WILMINGTON
UNIVERSITY

Latest Cybersecurity Sobering Stats

- April 15th 2021; US Formally Attributes SolarWinds Attack to Russian Intelligence Agency
- SolarWinds cleanup cost Fortune 500 companies - $100 billion
- Ransomware damage costs to companies will be over $11.5 billion in 2019
- A business will fall victim to an “cyber” attack every 14 seconds
- Biggest attack vector is by phishing email
- 95% of all cyber attacks are financially motivated
- 95% of all successful cyber attacks is cause by human error
- The average time to identify a breach in 2020 was 228 days
- Estimates show there have been as many as 192,000 coronavirus-related cyberattacks per week in May 2020 alone, a 30% increase compared to April

SolarWinds or Sunburst

What Happened?

- In short, an IT management company known as SolarWinds was breached back in March 2020, affecting a massive number of organizations – estimated to be over 20,000
- Commercial organizations include Microsoft, Cisco, and FireEye
- Federal organizations include:
  - U.S. Department of State
  - U.S. Department of the Treasury
  - U.S. Department of Homeland Security
  - U.S. Department of Energy
  - U.S. National Telecommunications and Information Administration
  - National Institutes of Health, of the U.S. Department of Health
  - U.S. National Nuclear Security Administration

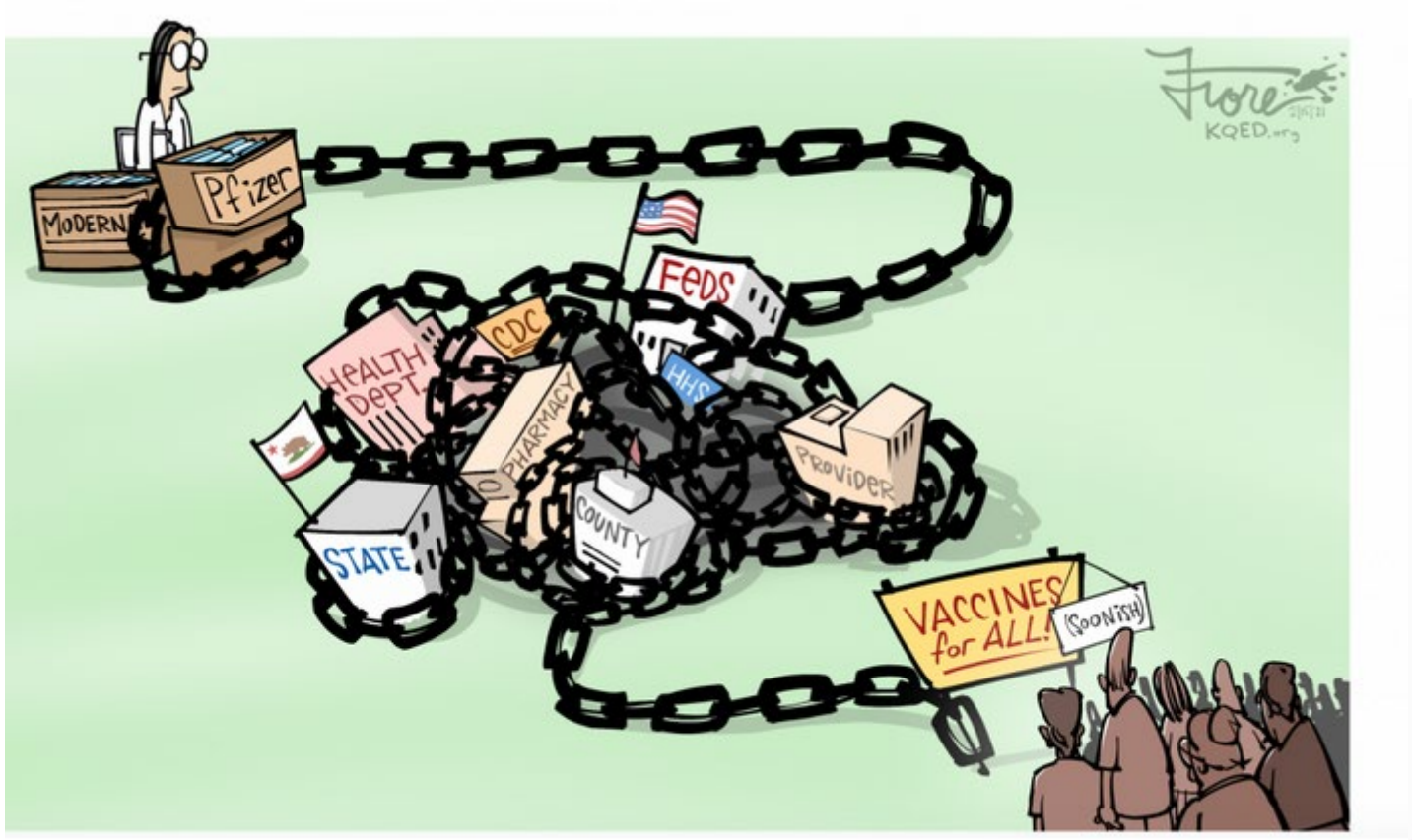
US Government Response

- Public Attribution
  - U.S. Government formally attributed the SolarWinds incident to the Russian SVR and characterized the incident as a “broad-scope cyber espionage campaign.”
- Joint Advisory and Malware Analysis Report
  - NSA-CISA-FBI released an advisory that provides additional information about the SVR’s tradecraft, as well as a CISA Malware Analysis Report (developed in partnership with U.S. Cyber Command)
- A New Red Line for Cyber Espionage
  - The US. Government’s decision to take action against Russia for the SolarWinds compromise (notwithstanding the Intelligence Community’s assessment that it was an espionage campaign)
  - USG pushes for a new norm in cyberspace: that cyber espionage campaigns should not impact thousands of private-sector computer systems, result in millions of dollars in mitigation costs, and trigger concerns about public safety.

SolarWinds Attack/Breach

- On December 13, 2020, Chris Bing (Reuters) broke the story that the US Department of Treasury had been compromised by a sophisticated supply chain attack
- A few days later, Ellen Nakashima (Washington Post) confirmed the following:
  - US Department of Treasury was breached by the same group that targeted FireEye
  - SolarWinds was involved in both breaches
  - The threat group was APT29 (Cozy Bear/Russian SVR)

Supply Chain Attack?



WILMINGTON UNIVERSITY®

Supply Chain Attack?

A supply chain attack is a cyberattack that attempts to inflict damage to a company by exploiting vulnerabilities in its supply chain network. A supply chain attack entails continuous network hacking or infiltration processes to gain access to an organization's network. More than 60% of cyberattacks originate from the supply chain or from external parties exploiting security vulnerabilities within the supply chain.

SolarWinds Discovery

- An employee was alerted of unusual activity and took that alert seriously
- Does your security team know what they are looking out for, and how to proceed if they find something?
- SolarWinds proves the point…

What is SolarWinds?

WILMINGTON UNIVERSITY®

SolarWinds Orion

Leverage Automation to Improve IT Operations

- **Alerts**—leverage intelligent alerting to notify the appropriate staff members and use thresholds to trigger alerts
- **Configuration management**—for networks, back up and standardize configs and automate repetitive tasks during upgrades; for systems, establish baselines and get notified of changes
- **Capacity planning**—monitor system capacity and get notified when trends indicate shortages will occur; get virtualization recommendations based on data from your environment
- **Threat response**—establish conditions for active responses to automatically make changes to deter active cyberthreats

What is SolarWinds?

- SolarWinds is a software company that primarily deals in systems management tools used by IT and Managed Service Providers (MSPs)
- SolarWinds product Orion, is a widely used Network Management System (NMS)
- Network Management System (NMS) is not a Network Security Monitor (NSM)
- The Orion NMS has broad capabilities for monitoring and managing systems - servers, workstations, network devices, etc.
- SolarWinds was estimated to be used on over 70% of large enterprise network operations

SolarWind Attack – When?

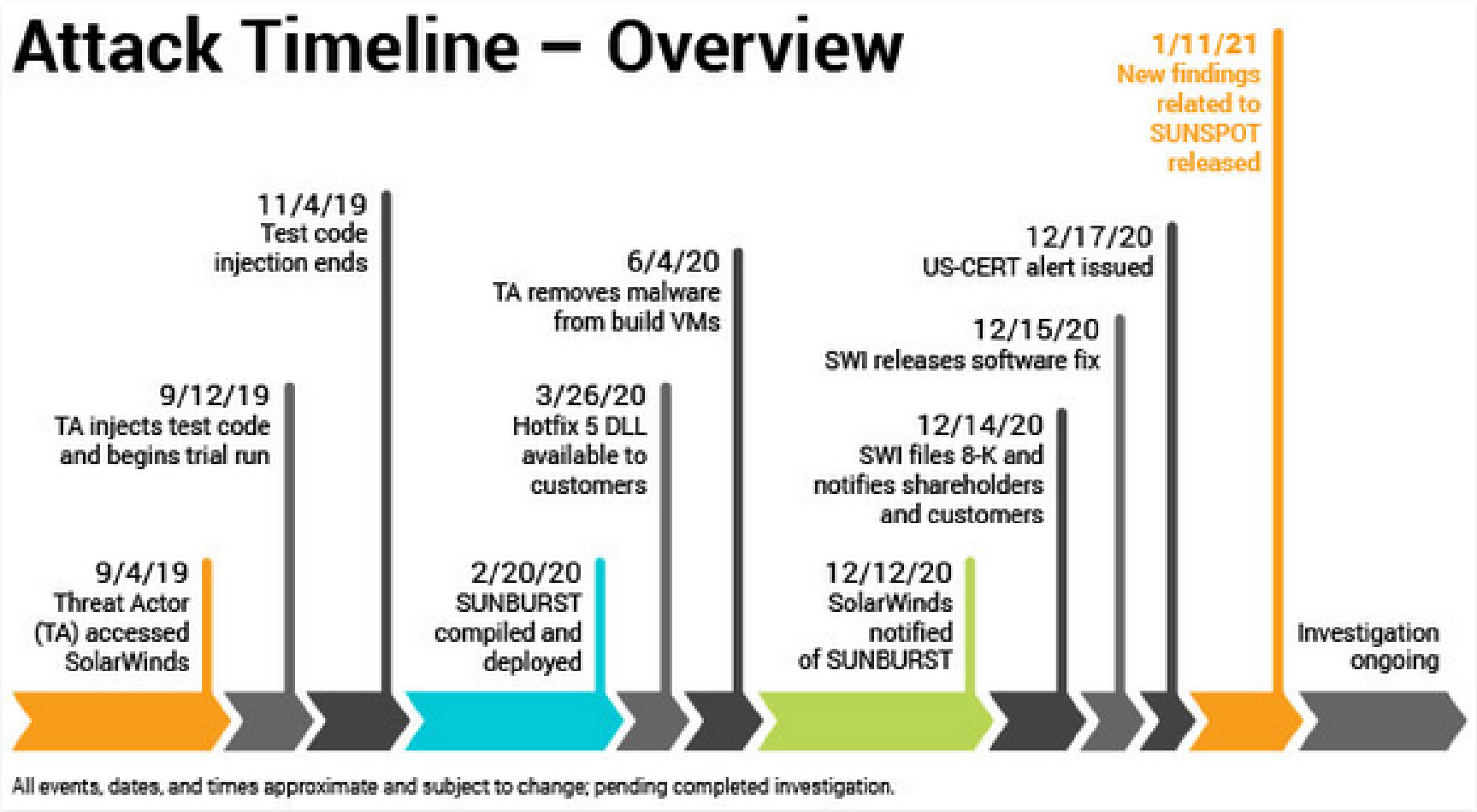


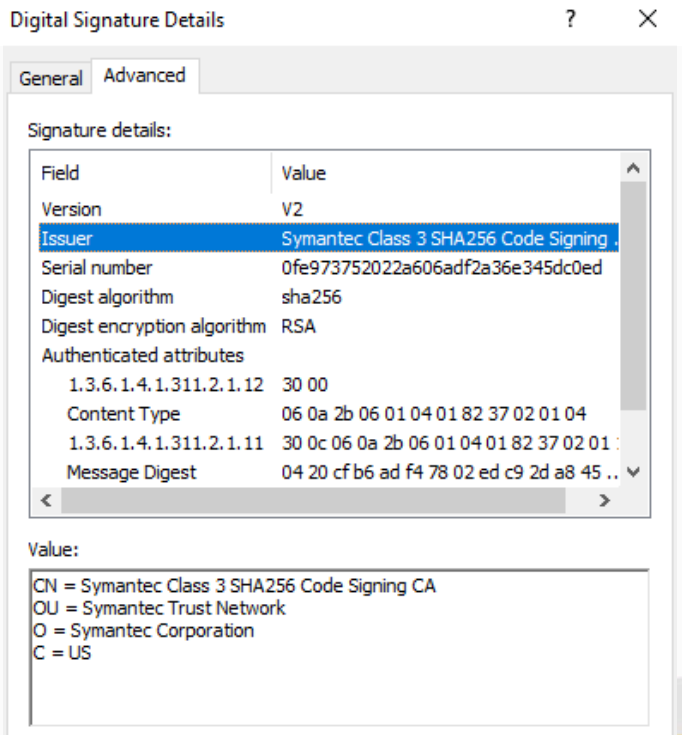
Image: SolarWinds.

Where is SolarWinds?

- Everywhere…..300,000 Organizations Worldwide

How did this happen?

- Embedded Malware was deployed as an update from SolarWinds' own servers and was digitally signed by a valid digital certificate
- Multiple Researcher Firms confirm SolarWinds as a sophisticated supply chain attack



SolarWind Attack/Breach

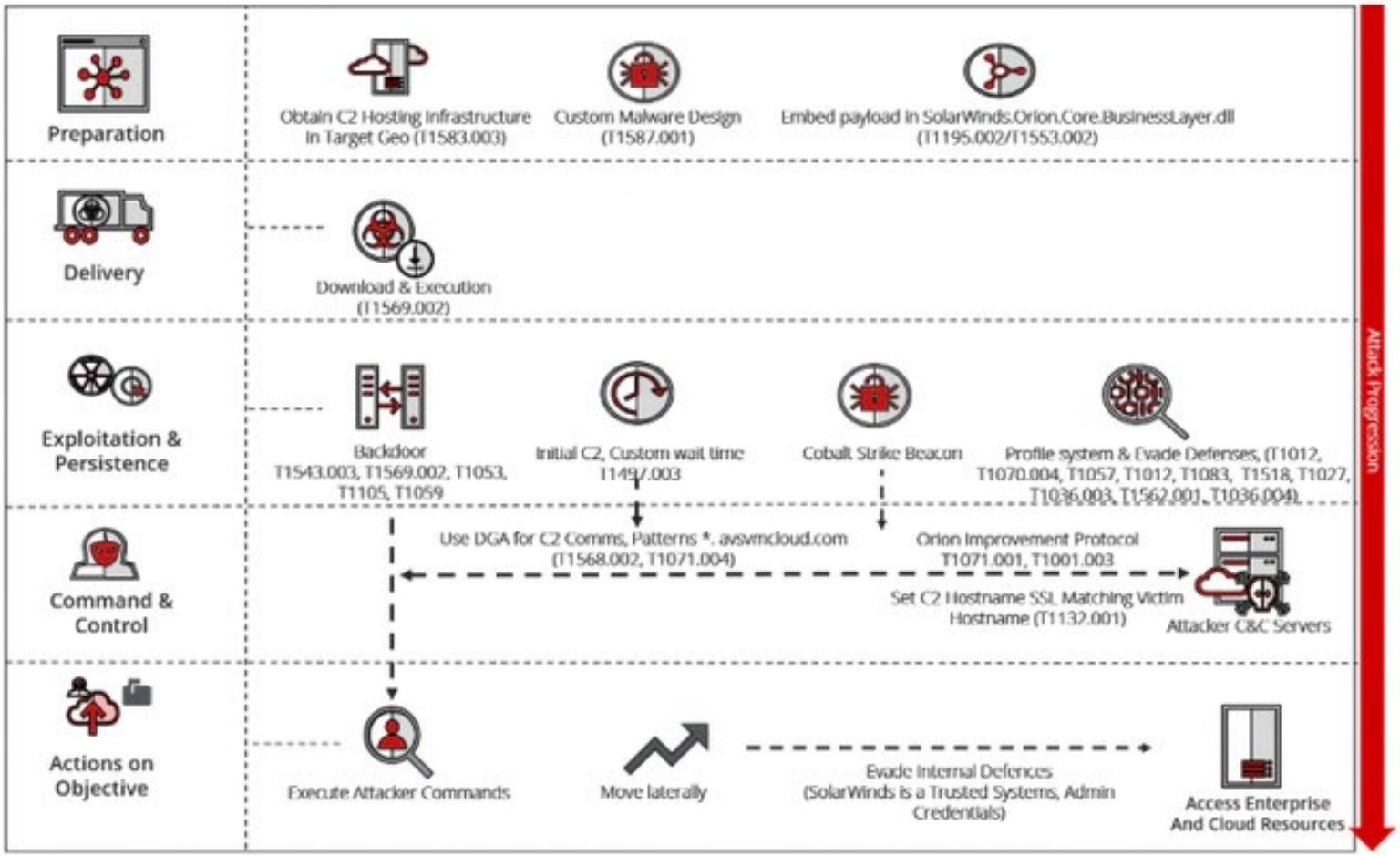


Figure 1: SUNBURST Attack Progression

New Attack? No.

- Nation-state actors have used Advanced Persistent Threat (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

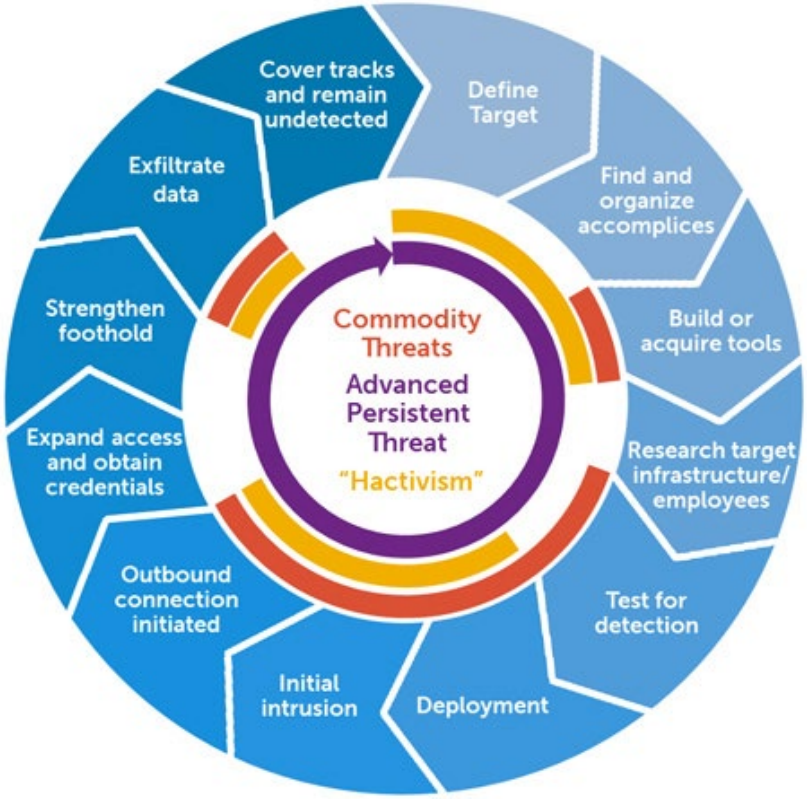
Why is SolarWind different?

Attackers are really Sophisticated….honest!!

- Attack Vectors include:
  - Malware Development and Malware Operational teams
  - Understanding of how and who was using the software
  - Development teams deployed anti-analysis countermeasures to limit discovery
  - Operational teams appear to have used specific infrastructure tailored for each victim, reducing the usefulness of network-based IOCs
- APT is used to describe this attack….

Advanced Persistent Threats (APT)

- An advanced persistent threat (APT) is a stealthy threat actor, typically a nation state, state-sponsored group, or organized crime which gains unauthorized access to a computer network and remains undetected for an extended period.
- Such threat actors' motivations are typically political or economic with no fear of prosecution.



Why is SolarWind so different?

- In one word – sophisticated
- Network IOCs
  - FireEye has released domains useful for hunting (DiscoveryCoA) 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

Why is SolarWind so different?

- Delayed Execution - FireEye notes that the malware checks file system timestamps to ensure the product has been deployed 12-14 days
- Why? Effectively prevents the use of malware sandboxes and other instrumented environments to detect it

https://www.fireeye.com/blog/threatresearch/2020/12/evasive-attackerleverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

Why is SolarWind so different?

- 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-attackerleverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

Why is SolarWind so different?

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
- Several Microsoft IP addresses are also in the "stop execution list"

https://www.fireeye.com/blog/threatresearch/2020/12/evasive-attacker-leverages-solarwindssupply-chain-compromises-with-sunburst-backdoor.html

Why is SolarWind so different?

- Hunting for APT – Good Luck!!
- Known Paths For SolarWinds.Orion.Core.BusinessLayer.dll

```
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
```

What Now?

- If you have SolarWinds Orion, assume compromise and ensure the latest release of software is deployed
- 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
- Consider/Evaluate the number of devices your NMS touches/manages
  - 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)

What Now?

Threat hunt in your network…

- Prioritize the Discovery CoA (looking backwards) over the Detection CoA (looking forward)
- This attack 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
- Anticipate the Attackers will be retooling, so don't anticipate finding specifics for SUNBURST malware
- FireEye noted that this code doesn’t overlap with any other malware

Not Impacted

- We Don't Have SolarWinds Orion – we are good right?
- Could your current NMS be a target? Probably...
- Why worry?
  - Most NMS are configured by Ops, which almost always prioritizes **availability** in the CIA Triad
  - Most Security teams will evaluate threats on entry not after “in production” – that’s an Ops job….a compromised NMS would potentially go undetected
  - This is no longer theoretical threat – it is real…
- Monitor for intrusions and log, log, log
- Alert on events and investigate as required

Supply Chain Compromise

- Supply chain compromises will continue and evolve over time – with more sophistication – yikes!
- Supply chain compromises are extremely difficult to protect against, highlighting the need for security to be considered as part of the vendor selection process
- Supply chain security compromises extend to SaaS applications - your CSP/SaaS vendor doesn't have a magic detection button
- Technology predictions are not very good over time - but you can bet that supply chain compromises will be

QUESTIONS?

WILMINGTON UNIVERSITY®