GUIDEPOINT SECURITY

SOLARWINDS SUPPLY CHAIN ATTACK:

Indicators of Compromise (IOCs)

Behavioral Indicators

The primary communication mechanisms reported are HTTP with domain name fields matching the domains listed in the FireEye IOCs, and HTTP communications containing XML responses containing control codes embedded in various locations in the XML tree.

SUNBURST SolarWinds Orion Backdoor

The SUNBURST malware communicates over an HTTP C2 channel with callouts delayed by a configurable timeframe. The default value for this delay is one minute between callouts. This communication channel uses a separate set of HTTP methods for requesting data from and sending data to the C2 server. The HTTP GET or HEAD methods are used when the malware is requesting data from the C2 server, and the HTTP PUT or POST methods are used when the malware needs to send data to the C2 server. The malware will use the PUT method to send data when the payload (HTTP body length) is less than 10,000 bytes. Any payloads larger than 10,000 bytes will use the POST method. The payload format being sent to the C2 server for both the PUT and POST requests is JSON containing the following schema:

```
{
        “userid”: value,
        “sessionid”: value,
        “steps”: [
          {
                “Timestamp”: integer,
                “Index”: value,
                “EventType”: “Orion”,
                “EventName”: “EventManager”,
                “DurationMs”: integer,
                “Succeeded”: value,
                “Message”: string
          }
        ]
}
```

Each HTTP Request contains the 'If-None-Match' HTTP header, with a XOR encoded value. Methods of hunting for this activity are as follows:

- Outbound HTTP PUT Requests with Content-Length < 10000 and 'If-None-Match' HTTP Header
- Outbound HTTP POST Requests with Content-Length > 10000 and 'If-None-Match' HTTP Header
- Outbound HTTP PUT or POST Requests with HTTP Request Content-Type Header value of 'application/json'

Analysis conducted by FireEye and Microsoft determined that the SUNBURST backdoor used DNS resolutions of avsvmcloud[.]com as a built in killswitch depending on the IP address returned during the DNS query. FireEye and Microsoft worked together with GoDaddy to take over the malicious domain and modify the IP address returned during DNS resolution to mitigate the effectiveness of the SUNBURST backdoor.

TEARDROP Dropper

During FireEye's analysis of the SolarWinds Supply Chain Compromise, they discovered a previously unobserved dropper that they have dubbed TEARDROP. This dropper has been found to run as a service and is responsible for loading additional executable code into memory with no on-disk presence. Based on details from FireEye, it appears that the TEARDROP dropper is associated with the file "C:\Windows\SYSWOW64\netsetupsvc.dll."

Additionally, FireEye observed TEARDROP's loading process which reads from the file "gracious_truth.jpg," which contains the obfuscated payload, uses a fake JPG file header, and uses a rolling XOR algorithm to decode the payload before executing it in memory. According to FireEye's analysis of TEARDROP, this dropper could load any executable code into memory for execution, but was likely used to execute a customized Cobalt Strike BEACON.

FireEye created YARA signatures that can be used to detect TEARDROP on impacted systems which can be found at: https://github.com/fireeye/sunburst_countermeasures/tree/main/rules/TEARDROP/yara.

GUIDEPOINT SECURITY

SUPERNOVA .NET SolarWinds Service Webshell

GuidePoint recently released a blog regarding the SUPERNOVA .NET webshell backdoor (https://www.guidepointsecurity.com/supernova-solarwinds-net-webshell-analysis/) masquerading as a legitimate SolarWinds web service handler. This .NET module inspects inbound HTTP requests and responds to HTTP requests sent with specific query strings, cookies, or HTML form values. The .NET webshell is located under the filename 'app_web_logoimagehandler.ashx.<8 alphanumeric chars>.dll'. The request will also contain values for the following parameters that are used to compile anonymous code for execution by the webshell:

- codes: This parameter stores compiler codes to be passed to the webshell during compilation
- clazz: The C# Class name to compile as module for execution by the webshell
- method: The C# Class Method to be called within the C# Class listed by the 'clazz' parameter
- args: Newline-delimited list of arguments to pass as parameters to the C# Method listed by the 'method' parameter

The result of the memory execution of this compiled code will be written directly to the HTTP Response body, and the HTTP Response Content-Type Header will have the value of 'text/plain'. Methods to identify this activity are as follows:

- Inbound HTTP GET Requests with:
  - URI file ending with *logoimagehandler.ashx* AND
  - HTTP body parameters of 'codes', 'clazz', 'method', or 'args' AND
  - HTTP Response Status Code of 200, AND
  - HTTP Response Content-Type Header Value of *text/plain*
- Inbound HTTP POST Requests with:
  - URI file ending with *logoimagehandler.ashx AND*
  - HTTP Response Status Code of 200, AND/OR
  - HTTP Response Content-Type Header Value of text/plain

Cobalt Strike BEACON

One method of lateral movement was reported as remote scheduled tasks implementing Cobalt Strike BEACON via %COMSPEC% or PowerShell encoded command executions. For each Cobalt Strike BEACON Scheduled Task, there would be a network communication occurring commensurate with the execution of the Scheduled Task. One method of identifying this activity is to review Scheduled Task execution in the environment, specifically Task Names and their associated binary/command executions. Since these actors have been reported to execute the malicious Task in-between a remove-and-restore cycle of a legitimate Schedule Task, analysts will want to review:

- Any Scheduled Task modifications conducted in rapid succession
- Multiple Scheduled Task executions of the same Task Name with differing binaries/command executions on the same host
- Scheduled Task executions in which there is a network connection outbound to TCP/443 by the Task binary
- Scheduled Task executions with a Command Line value containing '%COMSPEC%', 'cmd', or 'powershell', or with cmd.exe or powershell.exe executions associated with the Scheduled Task execution

Additional behavioral indications of usage of modules present within Cobalt Strike BEACON and reported lateral movement are as follows:

- Windows Service (Event ID 7045) or Scheduled Task (EventID 4698, 4700) creations with 7-character pseudo-random alphanumeric character Service or Task Names
- Windows Services (Event ID 7045) or Scheduled Tasks (EventID 4698, 4700) with Service Filename or Command containing UNC ADMIN$ share path references, beginning with either the loopback IP address or RFC1918 localhost IP address (ex: '\\127.0.0.1\ADMIN$\<7-character>.exe')
- PowerShell (Event ID 400) with the following values:
    - HostName: ConsoleHost
    - HostApplication contains 'rundll32.exe'
    - HostVersion and EngineVersion with different version numbers
        - Ex: HostVersion:1.0 and EngineVersion: 5.1.17763.1
- PowerShell (Event ID 400) with Base64 encoded value in HostApplication field
- Recent changes in NTFS FileName Creation Time for Scheduled Task or at job files located in C:\Windows\System32\Tasks or C:\Windows\Tasks. Each Scheduled Task and at job should be reviewed for any outlying recent NTFS Creation timestamps or unauthorized commands.

GUIDEPOINT SECURITY

Atomic Indicators

Domains

Domain	Association
avsvmcloud[.]com	SUNBURST
databasegalore[.]com	SUNBURST/BEACON
deftsecurity[.]com	SUNBURST
digitalcollege[.]org	SUNBURST
ervsystem[.]com	TEARDROP
freescanonline[.]com	SUNBURST
globalnetworkissues[.]com	SUNBURST
highdatabase[.]com	SUNBURST
incomeupdate[.]com	BEACON
infinitysoftwares[.]com	TEARDROP
kubecloud[.]com	BEACON
lcomputers[.]com	BEACON
mobilnweb[.]com	Unknwn Association
panhardware[.]com	SUNBURST/BEACON
seobundlekit[.]com	SUNBURST
solartrackingsystem[.]net	BEACON
thedoccloud[.]com	SUNBURST
virtualdataserver[.]com	SUNBURST
virtualwebdata[.]com	SUNBURST
webcodez[.]com	BEACON
websitetheme[.]com	SUNBURST
zupertech[.]com	SUNBURST/BEACON

IP Addresses

IP Address	Association
162.223.31[.]184	BEACON
173.237.190[.]2	BEACON
3.87.182[.]149	BEACON
34.219.234[.]134	BEACON
45.141.152[.]18	BEACON
13.57.184[.]217	SUNBURST

GUIDEPOINT SECURITY

13.59.205[.]66	SUNBURST
139.99.115[.]204	SUNBURST
18.220.219[.]143	SUNBURST
18.253.52[.]187	SUNBURST
204.188.205[.]176	SUNBURST
3.16.81[.]254	SUNBURST
34.203.203[.]23	SUNBURST
5.252.177[.]21	SUNBURST
5.252.177[.]25	SUNBURST
51.89.125[.]18	SUNBURST
54.193.127[.]66	SUNBURST
54.215.192[.]52	SUNBURST
107.152.35[.]77	Unknown Association
167.114.213.199	Unknown Association
18.217.225[.]111	Unknown Association
184.72.1[.]3	Unknown Association
184.72.101[.]22	Unknown Association
184.72.113[.]55	Unknown Association
184.72.145[.]34	Unknown Association
184.72.209[.]33	Unknown Association
184.72.21[.]54	Unknown Association
184.72.212[.]52	Unknown Association
184.72.224[.]3	Unknown Association
184.72.229[.]1	Unknown Association
184.72.240[.]3	Unknown Association
184.72.245[.]1	Unknown Association
184.72.48[.]22	Unknown Association
196.203.11[.]89	Unknown Association
198.12.75[.]112	Unknown Association
20.141.48[.]154	Unknown Association
8.18.144[.]11	Unknown Association
8.18.144[.]12	Unknown Association
8.18.144[.]130	Unknown Association
8.18.144[.]135	Unknown Association
8.18.144[.]136	Unknown Association
8.18.144[.]149	Unknown Association
8.18.144[.]156	Unknown Association
8.18.144[.]158	Unknown Association
8.18.144[.]165	Unknown Association

8.18.144[.]170	Unknown Association
8.18.144[.]180	Unknown Association
8.18.144[.]188	Unknown Association
8.18.144[.]20	Unknown Association
8.18.144[.]40	Unknown Association
8.18.144[.]44	Unknown Association
8.18.144[.]62	Unknown Association
8.18.144[.]9	Unknown Association
8.18.145[.]131	Unknown Association
8.18.145[.]134	Unknown Association
8.18.145[.]136	Unknown Association
8.18.145[.]139	Unknown Association
8.18.145[.]150	Unknown Association
8.18.145[.]157	Unknown Association
8.18.145[.]181	Unknown Association
8.18.145[.]21	Unknown Association
8.18.145[.]3	Unknown Association
8.18.145[.]33	Unknown Association
8.18.145[.]36	Unknown Association

File Hashes: SUNBURST

Microsoft published a list of nineteen malicious SolarWinds.Orion.Core.BusinessLayer.dll DLL files spotted in the wild (https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/). We have listed them below with the file version and date first seen.

SHA256	**File Version**	**Date first seen**
e0b9eda35f01c1540134aba9195e7e6393286dde3e001fce36fb661cc346b91d	2020.2.100.11713	February 2020
a58d02465e26bdd3a839fd90e4b317eece431d28cab203bbdde569e11247d9e2	2020.2.100.11784	March 2020

32519b85c0b422e4656de6e6c41878e95fd95026267daab4215ee59c107d6c77	2019.4.5200.9083	March 2020
dab758bf98d9b36fa057a66cd0284737abf89857b73ca89280267ee7caf62f3b	2020.2.100.12219	March 2020
eb6fab5a2964c5817fb239a7a5079cabca0a00464fb3e07155f28b0a57a2c0ed	2020.2.100.11831	March 2020
c09040d35630d75dfef0f804f320f8b3d16a481071076918e9b236a321c1ea77	Not available	March 2020
ffdbdd460420972fd2926a7f460c198523480bc6279dd6cca177230db18748e8	2019.4.5200.9065	March 2020
b8a05cc492f70ffa4adcd446b693d5aa2b71dc4fa2bf5022bf60d7b13884f666	2019.4.5200.9068	March 2020
20e35055113dac104d2bb02d4e7e33413fae0e5a426e0eea0dfd2c1dce692fd9	2019.4.5200.9078	March 2020
0f5d7e6dfdd62c83eb096ba193b5ae394001bac036745495674156ead6557589	2019.4.5200.9078	March 2020
cc082d21b9e880ceb6c96db1c48a0375aaf06a5f444cb0144b70e01dc69048e6	2019.4.5200.9083	March 2020
ac1b2b89e60707a20e9eb1ca480bc3410ead40643b386d624c5d21b47c02917c	2020.4.100.478	April 2020
019085a76ba7126fff22770d71bd901c325fc68ac55aa743327984e89f4b0134	2020.2.5200.12394	April 2020
ce77d116a074dab7a22a0fd4f2c1ab475f16eec42e1ded3c0b0aa8211fe858d6	2020.2.5300.12432	May 2020
2b3445e42d64c85a5475bdbc88a50ba8c013febb53ea97119a11604b7595e53d	2019.4.5200.9078	May 2020
92bd1c3d2a11fc4aba2735d9547bd0261560fb20f36a0e7ca2f2d451f1b62690	2020.4.100.751	May 2020

a3efbc07068606ba1c19a7ef21f4de15d15b41ef680832d7bcba485143668f2d	Not available	Not available
a25cadd48d70f6ea0c4a241d99c5241269e6faccb4054e62d16784640f8e53bc	2019.4.5200.8890	October 2019
d3c6785e18fba3749fb785bc313cf8346182f532c59172b69adfb31b96a5d0af	2019.4.5200.8890	October 2019

File Hashes: SUPERNOVA and TEARDROP

SHA256 Hash	**Association**
c15abaf51e78ca56c0376522d699c978217bf041a3bd3c71d09193efa5717c71	SUPERNOVA
118189f90da3788362fe85eafa555298423e21ec37f147f3bf88c61d4cd46c51	TEARDROP
1817a5bf9c01035bcf8a975c9f1d94b0ce7f6a200339485d8f93859f8f6d730c	TEARDROP

Should you have any questions or would like to discuss, please don't hesitate to contact the GuidePoint Security DFIR team (dfir.team@guidepointsecurity.com).