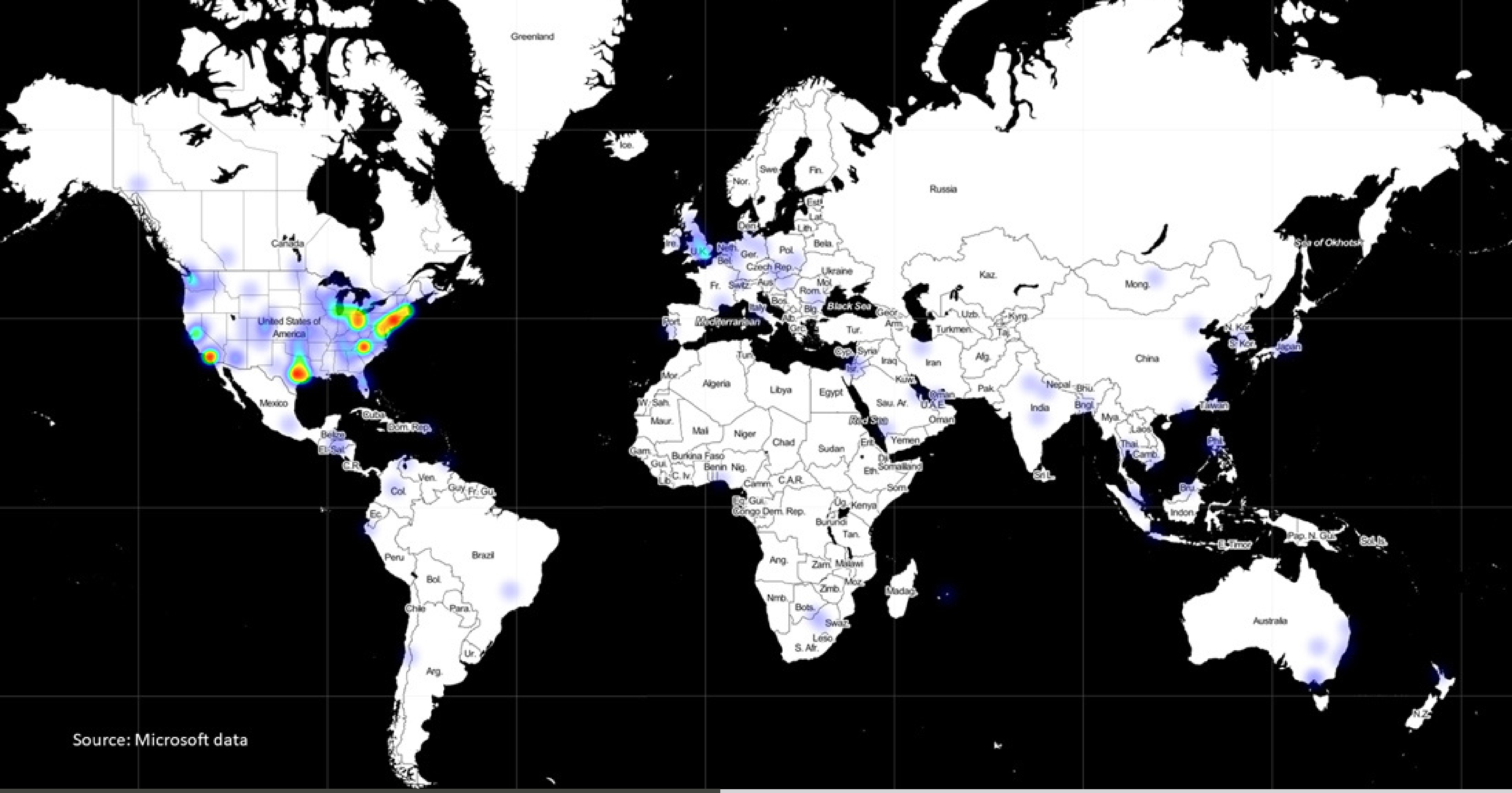
OPERATION SUNBURST

AN INDEPTH LOOK INTO SOLAR WINDS SUPPLY CHAIN HACK

REPORT BY ARGONYTE



Source: Microsoft data

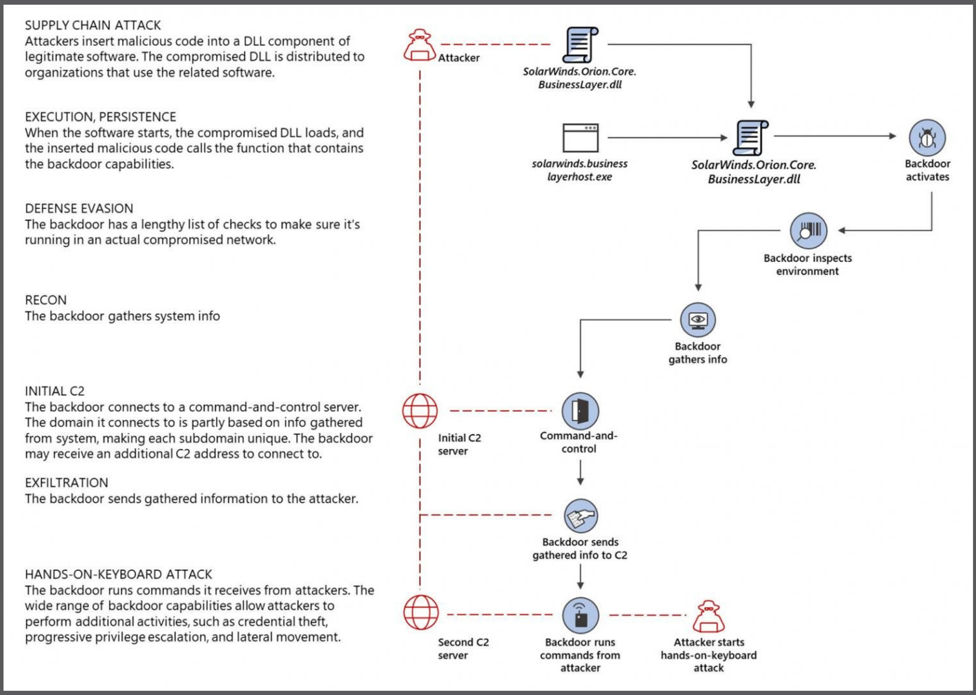
AN OVERVIEW

On December 8th, 2020, FireEye had announced that they had been breached by a nation-state adversary with top-tier offensive capabilities. This adversary, according to them, was highly trained in OPSEC. The Development teams deployed anti-analysis countermeasures and the Operational Teams have used specific infrastructure for each victim, in turn reducing the usefulness of Network-based IOCs.

Further investigations revealed that UNC2452 (FireEye)/DarkHalo (Volexity)/ SolarStorm(Palo Alto) is behind the attack. Though FireEye explicitly states that UNC2452 does not share code with any other know samples, few other external sources state that APT29 is behind this.

Following FireEye's Investigation, on 13th December 2020, it was revealed that Solar Winds Orion NMS products have had Trojanized Updates and have been active since March 2020. The malicious updates had been pushed out to nearly 18k customers out of the 300k customers.

The campaign, now known as SUNBURST, used signed, backdoored infected DLL's to gain access to organizations. The backdoor in question was being exploited in SolarWinds Orion Network Management V2019.4 to 2020.2.1. This attack not only targeted Companies but several large U.S. Federal Agencies, including the Department of Treasury, Department of Energy, and Department of Homeland Security. The prevailing theory is that attackers used exposed FTP server credentials found on GitHub in 2018 to gain access to Company's software update infrastructure.



SUPPLY CHAIN ATTACK
Attackers insert malicious code into a DLL component of legitimate software. The compromised DLL is distributed to organizations that use the related software.

EXECUTION, PERSISTENCE
When the software starts, the compromised DLL loads, and the inserted malicious code calls the function that contains the backdoor capabilities.

DEFENSE EVASION
The backdoor has a lengthy list of checks to make sure it's running in an actual compromised network.

RECON
The backdoor gathers system info

INITIAL C2
The backdoor connects to a command-and-control server. The domain it connects to is partly based on info gathered from system, making each subdomain unique. The backdoor may receive an additional C2 address to connect to.

EXFILTRATION
The backdoor sends gathered information to the attacker.

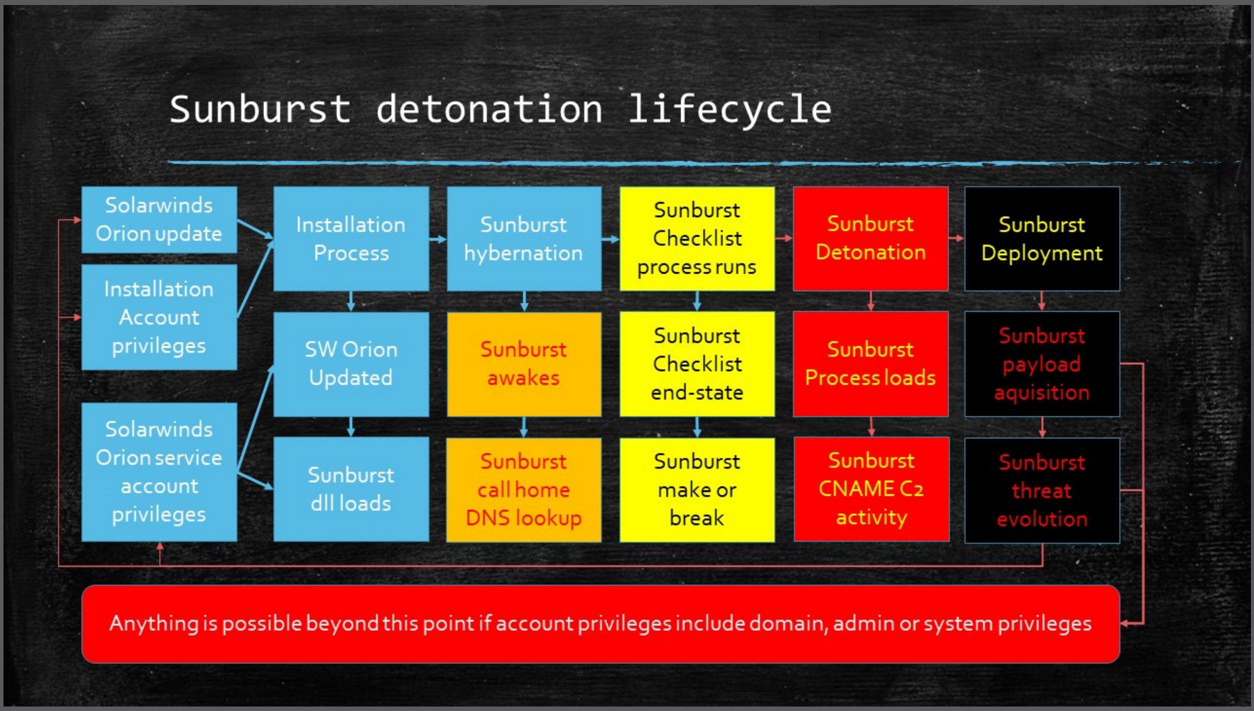
HANDS-ON-KEYBOARD ATTACK
The backdoor runs commands it receives from attackers. The wide range of backdoor capabilities allow attackers to perform additional activities, such as credential theft, progressive privilege escalation, and lateral movement.

Attacker
SolarWinds.Orion.Core.BusinessLayer.dll
solarwinds.businesslayerhost.exe
SolarWinds.Orion.Core.BusinessLayer.dll
Backdoor activates
Backdoor inspects environment
Backdoor gathers info
Initial C2 server
Command-and-control
Backdoor sends gathered info to C2
Second C2 server
Backdoor runs commands from attacker
Attacker starts hands-on-keyboard attack

Microsoft's Solorigate malware infection chain

This is the High Level Overview of the Sunburst Campaign:

- Post Infiltration a file named SolarWinds.Orion.Core.BusinessLayer.dll was inserted into the distribution system and installed as an update from the vendor.
- It then proceeds to lie dormant for for 12+ days before taking action.
- Once active, the backdoor takes steps to ensure its running in enviroments targeted by the attacker. This was done with the sole objective to stay under the radar while carrying out missions.



Sunburst detonation lifecycle

Solarwinds Orion update

Installation Account privileges

Solarwinds Orion service account privileges

Installation Process

SW Orion Updated

Sunburst dll loads

Sunburst hybernation

Sunburst awakes

Sunburst call home DNS lookup

Sunburst Checklist process runs

Sunburst Checklist end-state

Sunburst make or break

Sunburst Detonation

Sunburst Process loads

Sunburst CNAME C2 activity

Sunburst Deployment

Sunburst payload aquisition

Sunburst threat evolution

Anything is possible beyond this point if account privileges include domain, admin or system privileges

Sunburst's Detonation Cycle

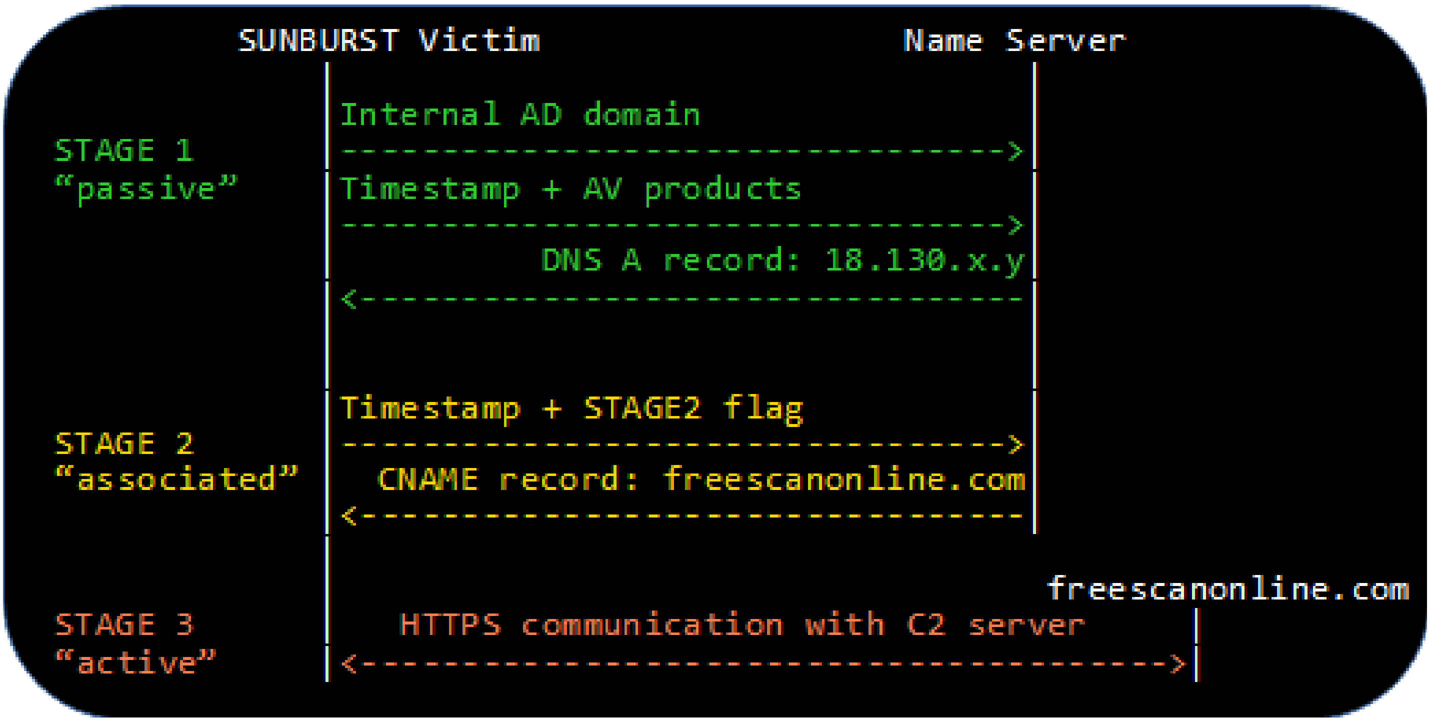
THE LIST OF ORION PRODUCTS AFFECTED IS QUITE COMPREHENSIVE

The list of products that were affected:

- Application Centric Monitor (ACM)
- Database Performance Analyzer Integration Module (DPAIM)
- Enterprise Operations Console (EOC)
- High Availability (HA)
- IP Address Manager (IPAM)
- Log Analyzer (LA)
- NetFlow Traffic Analyzer (NTA)
- Network Automation Manager (NAM)
- Network Configuration Manager (NCM)
- Network Operations Manager (NOM)
- Network Performance Monitor (NPM)
- Server & Application Monitor (SAM)
- Server Configuration Monitor (SCM)
- Storage Resource Monitor (SCM)
- User Device Tracker (UDT)
- Virtualization Manager (VMAN)
- VoIP & Network Quality Manager (VNQM)
- Web Performance Monitor (WPM)

ANALYSIS

- The files in question will be downloaded through trojanized patches dating back to March 2020. Once downloaded, the specific component is a DLL named SolarWinds.Orion.Core.BusinessLayer.dll. The files use the signed using the Certificate: 0f:e9:73:75:20:22:a6:06:ad:f2:a3:6e:34:5d:c0:ed. This DLL was created by modifying the code of a legitimate component of Solar Winds Orion.
- Injecting the code into InventoryManager.cs initiates the Sunburst Backdoor. It actively checks file system timestamps to ensure the product has been deployed for two weeks before it releases its first beacon. Once it becomes active, it will attempt to resolve avsvmcloud[.]com. Once resolved it'll return a CNAME record in order to perform C2 communications.
- It uses a Domain Generation Algorithm to generate specific subdomains for a initial set C2 domain. It will try to communicate with the domain over a random interval, either from 1-3 minutes, 30-120 min and up to 420-540 minutes. The C2 traffic to the malicious domains is designed to mimic normal SolarWinds API communications: Orion Improvement Program (OIP) protocol. The backdoor retrieves and executes commands, that include the ability to transfer files, execute files, profile the system, reboot the machine, and disable system services. FireEye noted that if the malware resolves a domain to a private IP address, it will not execute. Its also noted that the malware will not execute if the machine is not joined to a specific domain or environment.

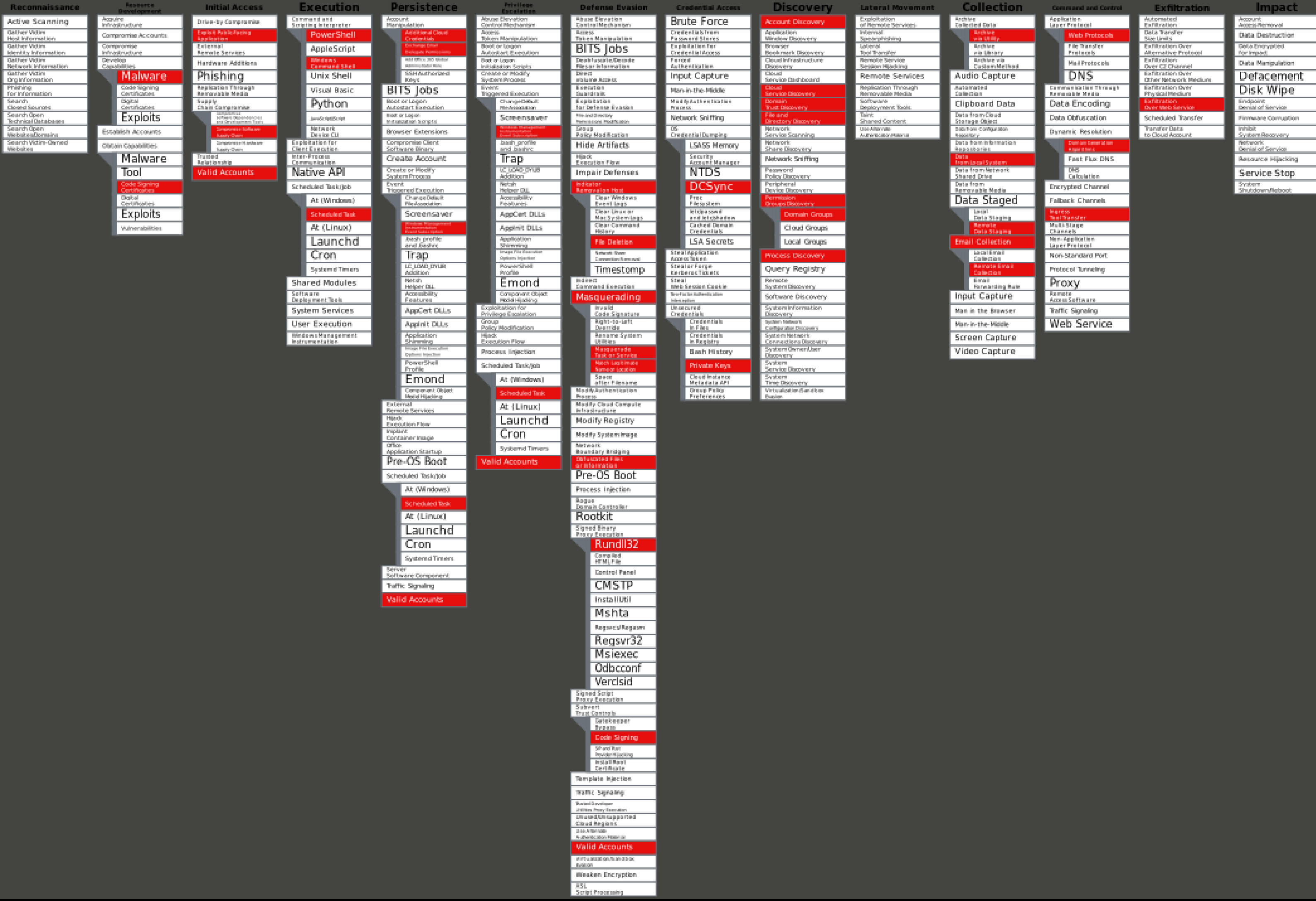


```
          SUNBURST Victim                      Name Server
                    |                                  |
                    |Internal AD domain                |
STAGE 1             |---------------------------------->|
"passive"           |Timestamp + AV products           |
                    |---------------------------------->|
                    |         DNS A record: 18.130.x.y|
                    |<----------------------------------|
                    |                                  |
                    |Timestamp + STAGE2 flag           |
STAGE 2             |---------------------------------->|
"associated"        |  CNAME record: freescanonline.com|
                    |<----------------------------------|
                    |                                       freescanonline.com
STAGE 3             |   HTTPS communication with C2 server     |
"active"            |<---------------------------------------->|
```

Sunburst Backdoor can be shown in 3 stages

Having infected a victim host the threat actor will attempt to deliver additional malware threats:

- **Teardrop**: never-seen-before memory-only dropper which was used to deploy a Cobalt strike beacon. Its file path name was C:\windows\syswow64\netsetupsvc.dll; It spawns a thread and reads from the file “gracious_truth.jpg” ("upbeat_anxiety.jpg" and "festive_computer.jpg" in case of Symantec), which likely has a fake JPG header and relies on Steganography for payload download and execution. Next, it checks that HKU\SOFTWARE\Microsoft\CTF exists, decodes an embedded payload using a custom rolling XOR algorithm, and manually loads into memory an embedded payload using a custom PE-like file format.
- **Supernova**: a .NET C# Web Shell which was specifically written for usage on Solar Winds Orion Servers. Supernova leverages what was a zero-day vulnerability to install a trojanized DLL being app_web_logoimagehandler.ashx.b6031896.dll module. Its original purpose was to return the logo image configured by the user to various web pages of the Solar Winds Orion Web Application. The malicious additions were an extra try/catch block at the beginning of ProcessRequest() method and an extra method called DynamicRun().
- **Cosmicgale**: a malicious PowerShell script that was used for credential theft and reconnaissance. It used the Get-PassHashes routine to collect credentials. It also clears log files, writes data to a hard-coded path, and encrypts the file with a password.



TACTICS, TECHNIQUES AND PROCEDURES

Through MITRE's Blog, we can understand that the threat actor used numerous behaviours that was not currently described in ATT&CK Enterprise or Cloud Techniques.

Very commonly used techniques that were mapped to this Operation are:

- T1012 - Query Registry
- T1027 - Obfuscated Files
- T1057 - Process Discovery
- T1059 - Command and Script Interpreter
- T1105 - Ingress Tool Transfer
- T1218 - Signed Binary Proxy Execution
- T1195 - Supply Chain Compromise

Other behaviours that are not currently captured in existing techniques are:

- T1070 - Indicator Removal on Host
- T1098.002 - Account Manipulation
- T1098.001 - Forge Web Credentials
- T1552.004 - Unsecured Credentials

INDICATORS OF COMPROMISE

SUNBURST DOMAINS

- .appsync-api.eu-west-1[.]avsvmcloud[.]com
- .appsync-api.us-east-1[.]avsvmcloud[.]com
- .appsync-api.us-east-2[.]avsvmcloud[.]com
- .appsync-api.us-west-2[.]avsvmcloud[.]com
- deftsecurity[.]com
- digitalcollege[.]com
- digitalcollege[.]org
- freescanonline[.]com
- globalnetworkissues[.]com
- seobundlekit[.]com
- solartrackingsystem[.]net
- thedoccloud[.]com
- virtualwebdata[.]com
- websitetheme[.]com

BEACON DOMAINS

- databasegalore[.]com
- highdatabase[.]com
- panhardware[.]com
- zupertech[.]com
- lcomputers[.]com
- webcodez[.]com
- kubecloud[.]com
- incomeupdate[.]com

SHA256

SUNBURST

- 019085a76ba7126fff22770d71bd901c325fc68ac55aa743327984e89f4b0134 (Mal/Sunburst-A(SolarWinds.Orion.Core.BusinessLayer.dll))
- 292327e5c94afa352cc5a02ca273df543f2020d0e76368ff96c84f4e90778712 (Mal/Generic-S(OrionImprovementBusinessLayer.2.cs))
- 32519b85c0b422e4656de6e6c41878e95fd95026267daab4215ee59c107d6c77 (Mal/Sunburst-A(SolarWinds.Orion.Core.BusinessLayer.dll))
- 53f8dfc65169ccda021b72a62e0c22a4db7c4077f002fa742717d41b3c40f2c7 (Mal/Generic-S(Solarwinds Worldwide LLC))
- ce77d116a074dab7a22a0fd4f2c1ab475f16eec42e1ded3c0b0aa8211fe858d6 (Mal/Sunburst-A(SolarWinds.Orion.Core.BusinessLayer.dll))
- d0d626deb3f9484e649294a8dfa814c5568f846d5aa02d4cdad5d041a29d5600 (Troj/SunBurst-A(Installer|CORE-2019.4.5220.20574-SolarWinds-Core-v2019.4.5220-Hotfix5.msp))
- a25cadd48d70f6ea0c4a241d99c5241269e6faccb4054e62d16784640f8e53bc (SolarWinds.Orion.Core.BusinessLayer.dll)
- d3c6785e18fba3749fb785bc313cf8346182f532c59172b69adfb31b96a5d0af (SolarWinds.Orion.Core.BusinessLayer.dll)
- ac1b2b89e60707a20e9eb1ca480bc3410ead40643b386d624c5d21b47c02917c
- c09040d35630d75dfef0f804f320f8b3d16a481071076918e9b236a321c1ea77
- dab758bf98d9b36fa057a66cd0284737abf89857b73ca89280267ee7caf62f3b
- eb6fab5a2964c5817fb239a7a5079cabca0a00464fb3e07155f28b0a57a2c0ed

INDICATORS OF COMPROMISE

SHA256

TEARDROP

- b820e8a2057112d0ed73bd7995201dbed79a79e13c79d4bdad81a22f12387e07
- 1817a5bf9c01035bcf8a975c9f1d94b0ce7f6a200339485d8f93859f8f6d730c
- 118189f90da3788362fe85eafa555298423e21ec37f147f3bf88c61d4cd46c51
- 6e4050c6a2d2e5e49606d96dd2922da480f2e0c70082cc7e54449a7dc0d20f8d

SUPERNOVA

- c15abaf51e78ca56c0376522d699c978217bf041a3bd3c71d09193efa5717c71 (Mal/Sunburst-B(app_web_logoimagehandler.ashx.b6031896.dll).SuperNova webshell backdoor)

DLL FILE PATHS

- C:\Program Files (x86)\N-able Technologies\Windows Software Probe\bin\SolarWinds.Orion.Core.BusinessLayer.dll
- C:\Program Files (x86)\Solarwinds\Network Topology Mapper\SolarWinds.Orion.Core.BusinessLayer.dll
- C:\Program Files (x86)\Solarwinds\Network Topology Mapper\Service\SolarWinds.Orion.Core.BusinessLayer.dll
- C:\Program Files (x86)\SolarWinds\Orion\SolarWinds.Orion.Core.BusinessLayer.dll
- C:\Program Files (x86)\SolarWinds\Orion\DPI\SolarWinds.Orion.Core.BusinessLayer.dll
- C:\Program Files (x86)\SolarWinds\Orion\NCM\SolarWinds.Orion.Core.BusinessLayer.dll
- C:\Program Files (x86)\SolarWinds\Orion\Interfaces.Discovery\SolarWinds.Orion.Core.BusinessLayer.dll
- C:\Program Files (x86)\SolarWinds\Orion\DPA\SolarWinds.Orion.Core.BusinessLayer.dll
- C:\Program Files (x86)\SolarWinds\Orion\HardwareHealth\SolarWinds.Orion.Core.BusinessLayer.dll
- C:\Program Files (x86)\SolarWinds\Orion\Interfaces\SolarWinds.Orion.Core.BusinessLayer.dll
- C:\Program Files (x86)\SolarWinds\Orion\NetFlowTrafficAnalysis\SolarWinds.Orion.Core.BusinessLayer.dll
- C:\Program Files (x86)\SolarWinds\Orion\NPM\SolarWinds.Orion.Core.BusinessLayer.dll

INDICATORS OF COMPROMISE

POWERSHELL COMMANDS USED

- Get-AcceptedDomain
- Get-CASMailbox
- Get-Mailbox
- Get-ManagementRoleAssignment
- Get-OrganizationConfig
- Get-OwaVirtualDirectory
- Get-Process
- Get-WebServicesVirtualDirectory
- New-MailboxExportRequest
- Remove-MailboxExportRequest
- Set-CASMailbox

REFERENCES

- https://github.com/fireeye/sunburst_countermeasures
- https://github.com/sophos-cybersecurity/solarwinds-threathunt/blob/master/iocs.csv
- https://medium.com/mitre-attack/identifying-unc2452-related-techniques-9f7b6c7f371
- https://news.sophos.com/en-us/2020/12/21/how-sunburst-malware-does-defense-evasion/
- https://www.microsoft.com/security/blog/2020/12/18/analyzing-solorigate-the-compromised-dll-file-that-started-a-sophisticated-cyberattack-and-how-microsoft-defender-helps-protect/
- https://www.varonis.com/blog/solarwinds-sunburst-backdoor-inside-the-stealthy-apt-campaign/
- https://www.splunk.com/en_us/blog/security/detecting-supernova-malware-solarwinds-continued.html
- https://blog.cyberint.com/solarwinds-supply-chain-attack
- https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html
- https://pastebin.com/6EDgCKxd