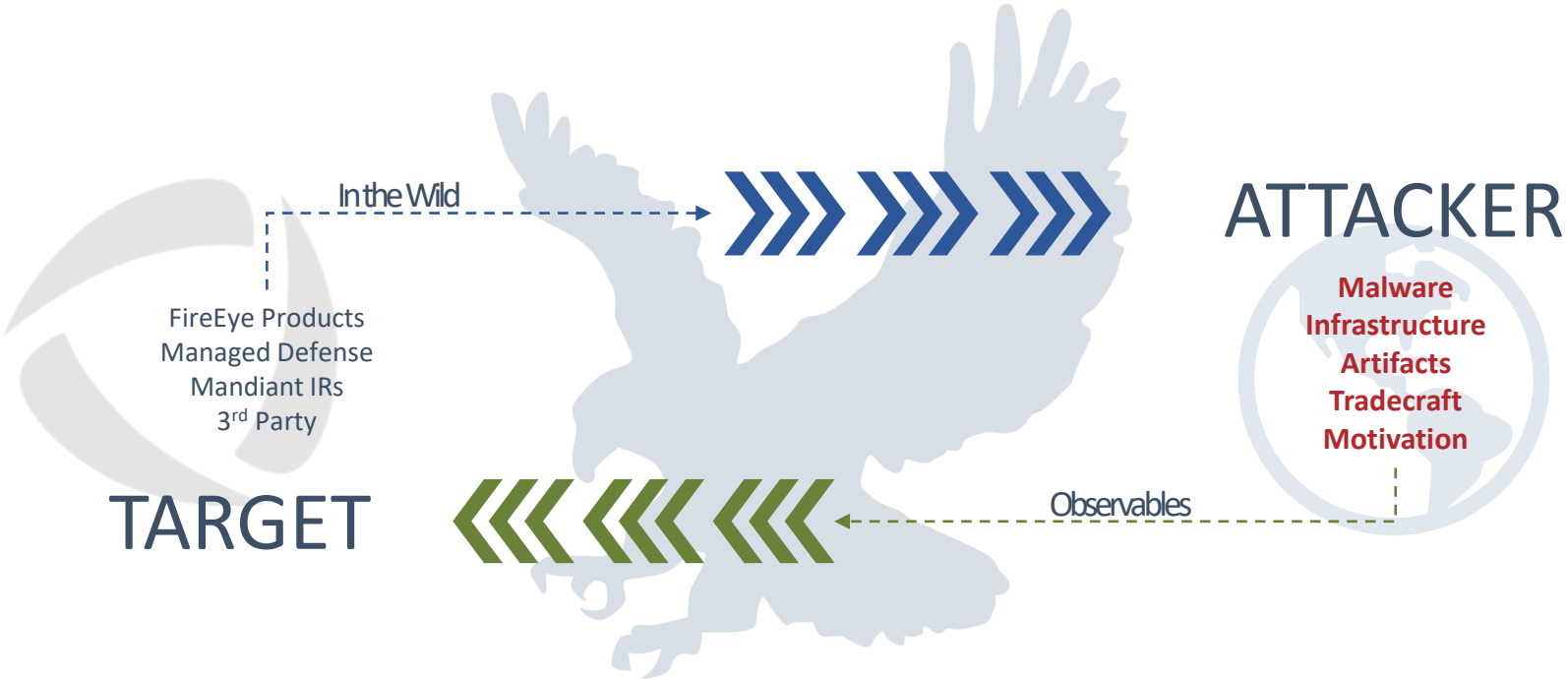
UNC2452: Highly Evasive Attacker Leverages Supply Chain to Compromise Targets

Nicole Oppenheim

Ben Withnell

Willi Ballenthin

Innovation Cycle



UNC2452 & FireEye Customers

- Detections
- Hunting
- Notifications
- Webinar & Blog

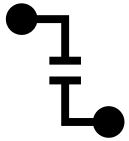
Threat Attribution Methodology

Threat Attribution Methodology

UNC2452 & Associated Clusters

Low Malware Footprint

Prioritizes Stealth



High OPSEC

Targeted & Resourced

TTPs of UNC2452

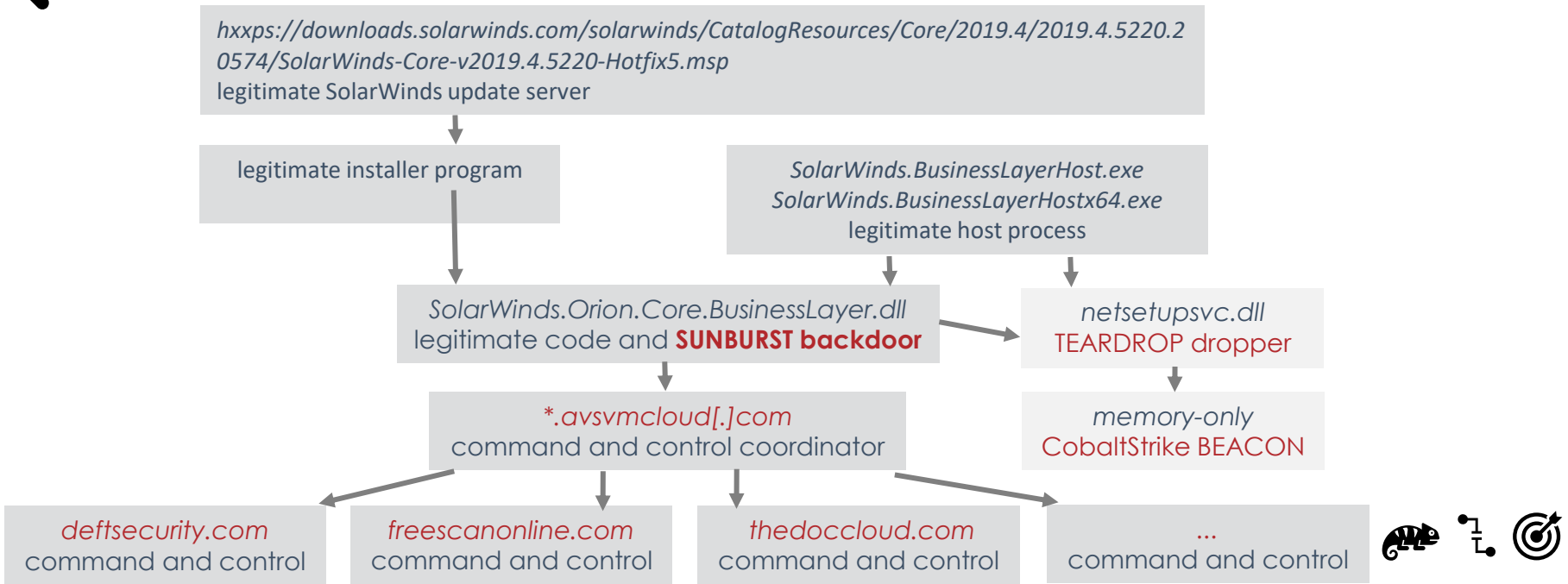
...and associated Clusters

Supply Chain Compromise

MITRE TECHNIQUE: T1195.002

Summary: UNC2452 has compromised the SolarWinds supply chain. They distribute backdoored updates to unsuspecting customers.

Supply Chain: SolarWinds



Supply Chain Compromise

MITRE TECHNIQUE: T1195.002

Summary: UNC2452 has compromised the SolarWinds supply chain. They distribute backdoored updates to unsuspecting customers.

Supply Chain: SolarWinds: SolarWinds.Orion.Core.BusinessLayer.dll

Digitally-signed plug-in for SolarWinds Orion

Large amount of legitimate code
- 400+ classes
- 3,000+ methods
- ~45,000 lines of source code

One namespace implements the SUNBURST backdoor
A second region of code invokes backdoor

Signature Dates:
- March, 2020
- April, 2020
- May, 2020

Hides in plain sight:
- OrionImprovementBusinessLayer
- appId
- ReportWatcherPostpone

Malware: SUNBURST

MD5: b91ce2fa41029f6955bff20079468448 (other variants, see blog)
SHA256: 32519b85c0b422e4656de6e6c41878e95fd95026267daab4215ee59c107d6c77
Digital signature date: March 24, 2020

No binary similarity or code reuse was identified in malware repositories.

Summary: SolarWinds.Orion.Core.BusinessLayer.dll (b91ce2fa41029f6955bff20079468448) is a SolarWinds-signed plugin component of the Orion software framework. This plugin contains a malicious class named that communicates via HTTP to a command-and-control (C2) server to retrieve commands, called “Jobs”, that are executed on the system.

Characteristics

Capabilities

- Blocklist of analysis tools and services including: FireEye HX, floss, AV
- System survey and reconnaissance
- Full control of system
  - Registry
  - Processes
  - Files

Network Protocol

- DGA + DNS-based C2 coordinator
- Outbound traffic masquerades as Orion Improvement Program
- Commands returned in fake .NET config (steganography)

Steganography

MITRE TECHNIQUE: T1027.003

Hidden C2 Protocol

Commands extracted from fake .NET assembly configs

Regular expressions select:

- GUIDs
- Hexadecimal strings

Decrypt, decode, and dispatch

```
<?xml version="1.0" encoding="utf-8"?>
<assembly Name="SolarWinds.Orion.Apollo" Version="4.8"
          Key="{e7140000-10fd-4a4b-83b2-5aa6ee3b03e3}">
    <dependencies>
        <assemblyIdentity
            Name="System.Reactive.Core" Version="3.0.3000.0" Culture='
            Key="{2a017710-db0d-fd99-8897-54119bfab21a}"
            PublicKeyToken="5abe213f12a64419"
            Hash="86aba554ede5f74b898090ca77f6755e" />
        <assemblyIdentity
            Name="SolarWinds.AgentManagement.Messaging.Core"
            Version="2.1.0.1257" Culture="neutral"
            Key="{8c9766ff-9e82-4c69-49a9-becf4a28e9db}"
            PublicKeyToken="4fb7efeddfe06d8b"
            Hash="6fc6eb6fae3ea79772e5e38febc5f123"/>
        <assemblyIdentity
            Name="SolarWinds.CortexPlugin.Orion.Monitoring.Contracts"
            Version="3.0.0.3149" Culture="neutral"
            Key="{ede8f3f1-afe2-a2ec-fb4f-82f88915c6f1}"
            PublicKeyToken="97bb0555a6a1cfc3"
            Hash="c1aa692e8561743f82006f57ce3ec50e"/>
```

Malware: SUNBURST

MD5: b91ce2fa41029f6955bff20079468448 (other variants, see blog)
SHA256: 32519b85c0b422e4656de6e6c41878e95fd95026267daab4215ee59c107d6c77
Digital signature date: March 24, 2020

No binary similarity or code reuse was identified in malware repositories.

Summary: SolarWinds.Orion.Core.BusinessLayer.dll (b91ce2fa41029f6955bff20079468448) is a SolarWinds-signed plugin component of the Orion software framework. This plugin contains a malicious class named that communicates via HTTP to a command-and-control (C2) server to retrieve commands, called “Jobs”, that are executed on the system.

Technologies

- FireEye NX
- FireEye HX

Countermeasures

- 4x Yara rules [code patterns]
- 16x Snort rules [C2 protocol]
- 4x HX IOCs [behavior]

Indicators

Domain: avsvmcloud[.]com

URL: /swip/Events

String: OrionImprovementBusinessLayer

Named Pipe:
583da945-62af-10e8-4902-a8f205c72b2e

Malware: TEARDROP

Memory-Only Dropper

No binary similarity or code reuse with the dropper was identified in malware repositories.

Summary: The malware runs as a service, spawns a thread, and reads from the file "gracious_truth.jpg" which has a fake JPEG header. Next, it decodes an embedded payload using custom rolling XOR algorithm, and manually loads into memory embedded payload using custom PE-like file format.

Data Source

- Endpoint Agent
- AV Logs

Technologies

- FireEye HX: MalwareGuard
- Windows Defender

Countermeasures

- MalwareGuard
- 2x Yara

Artifacts

HX *file_operation_closed*
actor-process: *SolarWinds.BusinessLayerHost.exe*
file-path: *C:\Windows\SysWOW64\NetSetupSvc.dll*

Windows Defender Exploit Guard log entries
Process '...*svchost.exe*' (PID ...) would have been blocked from loading the non-Microsoft-signed binary '*Windows\SysWOW64\NetSetupSvc.dll*'.

Payload

Layers of loaders unpack a BEACON backdoor in-memory.

Attacker Hostname Masquerades

MITRE TECHNIQUE: NOT FOUND

Summary: The Attackers use legitimate victim hostnames as the hostname on their C2 servers for masquerades during remote access sessions

Data Source

- Internet Scan Data
- Remote Access Logs

Impact

Results in enumerated attacker infrastructure and timelines of use, which can be used to trace attacker access through a compromised environment

Analyst Methodology

1. Identify Attacker Infrastructure:

- Query internet-wide scan data sources for infrastructure serving SSL certs on tcp/3389 with your environment's hostnames in the Common Name (CN).
  - NOTE: IP Scan history often showed IPs switching between default (WIN-*) hostnames and victim's hostnames

Pivot

2. Identify Malicious Remote Access:

- Cross Reference identified infrastructure with IP records from your Remote Access Logs
  - NOTE: Attacker has a high level of OPSEC, they'll most likely use a single account per IP Address

Domestic Infrastructure Hosting

MITRE TECHNIQUE: NOT FOUND

Summary: The Attackers use infrastructure originating from the country where their victims are located. However, their remote authentications often were from impossible locations when analyzed against that user's legitimate logins.

Data Source

- Remote Access Logs

Technologies

- SIEM
- https://github.com/fireeye/GeoLogonalyzer
- (Integrated into FireEye Helix)

Impact

Identify patterns of not only attacker behavior but of common legitimate-use behavior which can be excluded from intrusion analysis

Analyst Methodology

Identify Suspicious Logons

- Analyze logons sourced from different regions within windows of time in which a human being cannot feasibly travel

Identify Logins From Attacker ASNs

- After identifying malicious IP addresses, monitoring for remote access from the same ASN may yield further attacker infrastructure
- Baselining and normalizing ASNs used for legitimate remote access may identify attacker infrastructure

Remote Access From VPS

MITRE TECHNIQUE: T1583.003 or T1584.003

Summary: The Attackers primarily use DCH (distributed cloud hosting) infrastructure to authenticate to environments

Data Source

- ip2location
- Remote Access Logs

Technologies

- SIEM

Impact

Identify additional attacker infrastructure

Analyst Methodology

Identify Suspicious Logons

- Monitoring remote access authentications from DCH IP addresses may identify malicious access

- **Available Tool:**
  - https://github.com/fireeye/GeoLogonalyzer (integrated into FireEye Helix)

Lateral Movement

MITRE TECHNIQUE: T1021 (REMOTE SERVICES)

Summary: The Attackers move laterally with multiple credentials from one host, once authenticated to Remote Access

Data Source

- Windows Event Logs with EIDs: 4624, 4625, 4628, 21, 22

Technologies

- SIEM
- HX LogonTracker module

Impact

This analysis quickly identifies systems used by an attacker to move laterally through the environment and can help prioritize those systems for deeper forensic analysis

Analyst Methodology

Identify One:Many relationships for Logons

- Use HX's LogonTracker module, to graph all logon activity and analyze for systems displaying a 1:many relationship between source systems and accounts.
  - One system authenticating to multiple systems, with multiple credentials
  - Never with the credentials used for remote access

Temporary File Replacement

MITRE TECHNIQUE: NOT FOUND

Summary: The Attackers remotely execute utilities by identifying a legitimate file, supplanting it with their own utility for use and then replacing the original file

Data Source

- SMB Logs

Technologies

- NSM Sensors

Impact

This analysis allows analysts to identify attackers staging, obfuscating, and executing malware on hosts.

Analyst Methodology

Identify Attackers Supplanting Utilities

- Look for SMB sessions that show access to legitimate directories and follow a delete-create-execute-delete-create pattern in a short amount of time

Temporary Task Modification

MITRE TECHNIQUE: T1053.005 (SCHEDULED TASK/JOB: SCHEDULED TASK)
MITRE SUB-TECHNIQUE: NOT FOUND

Summary: The Attackers temporarily **UPDATE** existing, legitimate Scheduled Tasks to execute their tools before returning the Scheduled Task to its original state

Data Source

- Microsoft-Windows-TaskScheduler/Operational event log -- EID 140, task updated
- Security event log -- EID 4702

Impact

This technique is likely used for OPSEC purposes, specific detections for this technique will increase likelihood of discovering an intrusion

Analyst Methodology

Monitor Existing Scheduled Tasks for Temporary Updates

- Use frequency analysis of task updates to identify anomalous modifications to tasks
  - Look for suspicious modifications to legitimate Windows tasks
- Monitor for legitimate Windows tasks executing new/unknown binaries

UNC2452 & FireEye Customers

- We've deployed detections across our Products
- Hunted across appliance telemetry and notified impacted customers
- We will continue to hunt across product telemetry
- Coordination across Incident Response engagements
- Managed Defense is actively hunting and providing compromise reports to their impacted customers
- Releasing a blog that includes
  - Overview Activity
  - Attacker techniques
  - In-depth Malware on SUNBURST

Recommended Actions

- Following recommendations are for immediate mitigation techniques:
  - Ensure the SolarWinds servers are isolated / contained until a further review
    - This should include blocking all Internet egress from SolarWinds servers.
  - If SolarWinds infrastructure is not isolated, consider taking the following steps:
    - Restrict scope of connectivity to endpoints from SolarWinds servers - especially those that would be considered Tier 0 / crown jewel assets
    - Restrict the scope of accounts that have local administrator privileged on SolarWinds servers.
    - Block Internet egress from servers or other endpoints with SolarWinds software.

Recommendation Actions (con't)

- Consider (at a minimum) changing passwords for accounts that have access to SolarWinds servers / infrastructure.

- If SolarWinds is used to managed networking infrastructure, consider conducting a review of network device configurations for unexpected / unauthorized modifications.
  - Note, this is a proactive measure due to the scope of SolarWinds functionality, not based on investigative findings.
  - SolarWinds should be releasing a blog post shortly which will include their specific mitigation actions and recommendations

Summary

- Best Operational Security we've seen across our investigations
- Attacker is highly skilled and motivated
- Leverages inherent Trust through Supply Chain
- Highly Evasive and Resourced

- FireEye's signatures to detect this threat actor and supply chain attack in the wild are available here: https://github.com/fireeye/sunburst_countermeasures