



## THE SOLARWINDS COMPROMISE AND ICS/OT NETWORKS

# HOUSEKEEPING

- Webinar is being recorded
- Phones are muted
- Please submit questions using the Q&A tool

# OUR PRESENTERS



**Sergio Caltagirone**  
Vice President  
Threat Intelligence



**Ben Miller**  
Vice President  
Professional Services  
and R&D



**Kai Thomsen**  
Director  
Global Response









# AGENDA

- What we know
- What we don't know, What we recommend
- What these environments looks like
- Assessing and hunting recommendations
- Q&A

# WHAT WE KNOW

- SolarWinds is used by both vendors and asset owners in industrial environments / critical infrastructure
- We know of compromised versions of SolarWinds within customer industrial environments in critical infrastructure sectors
- Most do not have the visibility to know if the adversary conducted operations in their environment

# WHAT IS SOLARWINDS?

AVAILABILITY & PERFORMANCE	APPLICATION & INFRASTRUCTURE	DATABASE PERFORMANCE	SERVICE & ASSET MANAGEMENT
 Network Performance Monitor <ul style="list-style-type: none"><li>• Multi-vendor network monitoring for fault, performance, and availability</li><li>• Automated capacity forecasting, alerting, and reporting</li></ul> <a href="#">Learn More</a>	 Server & Application Monitor <ul style="list-style-type: none"><li>• Deep performance visibility of commercial and custom applications</li><li>• Monitor across private, public and hybrid cloud environments</li></ul> <a href="#">Learn More</a>	 Database Performance Analyzer <ul style="list-style-type: none"><li>• Find, analyze, and optimize your database performance story</li><li>• Multi-vendor support across physical, virtual, or cloud deployments</li></ul> <a href="#">Learn More</a>	 Service Desk <ul style="list-style-type: none"><li>• ITSM platform that includes incident, problem, change and request management</li><li>• Fully integrated ITAM provides ability to discover, map and manage software and hardware assets</li></ul> <a href="#">Learn More</a>
BANDWIDTH & TRAFFIC PATTERNS	STORAGE PERFORMANCE & CAPACITY	CONFIGURATION & CHANGE MANAGEMENT	SECURITY & COMPLIANCE
 Network Bandwidth Analyzer Pack <ul style="list-style-type: none"><li>• Customizable network traffic reports</li><li>• Multi-vendor device and flow support</li></ul> <a href="#">Learn More</a>	 Storage Resource Monitor <ul style="list-style-type: none"><li>• Unified storage monitoring across different storage vendors and devices</li><li>• Pinpoint storage performance bottlenecks</li></ul> <a href="#">Learn More</a>	 Network Configuration Manager <ul style="list-style-type: none"><li>• Multi-vendor network change and configuration management</li><li>• Real-time configuration change notification</li></ul> <a href="#">Learn More</a>	 Security Event Manager <ul style="list-style-type: none"><li>• Normalize log data to quickly spot security incidents</li><li>• Out of the box rules and reports help make it easy to meet compliance requirements</li></ul> <a href="#">Learn More</a>

# WHAT HAPPENED TO SOLARWINDS?

- Sometime in 2019 (best knowledge) an adversary compromised SolarWinds and their code base was accessed to add malicious code
- Because the malicious code was signed (and therefore given permissions to execute) we know the compromise happened early in the software development lifecycle

# WHAT HAPPENED TO SOLARWINDS CUSTOMERS?

- Current evidence suggests first customer compromise infrastructure went live early 2020
- ~18k SolarWinds customers ran a compromised version of Orion
- Of those, some experienced a follow-on operation by an unknown adversary
- Microsoft identified critical credential attacks which bypassed multifactor authentication and leading to long-term access
- Current estimates: hundreds of accessed environments, we know current public estimates are undercounting based on the number of privately known victims
- Other evidence suggests a second adversary was using SolarWinds to conduct another attack of SolarWinds customers through a DLL side-loading attack



# ACCESS VS EFFECTS OPERATIONS

- Access Operations: Gain Access
- Effects Operations: Do Something
- Long-term and large-scale supply chain access is an objective for many offensive cyber teams. They want the flexibility to choose when and how to use that access later.

The Complex World of Offensive ICS Operations: <https://www.dragos.com/blog/industry-news/the-complex-world-of-offensive-ics-operations/>

# SOLARWINDS ICS THREAT PERSPECTIVE

- Industrial environments have been compromised by malicious SolarWinds code – some ICS sectors include electric, oil and gas, water, mining, and manufacturing
- SolarWinds is a critical part of many IT operations, almost akin to Microsoft in its depth
- In ICS, because of the risk and potential disruptive or destructive impact of such deep and long-term access we cannot assume away the problem as “espionage”

## Supply Chain Issues

- SolarWinds is not unique – there are hundreds of companies like them
- XENOTIME is an ICS threat group actively compromising vendors and OEMs likely to conduct similar attacks
- MeDoc/NotPetya was a similar style of attack and showcases how these software supply chain vendors and customers are going to face increasing pressure

# ASSUME COMPROMISE

While Dragos is aware of compromised Solarwinds installations in industrial networks, we are currently not aware of a known breach (adversary access) in an industrial environment.

BUT

**Customers are lacking the logging and visibility to prove it**

# WHAT WE DON'T KNOW

- The extend of the supply chain compromise
- What was accessed in the environments
- The extent of tools and tactics used by adversary

# WHAT WE RECOMMEND

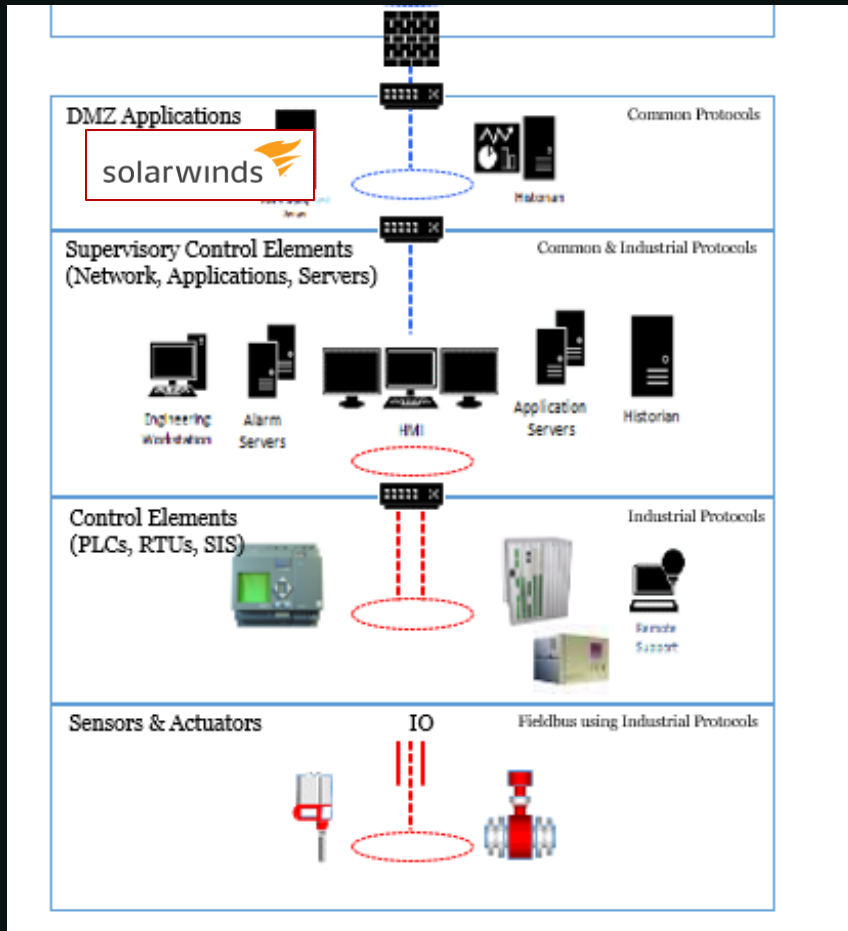
## IF YOU HAVE VISIBILITY

- Focus on critical sites
- Identify solarwinds versions
- Identify exfiltration, lateral movement attempts
- Network and Host data

## IF YOU LACK VISIBILITY

- Assume compromise.
- Identify solarwinds versions but you won't be able to identify adversary activity
- Assess and hunt
- Focus on present and future state
- Gain visibility of east-west network traffic

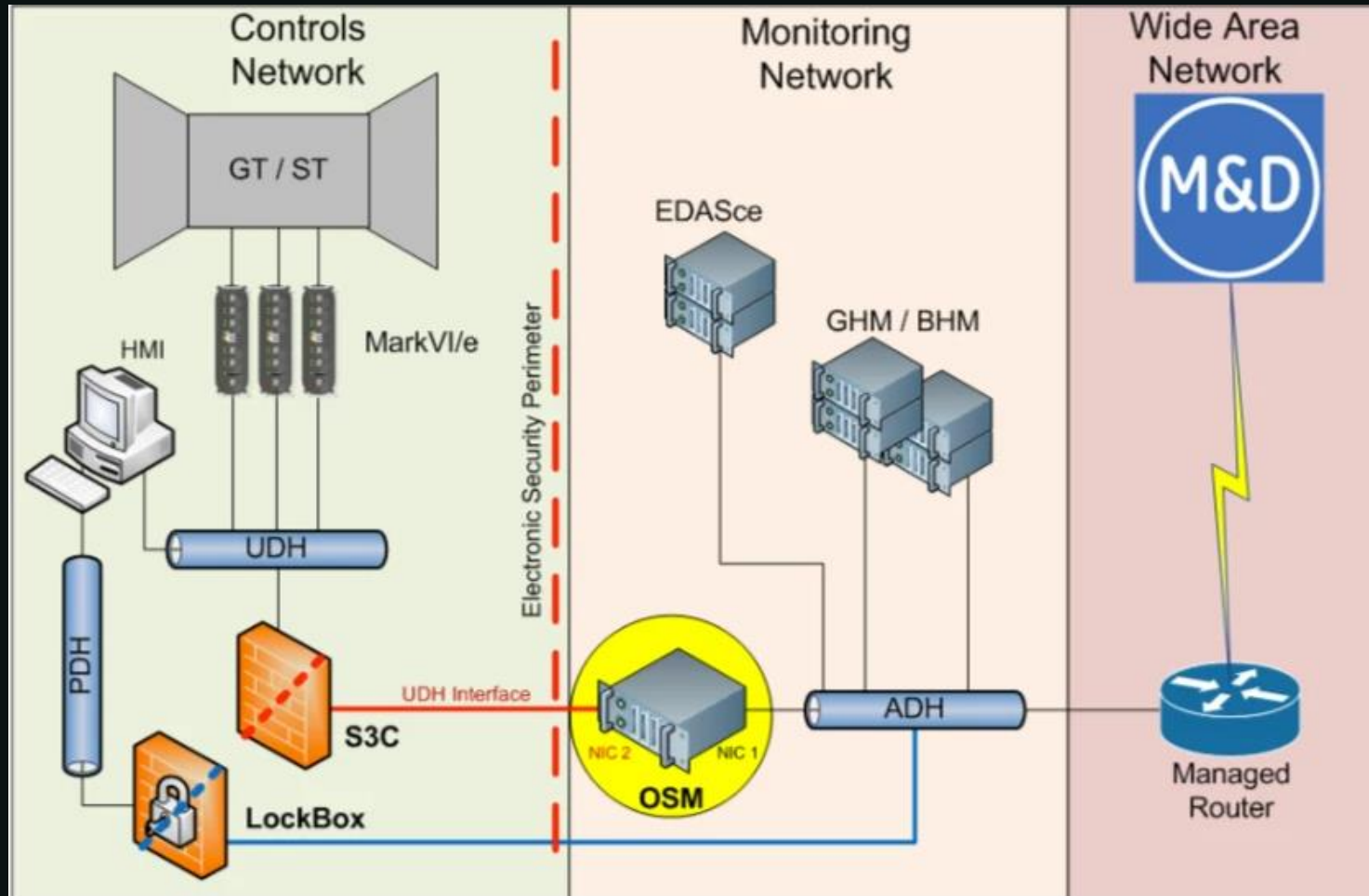
# A WELL ARCHITECTED SOLARWINDS



Takeaway:  
DMZ placement doesn't  
mean "solved"

SolarWinds is designed  
to monitor systems and  
hosts down to level 2  
and level 1. The  
compromised host has  
unfettered access.

# MAINTENANCE AND DIAGNOSTICS (EXAMPLE)



- Direct connections with vendors are common.
- The services are 'black box' and often owned and maintained by the vendor.
- Dragos Platform has seen vendor networks do unusual things (powershell, scanning and enumeration), work outside of maintenance windows

# IF YOU HAVE NETWORK VISIBILITY

- In General
  - East-West network traffic (e.g. Netflow/IPFIX) that can be used to track internal network communication and access to hosts
  - DNS Logs
  - Firewall Logs
  - Web Proxy Logs



# HUNTING FOR SUNBURST – DNS LOGS

- Look for DNS queries that look like this:

```
Dec 18 15:55:01 192.168.1.200 named[8094]: client  
192.168.1.50#64521 (if6a8eaoj4f1ugjw00esqiimln84vp.appsinc-  
api.eu-west-1.avsvmcloud.com): query:
```

- Breakdown of domain

- If6a8eaoj4f1ugjw00esqiimln84vp: randomly generated, based on data from the host
- appsync-api: constant
- eu-west-1: can be one of (eu-west-1, us-west-2, us-east-1, us-east-2)
- avsvmcloud.com

- More details here:

<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/>

- All hosts trying to connect to C2 servers are eligible for forensic data collection!

# IF YOU DON'T HAVE NETWORK VISIBILITY

- Logs
  - Antivirus / endpoint protection logs
  - All Windows logs - PowerShell usage logs
- On Hosts with a compromised Solar Winds Orion
  - Memory Dump
  - Full Disk Image
- In an ICS Environment Deemed Compromised without Continuous Network Security Monitoring
  - Memory Dump on all Windows hosts
  - Collect all event logs (.evt and .evtx), registry hives, and Master File Table

# TIMELY ANALYSIS – SOLAR WINDS SERVER



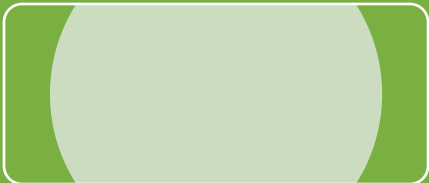
Verify compromised SUNBURST SolarWinds.Orion.Core.BusinessLayer.dll with Yara. You can get effective Yara rules from FireEye at [https://github.com/fireeye/sunburst\\_countermeasures](https://github.com/fireeye/sunburst_countermeasures)



Identify any potentially malicious processes via Memory Analysis



List all accounts registered on the system. These need all marked as compromised, especially if domain accounts or passwords reused for local accounts on other systems



Identify any unusual connections from Solar Winds Orion server to other systems, especially via command line and PowerShell

# HUNTING FOR COMPROMISED HOSTS

- From ALL hosts in your ICS environment, collect
  - Memory Dump
  - Windows event logs (.evt and .evtx files)
  - Registry hives
- Analyze for
  - Unusual connections to other systems
  - Connections from Solar Winds server(s). Take note of accounts!
  - Unknown/suspicious processes in memory
  - Unusual usage of command line and PowerShell commands

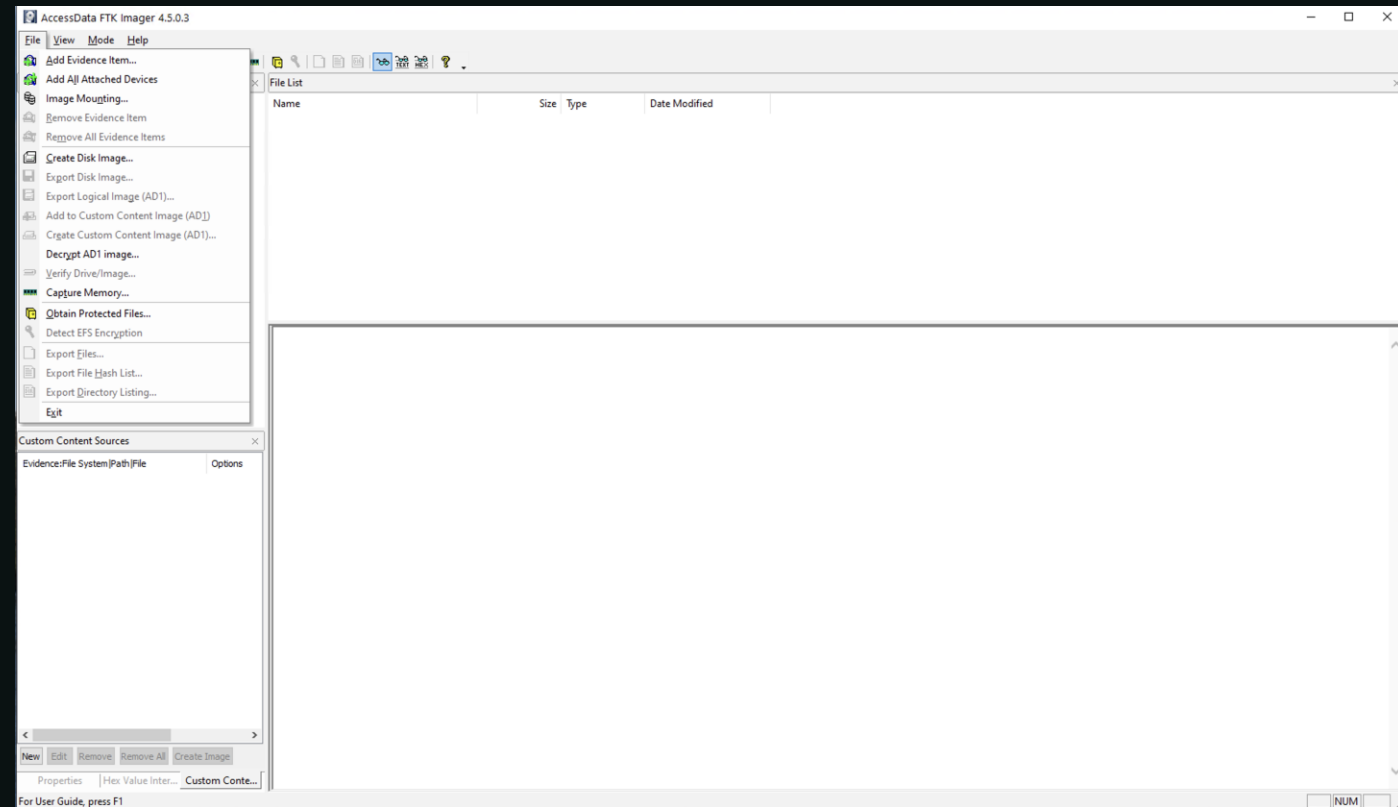
# DFIR CAVEAT

- If you have not done Digital Forensics and Incident Response (DFIR) before, get help
- At present, there aren't any tactics, techniques, and procedures known about this adversary that can be simply hunted for by novice analysts
- Focus on collecting the right data and get help from experienced incident responders
- Consider training internal staff in incident response basics. This won't be your last incident.

# FORENSIC COLLECTION 101 - PHYSICAL HOST

## USE A SIMPLE TOOL LIKE FTK IMAGER

- Perform “Capture Memory” and “Obtain Protected Files” as a minimum
- “Create Disk Image” if there is time
- Link to FTK Imager:  
<https://accessdata.com/product-download/ftk-imager-version-4-5>
- Collect all data onto an external USB drive



# FORENSIC COLLECTION 101 – VIRTUAL HOST

- For any VMWare product
  - Pause the VM, if deemed safe by IT Operations
  - For memory collection, identify any files with the extension “.vmss” and “.vmem” and copy these to your collection drive
  - For full disk image collection, copy all files with the “.vmdk” extension to your collection drive
- For other VMMs (Hyper-V, VirtualBox, etc.)
  - Use methods for physical collection described in previous slide

## CONSIDERATIONS WHEN DOING ASSESSMENTS ACROSS ONE OR MORE FACILITY

- Make sure you assess all networks to include backup, failover, and test networks
- Understand what third-party networks exist. Some OEMs, support vendors, or maintenance and diagnostic services are known to use SolarWinds
- Treat your corporate network as a third-party network. Particularly, if you own critical infrastructure and have a compromised SolarWinds installation you will want to disprove not only if there was a breach on the corporate network but that it did not extend into your industrial environment or focus on exfiltration of critical infrastructure data, plans, schematics, security posture, etc.



# NERC CIP CONSIDERATIONS

- **CIP-013** became mandatory and enforceable in October 2020
  - New contracts require provisions for vendor incident notifications, remote access, and additional procurement language **Each utility should ask their vendors if they use SolarWinds Orion**
- **CIP-005** - auditors may ask utilities regarding malicious communications potentially identified and the tools used, as well as **how the hotfixes and patches were installed (or other mitigation plans approved)** where BES Cyber Systems using SolarWinds Orion products were identified
- **CIP-008-5** and IR requirements - a potential investigation for SolarWinds Orion in a NERC CIP regulated BES Cyber System could become a “Cyber Security Incident.” That said, unless it impacted the Reliability Task of the BES CS, it would not be a “Reportable Cyber Security Incident”
  - Starting in January 2021 this could potentially impact the new undefined term “attempt to compromise” in **CIP-008-6**, featuring the latest version of NERC CIP incident response requirements. In which case, each utility would have new reporting responsibilities to both NERC and DHS

# RESOURCES

Whitepaper

## Collection Management Frameworks – Beyond Asset Inventories for Preparing for and Responding to Cyber Threats



By Dragos, Inc. 12.11.18

<https://www.dragos.com/resource/collection-management-frameworks-beyond-asset-inventories-for-preparing-for-and-responding-to-cyber-threats/>

DRAGO 

**THANK YOU!**

# SUMMARY

- The SolarWinds compromise is significant and affects industrial organizations
- **Dragos customers:**
  - Check the customer portal for the SolarWinds Advisory Alert, SolarWinds Playbook
  - Also in the portal the IR team has released a package that can help identify host-based signs of compromise without requiring the installation of any third-party software
- Even if you don't own SolarWinds you may be affected
  - 3<sup>rd</sup>-party networks, services, and vendors may use SolarWinds
- If you do not have monitoring and centralized logging in your ICS/OT networks then **you need to go hunting**
- Check NERC CIP considerations for notifying, assessing, reporting