Agenda

- Overview of distributed attacks
- Supply chain attacks
- Discussion of SolarWinds attack
- Managed Service Provider attacks
- Discussion of Blackbaud attack
- How to think about distributed attacks
- References
- Questions

Slides Key:

**Non-Technical:** Managerial, strategic and high-level (general audience)

**Technical:** Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)
What is a distributed attack?

**Traditional attack = a single compromise impacts a single organization**
What is a distributed attack?

**Distributed attack = a single compromise that impacts multiple organizations**

By targeting MSPs, threat actors can gain access to the MSP’s clients (including businesses, universities, and other institutions) without having to compromise each client directly.

Image source: cyber.gc.ca
But what about DDoS (distributed denial of service) attacks?

We will be discussing two types of distributed attacks in this presentation, both of which present a significant threat to healthcare: supply chain attacks and managed service provider attacks. We will be analyzing two cases: the SolarWinds attack (supply chain), as well as the Blackbaud breach (managed service provider).

This presentation is based on the best information available at the time of delivery – new details will emerge.
Supply Chain Attacks

What is a supply chain?
- A supply chain is the collection of elements that go into producing and providing a good or service; like materials, information, services, people, processes, and technology
- Sequential steps
- Transformation of materials

What is a supply chain attack?
- Inflicting damage on an organization by compromising a component of their supply chain
- Hardware and software are vehicles
- Customers are ultimate targets
- Palo Alto, December 2017: The Era of Software Supply-Chain Attacks Has begin
- Atlantic Council, July 2020 – “States have used software supply chain attacks to great effect.”
It all began with a FireEye compromise

- FireEye discovered they had been breached
  - SolarWinds Orion was the distribution mechanism
  - Their red team tools were compromised

- The compromise of SolarWinds involved many other organizations, both government and private sector – one estimate states that over 18,000 of their customers downloaded an applied the update

- Initial detection: December 2020
- Initial threat actor access to SolarWinds: September 2019
- SolarWinds files 8-K on December 14th
- US CERT releases first alert on December 17th
- The investigation and public disclosure of information continues
SolarWinds: What Happened? (continued)

- It utilizes at least three forms of malware
  - SUNSPOT (implant)
  - SUNBURST/Solarigate (backdoor)
  - TEARDROP (post-exploitation tool)
- It utilizes command-and-control (C2) infrastructure
- Actions on objectives:
  - Administrative account access via compromised credentials
  - Administrative account access via forged SAML tokens
- Who was it? Probably Russia foreign intelligence
  - Cozy Bear/APT29/Office Monkeys/Dark Halo/UNC2452
  - Connections to Turla
  - Ultimate targets likely selected manually

Image source: Microsoft
• Backdoor was included in malicious dynamic link library

• SolarWinds download site password: SolarWinds123

• Malicious update dll is distributed to customers (manually or automatically)

• Compromised update signed with legitimate digital signature

• C2 Beaconing waits for several weeks after initial installation to begin

• SUNBURST backdoor is distributed to all customers via the standard software update distribution channels:

“SolarWinds Orion is a network management tool. It knows EVERYTHING on your network. Device, software version, firmware version, applications, etc…. So they have a complete inventory – and as such, can look at the exploits they have available to them, and determine based on the devices that are vulnerable which organizations they will target. Quite frankly, it’s genius as it improves their return.”

- Marcus Hartwig, manager of security analytics at Vectra
SolarWinds claims over 300,000 customers; ~18,000 were reportedly exposed in this attack, including:

- More than a dozen critical infrastructure companies in the electric, oil, and manufacturing industries
- FireEye, CrowdStrike
- Several US Federal government departments including at least one that deals with healthcare
- State and local governments
- At least one hospital

These simply represent what was publicly disclosed at the time of this presentation – the list may continue to expand as time goes on.

---

**List of Hacked Organizations Tops 200 in SolarWinds Case**

*The number is expected to grow as the wide-ranging investigation continues. The hackers’ motive remains unknown, and it’s not clear what they reviewed or stole from the computer networks they infiltrated.*

BY WILLIAM TURTON, BLOOMBERG NEWS / DECEMBER 21, 2020
First, it’s always better to prevent an incident from happening. Below we have several sets of indicators of compromise (IOCs). Please note several things about these:

- There is a significant quantity of indicators of compromise related to the SolarWinds compromise available on the Internet. Only a very small sample of them are included below.
- Upon being released to the public, IOCs may become “burned” – the attackers will adjust their TTPs, weapons and infrastructure so that the public IOCs are no longer used.
- There are instances of obsolete IOCs being re-used, so any organization attempting to defend themselves should consider all possibilities.
- New IOCs will likely continue to be released. It is therefore incumbent upon any organization attempting to defend themselves to remain vigilant, maintain situational awareness, and be ever on the lookout for new IOCs to operationalize in their cyberdefense infrastructure.

**Indicators of Compromise:**

**Microsoft:**

**Malwarebytes:**

**Protiviti:**

**CISA:**
[https://us-cert.cisa.gov/ncas/alerts/aa20-352a](https://us-cert.cisa.gov/ncas/alerts/aa20-352a)
What can be done to ensure this attack doesn’t take place, and/or to minimize its impact

- “Kill switch” is already in place; but that doesn’t relieve potential victim organizations from taking action
  - FireEye and Microsoft collaborated to sinkhole traffic

- Detection is critical
  - Beaconing traffic to specific domains/IP addresses

- Isolate any potentially vulnerable systems
  - Orion platform versions 2019.4 HF 5 through 2020.2.1, released between March 2020 and June 2020
  - Create forensic images of potentially affected systems
    - Analyze images for new accounts
  - Analyze historic traffic for IOCs (connection attempts to domains/IP addresses

- Remain current on research released – 6 weeks after initial discovery, new information continues to be released by stakeholders on a daily basis

- Consider implementing “zero trust” principles into network security operations practices

- Review the documentation related to your supply chain partners and ensure they are practicing proper cyber hygiene
To help identify instances of SUNSPOT, YARA can be helpful. The YARA rule for SUNSPOT is on the right.

It can also be found here: https://www.crowdstrike.com/blog/sunspot-malware-technical-analysis/
The following alerts, guidance and background information may prove helpful:

- **DHS: Emergency Directive 21-01**

- **DHS: Supplemental Guidance for ED 21-01 (version 1)**

- **DHS: Supplemental Guidance for ED 21-01 (version 2)**

- **DHS: Supplemental Guidance for ED 21-01 (version 3)**

- **Alert (AA20-352A) Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations**
  [https://us-cert.cisa.gov/ncas/alerts/aa20-352a](https://us-cert.cisa.gov/ncas/alerts/aa20-352a)

- **SolarWinds Security Advisory**
  [https://www.solarwinds.com/securityadvisory](https://www.solarwinds.com/securityadvisory)

- **Microsoft: Understanding "Solorigate"'s Identity IOCs - for Identity Vendors and their customers**

- **National Security Agency: Russian State-Sponsored Actors Exploiting Vulnerability in VMware WorkspaceONE Access Using Compromised Credentials**

The following tools may prove helpful:

- **CISA Sparrow:**
  [https://github.com/cisagov/Sparrow](https://github.com/cisagov/Sparrow)

- **CrowdStrike Reporting Tool for Azure (CRT)**
  [https://github.com/CrowdStrike/CRT](https://github.com/CrowdStrike/CRT)

- **Using Microsoft 365 Defender to protect against Solorigate**
A managed service provider is the outsourcing of IT services:

**Common Types of Managed Services**

<table>
<thead>
<tr>
<th>Managed Services</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managed Networks &amp; Infrastructure</td>
<td>These services include managed IP VPNs, which are widely used for secure, high-performance and cost-effective networking. Also, managed hosting and storage services fall into this category. These services eliminate the cost of owning and running a data center — the MSP will provide that back-end under an SLA. Likewise, managed LAN and WAN services also help to reduce total cost of ownership (TCO).</td>
</tr>
<tr>
<td>Managed Security Services</td>
<td>This type of managed service provides a broad range of solutions from patch management to antivirus, malware and other remote security updates.</td>
</tr>
<tr>
<td>Managed Communications Services</td>
<td>This managed service merges data, voice, and video services on the same IP network. It also includes a managed contact center that combines traditional call centers with intelligent IP call routing and integrates e-mail, phone, Web, instant messaging, fax, and other human or automated forms of customer contact.</td>
</tr>
<tr>
<td>Managed Wireless &amp; Mobile Computing Services</td>
<td>Like managed hosting and storage, this service enables wireless capabilities without the capital expenditure and implementation.</td>
</tr>
<tr>
<td>Managed Print Services</td>
<td>Often grouped just outside the larger framework of managed services, managed print enables remote monitoring, updating and management of an organization’s document management infrastructure.</td>
</tr>
<tr>
<td>Managed Support Services</td>
<td>This service handles traditional help desk responsibilities, including trouble ticketing for IT problems among employees and resolution mechanisms.</td>
</tr>
<tr>
<td>Business Intelligence/Data Analytics Services</td>
<td>Increasingly, MSPs are capturing and analyzing data that reveal trends and patterns that clients can act upon to further their business goals. Case in point: Trending information on peak Internet usage times around e-commerce. If an MSP can provide a timeline of peaks and valleys in traffic on a quarterly basis, customers can make adjustments to their marketing, sales staffing, supply chain and inventory plans.</td>
</tr>
<tr>
<td>Managed Cloud Infrastructure Services</td>
<td>With managed cloud, the MSP’s or cloud provider’s engineers manage the customers’ computing, storage, networks and operating systems. It also may include managing the tools and application stacks (e.g., databases, e-commerce platforms and DevOps tools) that run on top of that infrastructure. Often customers can choose which functions to manage in-house and which to outsource to the service provider. In some cases where there are multiple cloud providers, the MSP fulfills the role of “cloud orchestrator.”</td>
</tr>
<tr>
<td>Managed Software as a Service</td>
<td>Software-as-a-service (SaaS) delivery is inherently managed. The provider hosts and delivers the application to the customer and makes sure that it is constantly updated and improved. In some cases, the MSP is the SaaS provider and in others it resells the services and assists with integrations to other on-premises and cloud applications.</td>
</tr>
</tbody>
</table>

Image source: CompTIA
Managed service providers:

- **Pros:**
  - Cost
  - Scalability
  - Technology
  - Expertise

- **Cons:**
  - Control
  - Flexibility/customization of services
  - Communication/management issues

Image source: TechTarget
Managed Service Provider Attacks

How does a managed service provider attack occur?

**STEP 1:**
Attacker compromises MSP

**STEP 2:**
MSP client communications are used to facilitate attacks

**STEP 3:**
Clients are compromised
Blackbaud: What Happened?

Who is Blackbaud?
• Managed IT services provider that serves nonprofits)
• Based in SC, publicly traded
• Claims over 25,000 clients in over 60 countries
• Awards:
  o Forbes: Leading Employer for Diversity
  o Fortune: 56 Companies Changing the World
  o IDC: Top 40 Global Cloud Software Service Providers

What are the details of the attack?
• Disclosed on July 16, 2020 that they were the victim of an unnamed ransomware attack, and they had paid the ransom
• Confirmed attackers were able to gain access to some customers' unencrypted banking information, login credentials, and social security numbers
• In November 2020, they confirmed they had been named as a defendant in 23 putative class suits
• They have received over 160 claims related to the attack
• 200 organizations (many healthcare) and millions of individuals have been impacted
Compromised healthcare organizations:

- A sample set is on the right, this list does not represent every healthcare organization impacted by Blackbaud
- Some of these are subject to change as updated information becomes available
- Blackbaud had to spend over $3 million to deal with the attack’s aftermath between July and September, and it also recorded almost $3 million in accrued insurance recoveries during the same time period

<table>
<thead>
<tr>
<th>Organization Name</th>
<th>Records breached</th>
</tr>
</thead>
<tbody>
<tr>
<td>Medical center in Kansas</td>
<td>315,811</td>
</tr>
<tr>
<td>Hospital in Michigan</td>
<td>52,711</td>
</tr>
<tr>
<td>Hospital in Michigan</td>
<td>95,000</td>
</tr>
<tr>
<td>Hospital in North Carolina</td>
<td>Unknown</td>
</tr>
<tr>
<td>Hospital in California</td>
<td>39,881</td>
</tr>
<tr>
<td>Healthcare provider in Ohio</td>
<td>118,874</td>
</tr>
<tr>
<td>Health center in Pennsylvania</td>
<td>3,320,726</td>
</tr>
<tr>
<td>Healthcare network in Virginia</td>
<td>1,045,270</td>
</tr>
<tr>
<td>Health service provider in Maine</td>
<td>657,392</td>
</tr>
<tr>
<td>Health service provider in Washington State</td>
<td>300,000</td>
</tr>
<tr>
<td>Health service provider in Pennsylvania</td>
<td>60,595</td>
</tr>
<tr>
<td>Healthcare providers in Illinois</td>
<td>55,983</td>
</tr>
</tbody>
</table>
Blackbaud: What Can Be Done?

- The HHS 405(d) Program published the Health Industry Cybersecurity Practices (HICP), which is a free resource that identifies the top five cyber threats and the ten best practices to mitigate them. Below are the practices from HICP that can be used to mitigate Maze:

<table>
<thead>
<tr>
<th>DEFENSE/MITIGATION/COUNTERMEASURE</th>
<th>405(d) HICP REFERENCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provide social engineering and phishing training to employees.</td>
<td>[10.S.A], [1.M.D]</td>
</tr>
<tr>
<td>Develop and maintain policy on suspicious e-mails for end users; Ensure suspicious e-mails are reported.</td>
<td>[10.S.A], [10.M.A]</td>
</tr>
<tr>
<td>Ensure emails originating from outside the organization are automatically marked before received.</td>
<td>[1.S.A], [1.M.A]</td>
</tr>
<tr>
<td>Apply patches/updates immediately after release/testing; Develop/maintain patching program if necessary.</td>
<td>[7.S.A], [7.M.D]</td>
</tr>
<tr>
<td>Implement spam filters at the email gateways; Keep signatures and rules updated.</td>
<td>[1.S.A], [1.M.A]</td>
</tr>
<tr>
<td>Block suspicious IP addresses at the firewall; Keep firewall rules are updated.</td>
<td>[6.S.A], [6.M.A], [6.L.E]</td>
</tr>
<tr>
<td>Implement whitelisting technology to ensure that only authorized software is allowed to execute.</td>
<td>[2.S.A], [2.M.A], [2.L.E]</td>
</tr>
<tr>
<td>Conduct system hardening to ensure proper configurations.</td>
<td>[7.S.A], [7.M.D]</td>
</tr>
<tr>
<td>Disable the use of SMBv1 (and all other vulnerable services and protocols) and require at least SMBv2.</td>
<td>[7.S.A], [7.M.D]</td>
</tr>
</tbody>
</table>

Background information can be found here: https://www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf
Distributed Attacks: How to Think About Them

We know healthcare organizations are potential targets of supply chain and MSP attacks. Why?

- Healthcare organizations utilize managed services and supply chains, just as organizations in other industry verticals do
- We know these attacks are increasing, and we know why these attacks are increasing

What are the bigger-picture action items for an organization that wants to defend against and avoid distributed attacks?

- Network engineers/Network security engineers should consider these attacks when designing, operating and maintaining their networks
  - What does your network layout look like?
  - Who do you trust? Do you trust anyone or anything more than you absolutely need to? The principle of least privilege applies
- Especially important: Review your contract language and ask questions about their security practices.
- Homogeneity makes them vulnerable – not having the most popular service provider might improve your attack surface
- **Think in terms of distributed attacks when developing/implementing your risk management approach!**
Differentiate supply chain attacks (part of the compromise vice the target of the compromise)

Modern Attacks Include Supply Chain "Hopping" and Reversing Agile Environments

Risks in IoT Supply Chain
https://unit42.paloaltonetworks.com/iot-supply-chain/

In wake of SolarWinds and Vietnam, more supply chain attacks expected 2021

Vietnam targeted in complex supply chain attack

North Korean software supply chain attack targets stock investors

Managed Security Services: Big Brothers and Guardian Angels
https://cisomag.eccouncil.org/managed-security-services/

Analysis: Supply Chain Management After SolarWinds Hack
https://www.healthcareinfosecurity.com/interviews/analysis-supply-chain-management-after-solarwinds-hack-i-4814
The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies

Managed Security Services Provider (MSSP) News: 24 December 2020

SolarStorm Supply Chain Attack Timeline
https://unit42.paloaltonetworks.com/solarstorm-supply-chain-attack-timeline/

2018 Predictions & Recommendations: The Era of Software Supply-Chain Attacks Has Begun

SolarWinds hackers have a clever way to bypass multi-factor authentication

~18,000 organizations downloaded backdoor planted by Cozy Bear hackers

DHS, State, NIH join list of federal agencies – now five – hacked in major Russian cyberespionage campaign

CNAME records associated with the #SUNBURST malware C2 beacon via @DomainTools Iris
https://twitter.com/jfslowik/status/1338320309816946690
References

U.S. Treasury, Commerce Depts. Hacked Through SolarWinds Compromise
https://krebsonsecurity.com/2020/12/u-s-treasury-commerce-depts-hacked-through-solarwinds-compromise/

Suspected Russian hackers spied on U.S. Treasury emails - sources
https://www.reuters.com/article/BigStory12/idUSKBN28N0PG

Important steps for customers to protect themselves from recent nation-state cyberattacks

DHS: Emergency Directive 21-01
https://cyber.dhs.gov/ed/21-01/

SolarWinds Security Advisory
https://www.solarwinds.com/securityadvisory

SolarWinds: How Orion Platform products work

FireEye, Microsoft create kill switch for SolarWinds backdoor

Continue Clean-up of Compromised SolarWinds Software

SolarWinds is the perfect storm attack on the US
https://thehill.com/opinion/cybersecurity/531141-solarwinds-is-the-perfect-storm-attack-on-the-us
References

Trump contradicts Pompeo in bid to downplay massive hack of U.S. government, Russia’s role

Microsoft to quarantine compromised SolarWinds binaries tomorrow

Alert (AA20-352A) Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations
https://us-cert.cisa.gov/ncas/alerts/aa20-352a

SolarWinds hackers breach US nuclear weapons agency

Analyzing Solorigate, the compromised DLL file that started a sophisticated cyberattack, and how Microsoft Defender helps protect customers

Sunburst: connecting the dots in the DNS requests

SolarWinds hackers breached US Treasury officials’ email accounts
Microsoft identifies second hacking group affecting SolarWinds software
https://www.cyberscoop.com/microsoft-solar-winds-hackers-supernova-backdoor/

Wyden Statement Following Treasury and IRS Briefing on SolarWinds Hack

Russia's FireEye Hack Is a Statement—but Not a Catastrophe

SolarWinds Campaign Focuses Attention on 'Golden SAML' Attack Vector

UK privacy watchdog warns SolarWinds victims to report data breaches

Lawmakers want more transparency on SolarWinds breach from State, VA
https://www.cyberscoop.com/menendez-blumenthal-state-va-solarwinds/

White House activates cyber emergency response under Obama-era directive

Grid regulator warns utilities of risk of SolarWinds backdoor, asks how exposed they are
https://www.cyberscoop.com/nerc-alert-solarwinds-grid-russia/

Partial lists of organizations infected with Sunburst malware released online

NSA, CISA Warn of Attacks on Federated Authentication

Massive Russian hack attack threatens national security and fuels disinformation warfare

White House confirms cyberattack report on U.S. Treasury by foreign government

Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor

Malicious Domain in SolarWinds Hack Turned into ‘Killswitch’

SolarWinds Hack Victims: From Tech Companies to a Hospital and University

Cisco, Intel, Deloitte Among Victims of SolarWinds Breach: Report
Cyberattack Hit Key US Treasury Systems: Senator
https://www.securityweek.com/cyberattack-hit-key-us-treasury-systems-senator

CISA: Supply Chain Compromise
https://www.cisa.gov/supply-chain-compromise

Partial lists of organizations infected with Sunburst malware released online

Kevin Mandia: 50 Firms ‘Genuinely Impacted’ By SolarWinds Attack

https://thecyberwire.com/newsletters/daily-briefing/9/245

IT giants VMware, Cisco confirmed as victims of SolarWinds hack

Kremlin officially rejects involvement in US hacker attacks

https://thecyberwire.com/podcasts/daily-podcast/1239/notes

SolarWinds is the perfect storm attack on the US
https://thehill.com/opinion/cybersecurity/531141-solarwinds-is-the-perfect-storm-attack-on-the-us
References

Continue Clean-up of Compromised SolarWinds Software

The List of Known SolarWinds Breach Victims Grows, as Do Attack Vectors

SOLARWINDS HACK INFECTED CRITICAL INFRASTRUCTURE, INCLUDING POWER INDUSTRY
https://theintercept.com/2020/12/24/solarwinds-hack-power-infrastructure/

Threat Research: SUNBURST Additional Technical Details
https://www.fireeye.com/blog/threat-research/2020/12/sunburst-additional-technical-details.html

Microsoft alerts CrowdStrike of hackers' attempted break-in
https://www.cyberscoop.com/crowdstrike-solarwinds-targeted-microsoft/

How we protect our users against the Sunburst backdoor
https://securelist.com/how-we-protect-against-sunburst-backdoor/99959/

CISA Releases ICT Supply Chain Risk Management Task Force Year 2 Report

Ex-NSA Director: SolarWinds Breach Is 'A Call for Action'
https://www.healthcareinfosecurity.com/ex-nsa-director-solarwinds-breach-a-call-for-action-a-15655

How SunBurst malware does defense evasion
References

Best Practice: Identifying And Mitigating The Impact Of Sunburst

CISA releases CISA Insights and creates webpage on ongoing APT cyber activity

CISA INSIGHTS: What Every Leader Needs to Know About the Ongoing APT Cyber Activity

SUPERNOVA SolarWinds .NET Webshell Analysis

Sunburst: Supply Chain Attack Targets SolarWinds Users

SUPERNOVA: A Novel .NET Webshell
https://unit42.paloaltonetworks.com/solarstorm-supernova/

Github: Remove COSMICGALE and SUPERNOVA rules #5
https://github.com/fireeye/sunburst_countermeasures/pull/5

Suspected Russian hackers used Microsoft vendors to breach customers
References

Threat Advisory: SolarWinds supply chain attack
https://blog.talosintelligence.com/2020/12/solarwinds-supplychain-coverage.html

Best of 2020: The SolarWinds Supply Chain Hack: What You Need to Know

McAfee Special Edition Webinar: Combating SolarWinds Supply Chain and SUNBURST Backdoor - from Device to Cloud

SANS Emergency Webcast: What you need to know about the SolarWinds Supply-Chain Attack
https://www.youtube.com/watch?v=qP3LQNsjKWw

SolarWinds: What It Means & What’s Next
https://www.youtube.com/watch?v=ZiA-5PuCI80

Microsoft has discovered yet more SolarWinds malware

The Sunburst attack, a second strain of malware and strengthening your security

A Timeline Perspective of the SolarStorm Supply-Chain Attack
https://unit42.paloaltonetworks.com/solarstorm-supply-chain-attack-timeline/

Threat Brief: SolarStorm and SUNBURST Customer Coverage
https://unit42.paloaltonetworks.com/fireeye-solarstorm-sunburst/
References

Top Treasury Email Accounts Exposed In SolarWinds Hack: Report

CrowdStrike releases free Azure security tool after failed hack

CISA Releases Free Detection Tool for Azure/M365 Environment

Russian hackers compromised Microsoft cloud customers through third party, putting emails & other data at risk

Grid regulator warns utilities of risk of SolarWinds backdoor, asks how exposed they are
https://www.cyberscoop.com/nerc-alert-solarwinds-grid-russia/

Experts who wrestled with SolarWinds hackers say cleanup could take months - or longer

SolarWinds Hackers "Impacting" State and Local Governments

SolarWinds releases updated advisory for new SUPERNOVA malware
References

Analysis: Supply Chain Management After SolarWinds Hack
https://www.healthcareinfosecurity.com/interviews/analysis-supply-chain-management-after-solarwinds-hack-i-4814

How to avoid subdomain takeover in Azure environments

SUNBURST, TEARDROP and the NetSec New Normal

SolarWinds roundup: Fixes, new bad actors, and what the company knew

SolarWinds: The Need for Persistent Engagement
https://www.lawfareblog.com/solarwinds-need-persistent-engagement

Visual Notes : SolarWinds Supply Chain compromise using SUNBURST backdoor Part 1

SUNBURST SolarWinds BackDoor : Crime Scene Forensics Part 2 (continued)
https://blog.shifleft.io/sunburst-solarwinds-backdoor-crime-scene-forensics-part-2-continued-3bcd8361f055

Best Practice: Identifying And Mitigating The Impact Of Sunburst

CISA releases CISA Insights and creates webpage on ongoing APT cyber activity
References

50 orgs 'genuinely impacted' by SolarWinds hack, FireEye chief says

Github: Remove COSMICGALE and SUPERNOVA rules #5
https://github.com/fireeye/sunburst_countermeasures/pull/5

SolarWinds Orion API authentication bypass allows remote command execution
https://kb.cert.org/vuls/id/843464

New Supernova Malware Found During SolarWinds Artifact Analysis
https://www.cyber.nj.gov/alerts-advisories/new-supernova-malware-found-during-solarwinds-artifact-analysis

SolarWinds Makes Fixes To Address Supernova Attack; Street Sees 34% Upside

Best Practice: Identifying And Mitigating The Impact Of Sunburst

How we protect our users against the Sunburst backdoor
https://securelist.com/how-we-protect-against-sunburst-backdoor/99959/

Microsoft: Understanding "Solorigate"'s Identity IOCs - for Identity Vendors and their customers.

Microsoft: Important steps for customers to protect themselves from recent nation-state cyberattacks

What Every Leader Needs to Know About the Ongoing APT Cyber Activity
https://www.cisa.gov/insights
CISA Releases Free Detection Tool for Azure/M365 Environment

GitHub CISA: Sparrow.ps1
https://github.com/cisagov/Sparrow

SolarWinds releases updated advisory for new SUPERNOVA malware

A New SolarWinds Flaw Likely Had Let Hackers Install SUPERNOVA Malware
https://thehackernews.com/2020/12/a-new-solarwinds-flaw-likely-had-let.html

Russia’s SolarWinds Attack

SolarWinds roundup: Fixes, new bad actors, and what the company knew

Using Microsoft 365 Defender to protect against Solorigate

Microsoft: SolarWinds hackers' goal was the victims' cloud data
https://www.bleepingcomputer.com/news/security/microsoft-solarwinds-hackers-goal-was-the-victims-cloud-data/
Upcoming Briefs

- Laying a Strong Cyber Foundation for the HPH
- ATT&CK for Emotet

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback to HC3@HHS.GOV.

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to HC3@HHS.GOV or call us Monday-Friday between 9am-5pm (EST) at 202-691-2110.
Health Sector Cybersecurity Coordination Center (HC3) Background

HC3 works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector

Products

Sector & Victim Notifications
Directs communications to victims or potential victims of compromises, vulnerable equipment, or PII/PHI theft, and general notifications to the HPH about currently impacting threats via the HHS OIG.

White Papers
Document that provides in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.

Threat Briefings & Webinar
Briefing document and presentation that provides actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

Need information on a specific cybersecurity topic, or want to join our listserv? Send your request for information (RFI) to HC3@HHS.GOV, or call us Monday-Friday between 9am-5pm (EST) at 202-691-2110.
Questions
Health Sector Cybersecurity Coordination Center (HC3)

202-691-2110

HC3@HHS.GOV