The SolarWinds Supply-Chain Attack: What You Need to Know

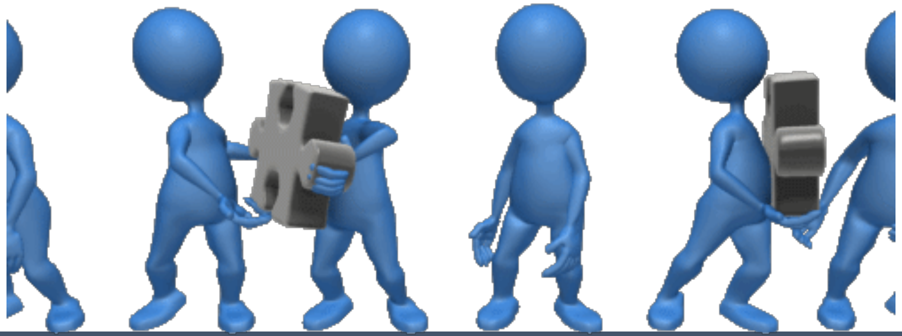
RENDITION INFOSEC
Security by any legal means

Evolving Situation

- As everyone is aware, this is an evolving situation
- More will become known as days progress
- If additional information becomes available that warrants follow-up briefings, those will be announced through SANS communication channels including email and Twitter

It Takes a Village

- Disclaimer: most of what you will hear is not original research
- The SANS instructor team has been working behind the scenes to help with aggregating public information as well as performing their own analysis
- This webcast **<u>would not be possible</u>** without the outstanding work of researchers both in and out of the SANS community sharing information on this rapidly evolving situation



SolarWinds Breach

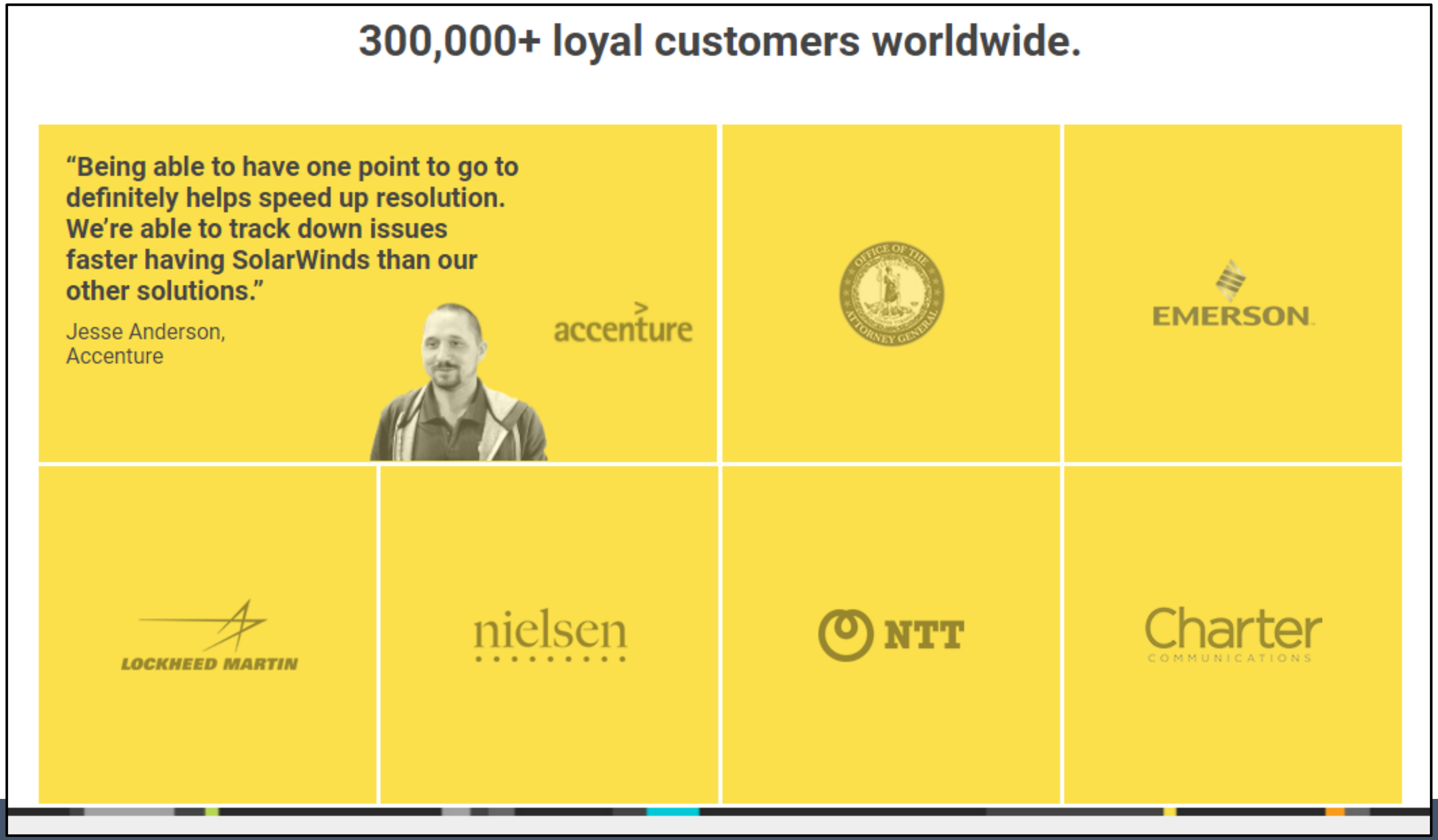
- On December 13, 2020, Chris Bing (Reuters) broke the story that the Treasury Department had been compromised by a sophisticated adversary
- Shortly after, Ellen Nakashima (Washington Post) confirmed with background sources that:
  - The Treasury Department breach was perpetrated by the same group that targeted FireEye
  - SolarWinds was involved in both breaches
  - The threat group was APT29 (Cozy Bear/Russian SVR)

What is SolarWinds?

- SolarWinds is a software company that primarily deals in systems management tools used by IT professionals
- Perhaps the most widely deployed SolarWinds product is Orion, a Network Management System (NMS)
  - Don't confuse Network Management System (NMS) with Network Security Monitor (NSM)
- The Orion NMS has broad capabilities for monitoring and managing systems
  - Including servers, workstations, network devices, etc.

Who Uses SolarWinds?

- Perhaps the better question is "who doesn't use it?"
  - SolarWinds Orion is to NMS what Kleenex™ is to tissues



300,000+ loyal customers worldwide.

"Being able to have one point to go to definitely helps speed up resolution. We're able to track down issues faster having SolarWinds than our other solutions."

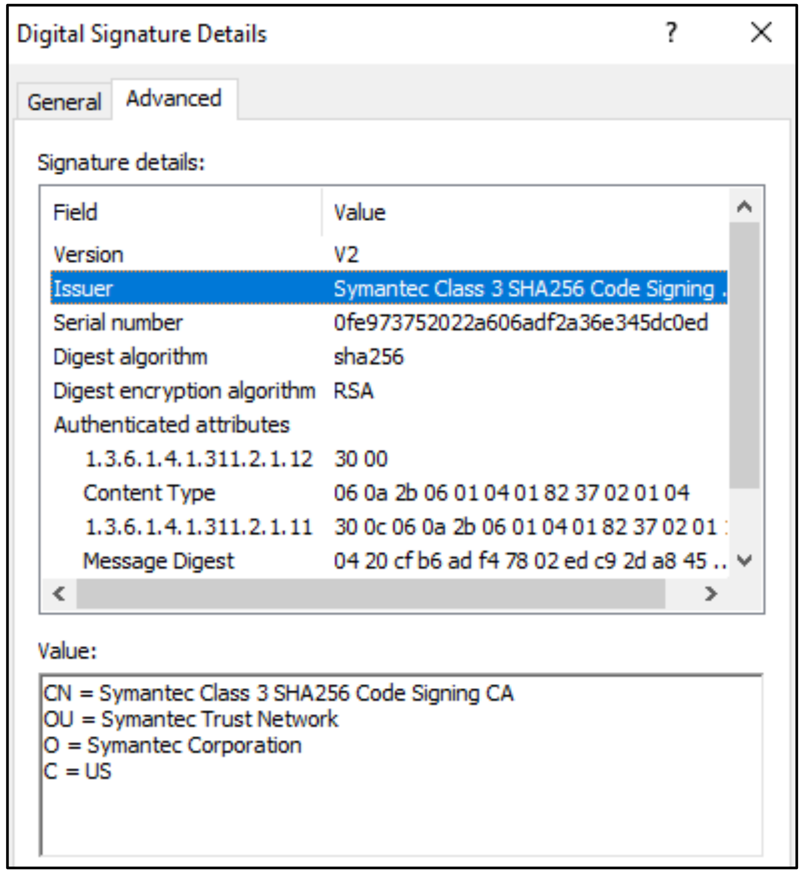
Jesse Anderson, Accenture

More About NMS

- NMS are prime targets for attackers because:
  - NMS must be able to communicate with all devices being managed/monitored, so outbound ACLs are ineffective
  - Many NMS are configured to both monitor for events and respond to them - any changes the NMS can make, the attacker can too
  - Even when NMS are "monitor only" the credentials used still offer some level of access to the attacker (typically read-only)
  - An attacker who compromises an NMS can usually reshape network traffic for MitM opportunities and can often use credentials for system monitoring to laterally move to target systems

How Was The SolarWinds Malware Deployed?

- It is known that the malware was deployed as an update from SolarWinds' own servers and was digitally signed by a valid digital certificate bearing their name
  - This strongly points to a supply chain attack
- The certificate was issued by Symantec
- Serial Number: 0fe973752022a606adf2a36e345dc0ed



Signature details:

Field	Value
Version	V2
Issuer	Symantec Class 3 SHA256 Code Signing .
Serial number	0fe973752022a606adf2a36e345dc0ed
Digest algorithm	sha256
Digest encryption algorithm	RSA
Authenticated attributes	
1.3.6.1.4.1.311.2.1.12	30 00
Content Type	06 0a 2b 06 01 04 01 82 37 02 01 04
1.3.6.1.4.1.311.2.1.11	30 0c 06 0a 2b 06 01 04 01 82 37 02 01
Message Digest	04 20 cf b6 ad f4 78 02 ed c9 2d a8 45 ..

Value:

CN = Symantec Class 3 SHA256 Code Signing CA
OU = Symantec Trust Network
O = Symantec Corporation
C = US

Hashtags to Track

- If you're following information on the breach, here are a few hashtags you can follow for breaking information:
  - #SolarWinds
  - #SolarWindsOrion
  - #UNC2542
- The latter is the designator assigned to the threat group by FireEye, which has very high attribution standards
  - Others have publicly attributed this breach to APT29 (aka Cozy Bear/Russian SVR)
  - Both are probably correct, but FireEye won't attribute to a nation-state without significant evidence

How Was SolarWinds Breached?

- We don't have that information yet
- This is not the first time we've seen state-backed APT targeting software vendors or masquerading as an update to deploy their malware payloads

Russian Attributed:

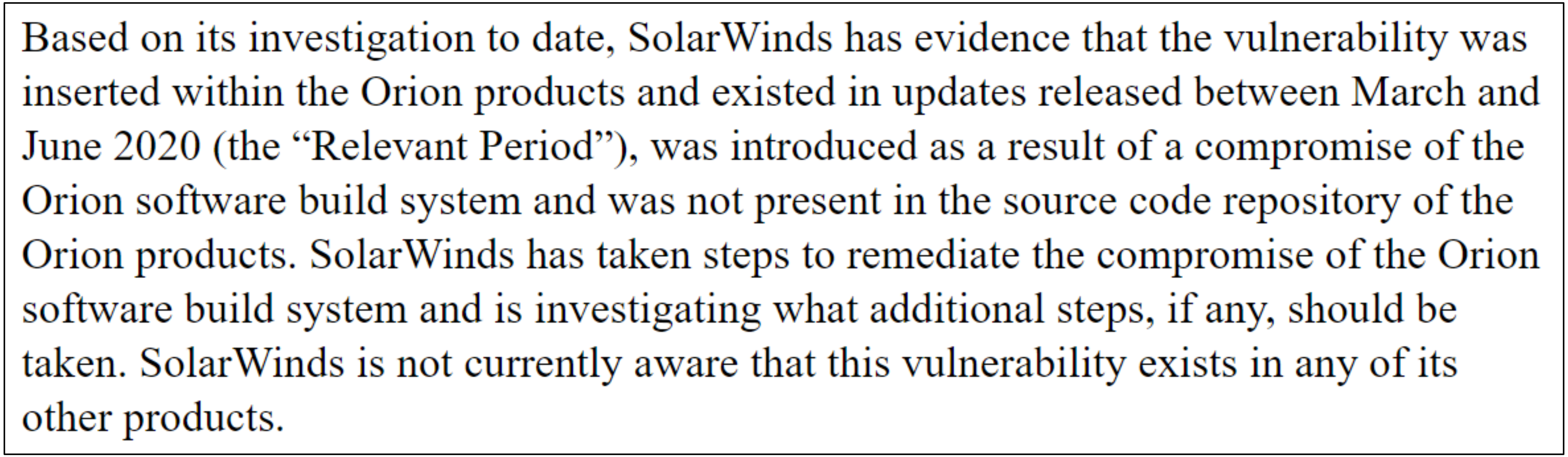
- NotPetya
- BadRabbit (masquerade only)

China Attributed:

- ShadowHammer
- ShadowPad
- Ccleaner

SolarWinds' Response

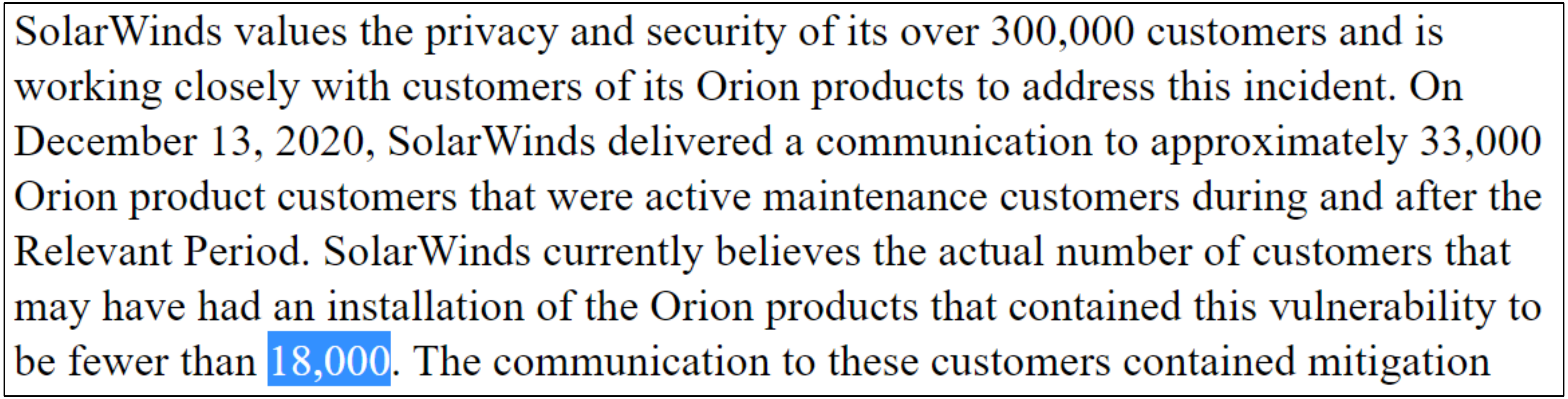
- SolarWinds has published limited information in which they state they believe the build environment was compromised



> Based on its investigation to date, SolarWinds has evidence that the vulnerability was inserted within the Orion products and existed in updates released between March and June 2020 (the “Relevant Period”), was introduced as a result of a compromise of the Orion software build system and was not present in the source code repository of the Orion products. SolarWinds has taken steps to remediate the compromise of the Orion software build system and is investigating what additional steps, if any, should be taken. SolarWinds is not currently aware that this vulnerability exists in any of its other products.

SolarWinds' Response (2)

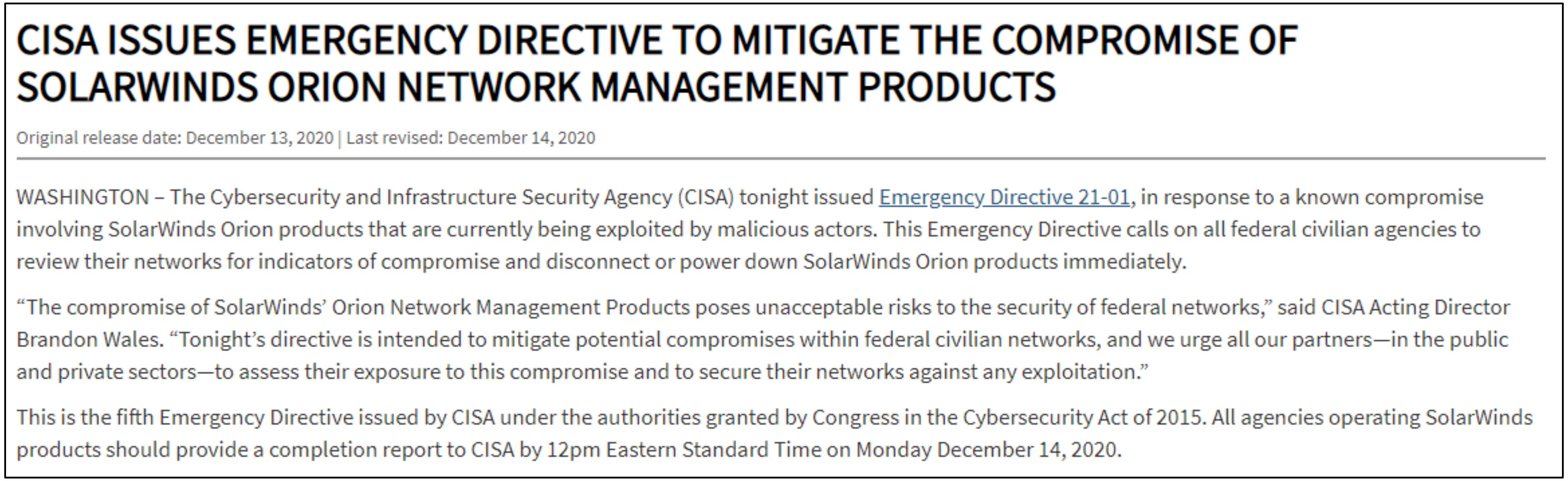
- SolarWinds states that it believes only about 18,000 of its 300,000 Orion customers are impacted by the update



SolarWinds values the privacy and security of its over 300,000 customers and is working closely with customers of its Orion products to address this incident. On December 13, 2020, SolarWinds delivered a communication to approximately 33,000 Orion product customers that were active maintenance customers during and after the Relevant Period. SolarWinds currently believes the actual number of customers that may have had an installation of the Orion products that contained this vulnerability to be fewer than 18,000. The communication to these customers contained mitigation

Because DHS Says So…

- If it's good enough for DHS, it's good enough for you
  - If CISA is directing government agencies to address this problem, you should take it seriously



CISA ISSUES EMERGENCY DIRECTIVE TO MITIGATE THE COMPROMISE OF SOLARWINDS ORION NETWORK MANAGEMENT PRODUCTS

Original release date: December 13, 2020 | Last revised: December 14, 2020

WASHINGTON – The Cybersecurity and Infrastructure Security Agency (CISA) tonight issued Emergency Directive 21-01, in response to a known compromise involving SolarWinds Orion products that are currently being exploited by malicious actors. This Emergency Directive calls on all federal civilian agencies to review their networks for indicators of compromise and disconnect or power down SolarWinds Orion products immediately.

"The compromise of SolarWinds' Orion Network Management Products poses unacceptable risks to the security of federal networks," said CISA Acting Director Brandon Wales. "Tonight's directive is intended to mitigate potential compromises within federal civilian networks, and we urge all our partners—in the public and private sectors—to assess their exposure to this compromise and to secure their networks against any exploitation."

This is the fifth Emergency Directive issued by CISA under the authorities granted by Congress in the Cybersecurity Act of 2015. All agencies operating SolarWinds products should provide a completion report to CISA by 12pm Eastern Standard Time on Monday December 14, 2020.

Network IOCs

- FireEye has released domains useful for hunting (Discovery CoA) if you have DNS logs or full PCAP:

SUNBURST Domains:

- avsvmcloud[.]com
- digitalcollege[.]org
- freescanonline[.]com
- deftsecurity[.]com
- thedoccloud[.]com
- virtualdataserver[.]com

BEACON Domains:

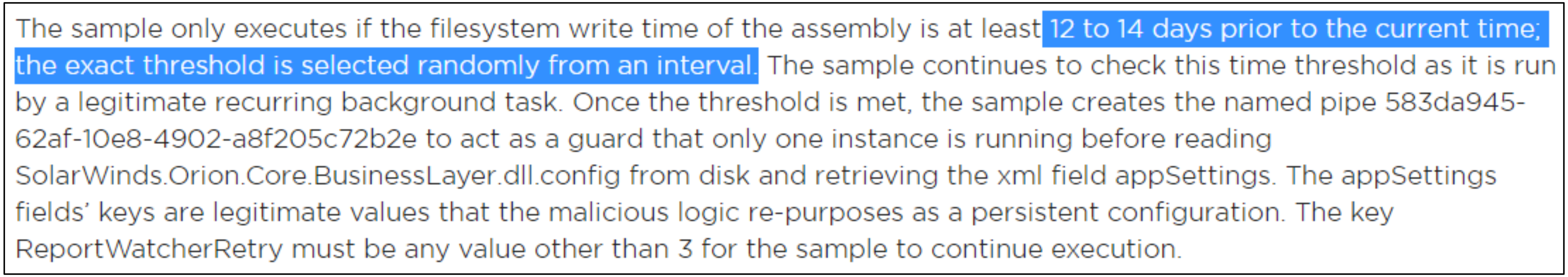
- incomeupdate[.]com
- zupertech[.]com
- databasegalore[.]com
- panhardware[.]com

Attackers Are Sophisticated

- "Sure they are - we hear that with EVERY breach"
- But in this case, the attackers are DEFINITELY sophisticated
- This includes sophistication on behalf of both the development and operational teams
  - Development teams deployed anti-analysis countermeasures
  - Operational teams appear to have used specific infrastructure for each victim, reducing the usefulness of network-based IOCs
- We throw the term APT around a lot, but this definitely is

Delayed Execution

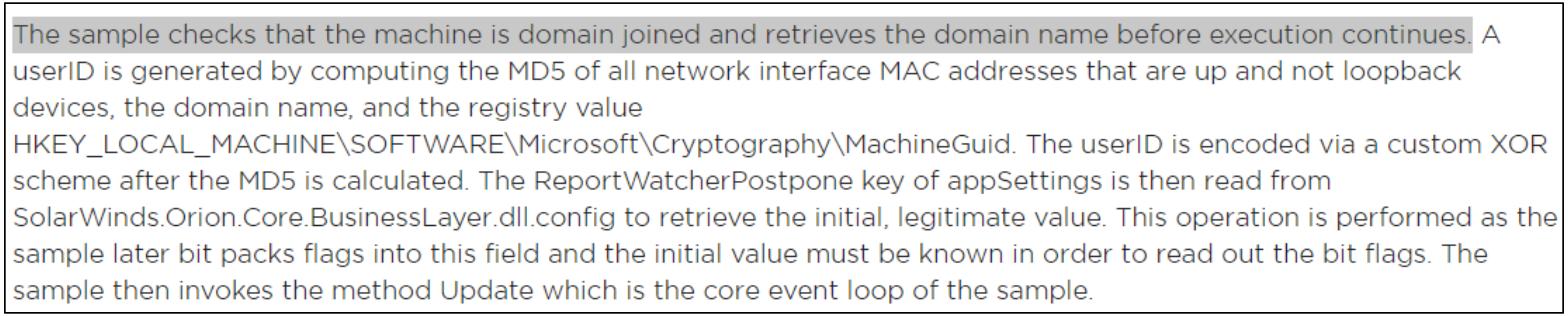
- FireEye notes that the malware checks filesystem timestamps to ensure the product has been deployed 12-14 days
  - This effectively prevents the use of malware sandboxes and other instrumented environments to detect it
    - https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html



The sample only executes if the filesystem write time of the assembly is at least 12 to 14 days prior to the current time; the exact threshold is selected randomly from an interval. The sample continues to check this time threshold as it is run by a legitimate recurring background task. Once the threshold is met, the sample creates the named pipe 583da945-62af-10e8-4902-a8f205c72b2e to act as a guard that only one instance is running before reading SolarWinds.Orion.Core.BusinessLayer.dll.config from disk and retrieving the xml field appSettings. The appSettings fields' keys are legitimate values that the malicious logic re-purposes as a persistent configuration. The key ReportWatcherRetry must be any value other than 3 for the sample to continue execution.

Anti-Sandbox Behavior

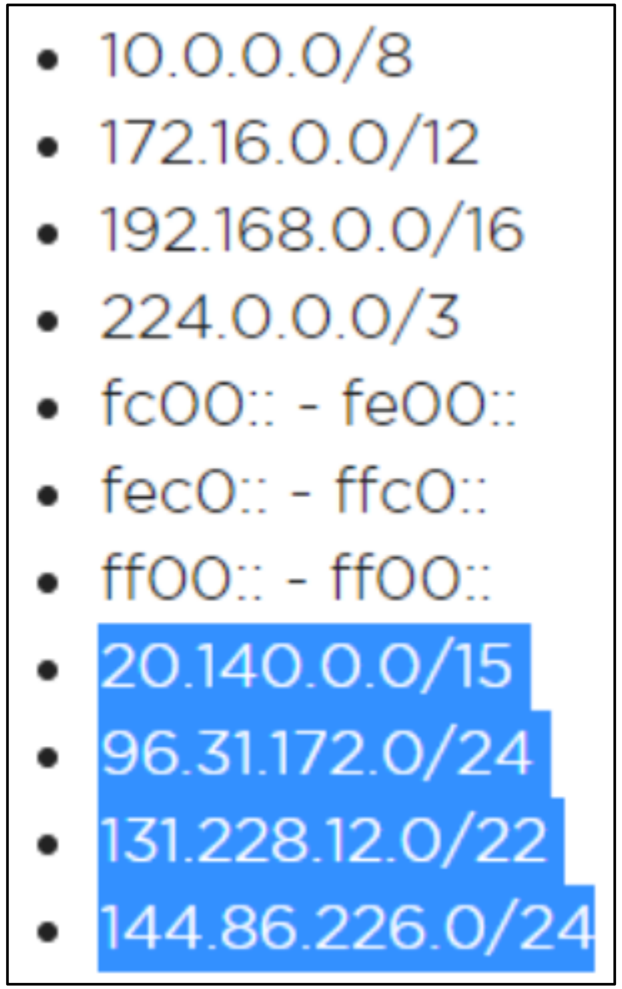
- FireEye notes that unless the machine is joined to a domain, the malware will not execute
  - Are your malware sandboxes (or other instrumented environments) domain joined?
    - https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html



The sample checks that the machine is domain joined and retrieves the domain name before execution continues. A userID is generated by computing the MD5 of all network interface MAC addresses that are up and not loopback devices, the domain name, and the registry value HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MachineGuid. The userID is encoded via a custom XOR scheme after the MD5 is calculated. The ReportWatcherPostpone key of appSettings is then read from SolarWinds.Orion.Core.BusinessLayer.dll.config to retrieve the initial, legitimate value. This operation is performed as the sample later bit packs flags into this field and the initial value must be known in order to read out the bit flags. The sample then invokes the method Update which is the core event loop of the sample.

DNS Resolution and IP Address Checks

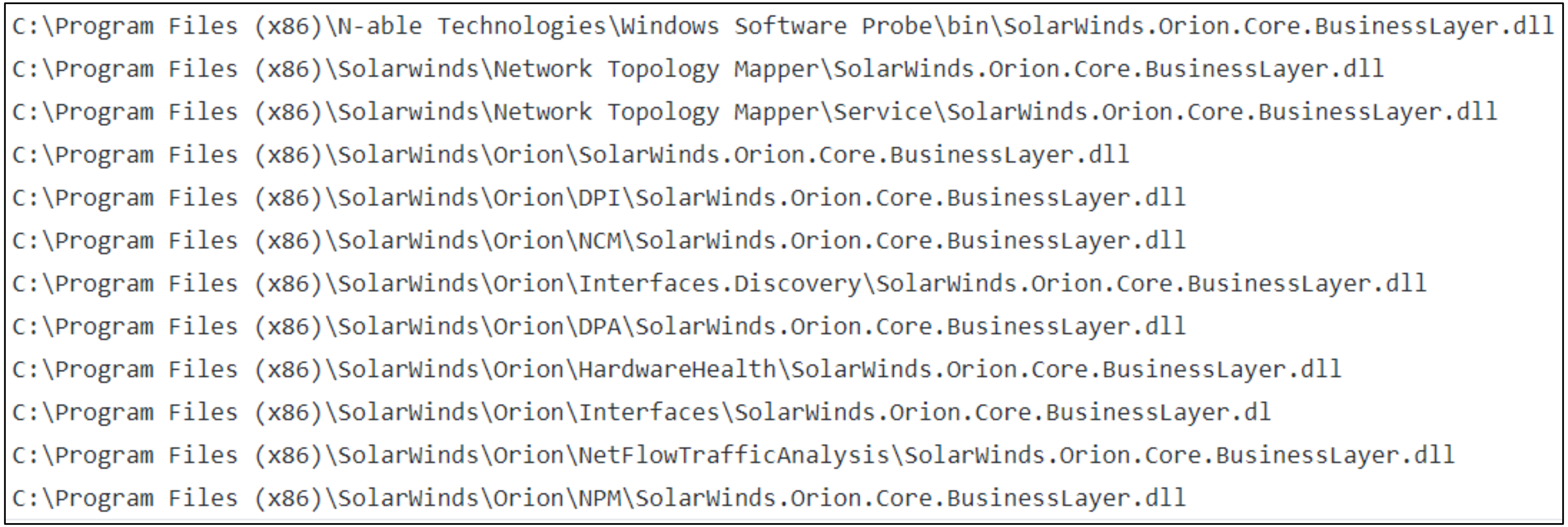
- FireEye notes that if the malware resolves a domain to a private IP address, the malware will not execute
  - Most malware sandboxes intercept DNS and point traffic to themselves for analysis
    - https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html
- Several Microsoft IP addresses are also in the "stop execution list"
  - We're left to guess why, but a huge shout out to @MSFTSecurity in any case, because clearly the adversary doesn't want them doing analysis



- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16
- 224.0.0.0/3
- fc00:: - fe00::
- fec0:: - ffc0::
- ff00:: - ff00::
- 20.140.0.0/15
- 96.31.172.0/24
- 131.228.12.0/22
- 144.86.226.0/24

Known Paths For SolarWinds.Orion.Core.BusinessLayer.dll

- https://gist.github.com/KyleHanslovan/0c8a491104cc55d6e4bd9bff7214a99e
- https://twitter.com/KyleHanslovan/status/1338583792508956672



```
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.dl
C:\Program Files (x86)\SolarWinds\Orion\NetFlowTrafficAnalysis\SolarWinds.Orion.Core.BusinessLayer.dll
C:\Program Files (x86)\SolarWinds\Orion\NPM\SolarWinds.Orion.Core.BusinessLayer.dll
```

Recommendations

- If you have SolarWinds Orion, assume compromise
  - Until more is known, don't assume that it's just the published versions that are compromised
- If you have other SolarWinds products (but not Orion), consider mapping your attack surface in case those were also compromised in the supply chain attack
- Even East/West netflow will be of limited value since the NMS is talking to so many devices in most cases
- Block access from the NMS to the Internet and if it is explicitly needed, limit destinations (think Zero-Trust networking)

Recommendations (2)

- Threat hunt in your network
  - Prioritize the Discovery CoA (looking backwards) over the Detection CoA (looking forward)
- The attacker is **very clearly** OPSEC aware and will likely have changed any filesystem-based IOCs
  - Because the attacker is performing counter-intelligence, IOCs that can be used for the discovery CoA are most useful
- Attackers will be retooling, so don't anticipate finding specifics for SUNBURST malware
  - FireEye noted that this code doesn’t overlap with other malware

Phew, We Don't Have SolarWinds Orion!

- If you're in the (potentially fortunate) situation that you don't use Orion, but you have another NMS, don't rest (yet)
  - Most NMS are configured by Ops, which almost always prioritizes availability in the CIA Triad
- Security teams will threat model the access that a compromise to an NMS will provide, but that's not in Ops' wheelhouse
  - This is no longer theoretical, **threat model it**
- Monitor for intrusions and log, log, log
  - Alert on events and investigate as required

Supply Chain Compromises Will Continue

- Technology predictions don't age well, but I'm confident predicting that supply chain compromises will continue
- Supply chain compromises are extremely difficult to protect against, highlighting the need for security to be considered as part of the vendor selection process
- Note that supply chain security compromises extend to SaaS applications - your SaaS vendor doesn't have any magic process that makes it easier for them to detect these issues

Evolving Situation Reminder

- Reminder: If additional information becomes available that warrants follow-up briefings, those will be announced through SANS communication channels including email and Twitter

Thank You For Attending!

- We're not doing live audience questions due to the number of people who are on this briefing
  - If we have time, a SANS facilitator will moderate questions

Jake Williams

Rendition Infosec (rsec.us)

@MalwareJake