LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

Distributed Attacks and the Healthcare Industry

01/14/2021

Report #: 202101141030

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

Image source: CBS News

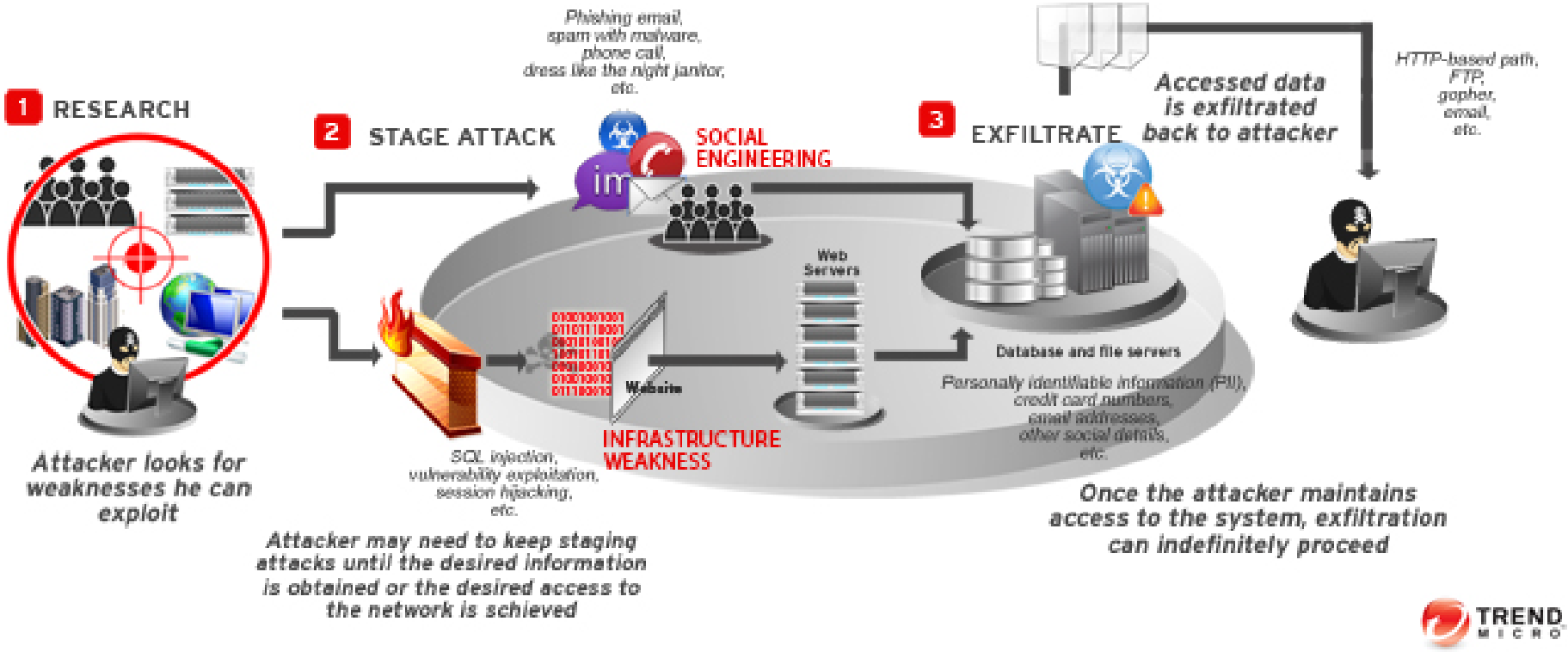
Slides Key:

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

Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

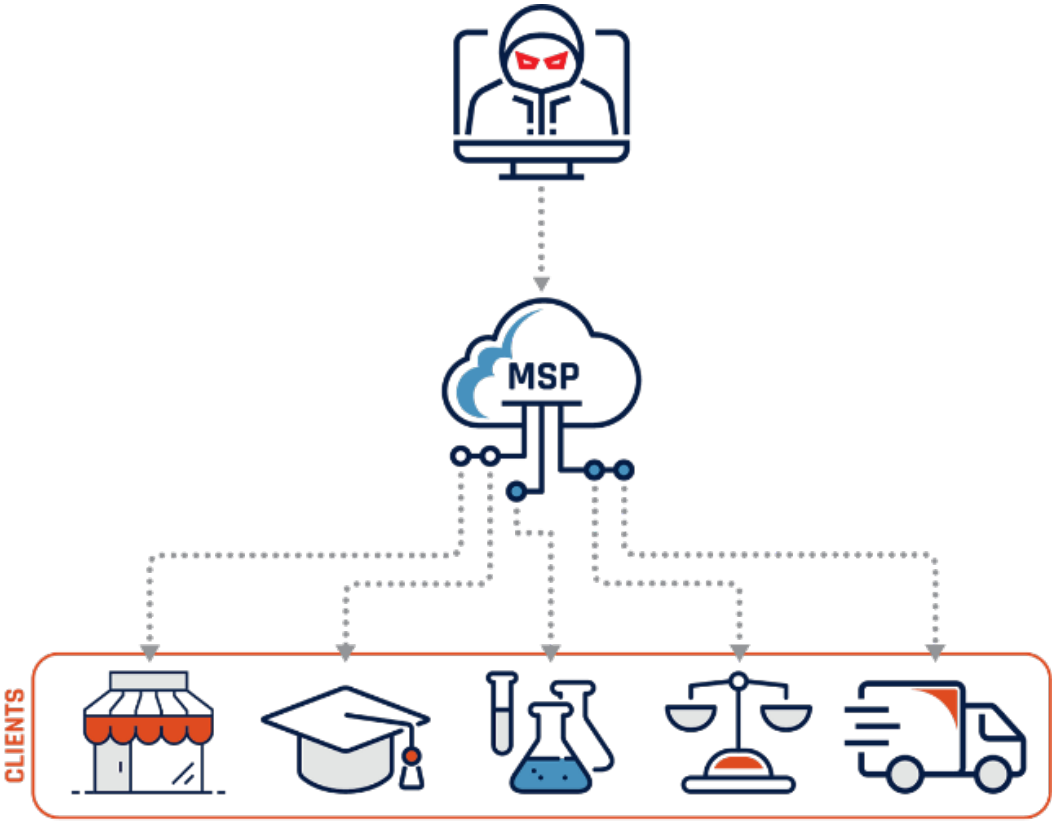
What is a distributed attack?

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?

Not a distributed attack in the context of the presentation, since it only targets one organization!

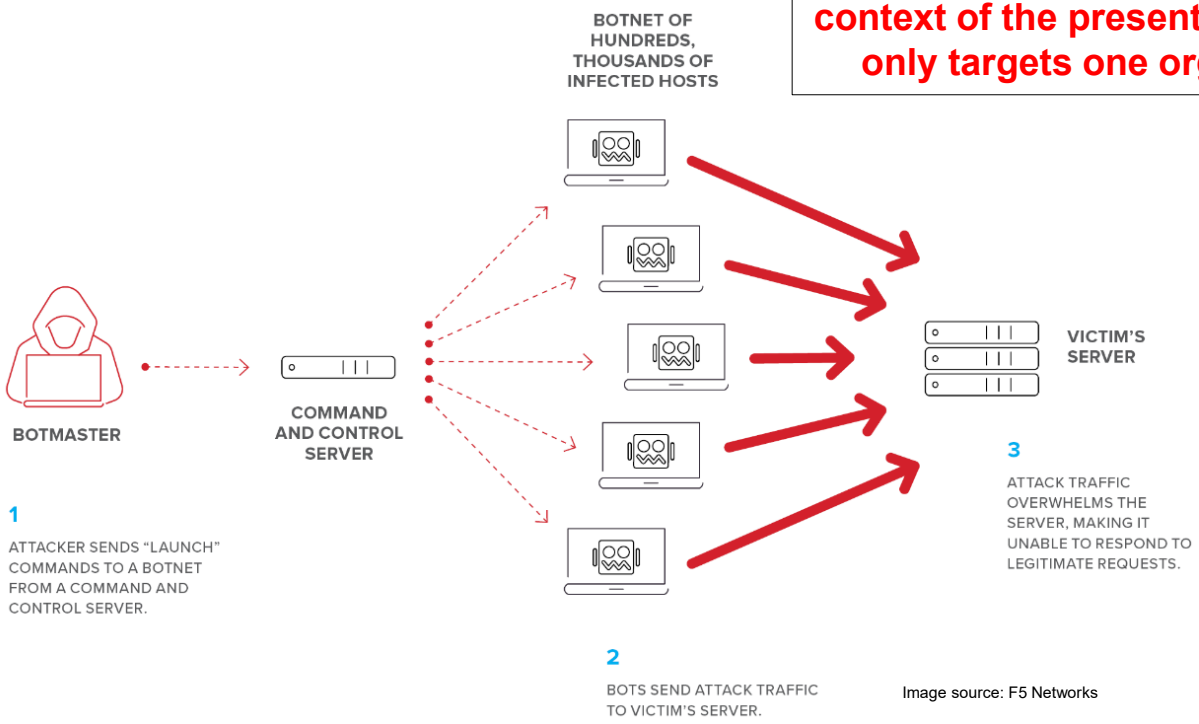


Image source: F5 Networks

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).

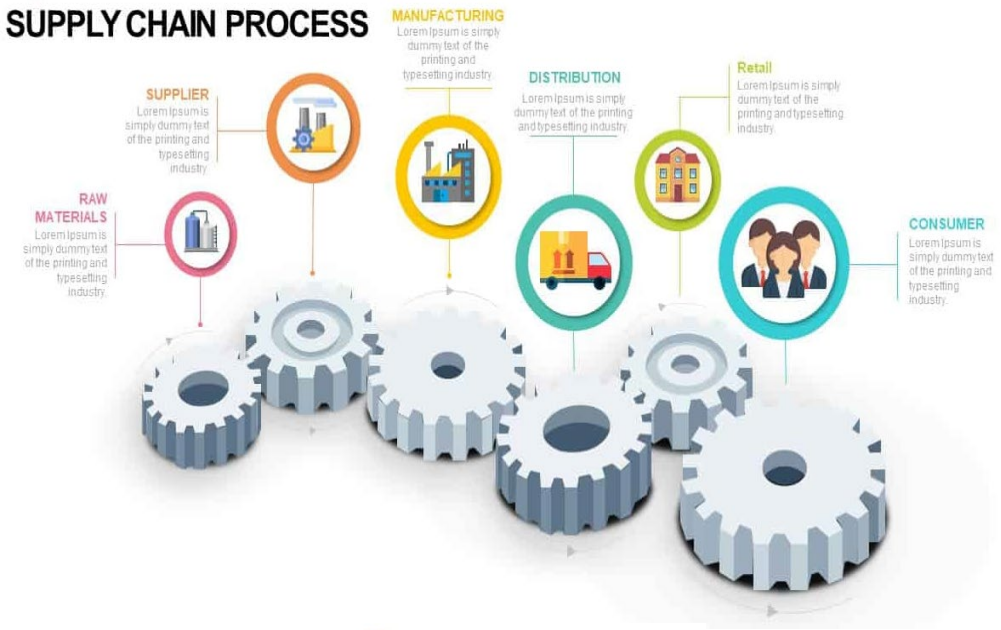
This presentation is based on the best information available at the time of delivery – new details will emerge.

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

Image source: Slidebazaar



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.”

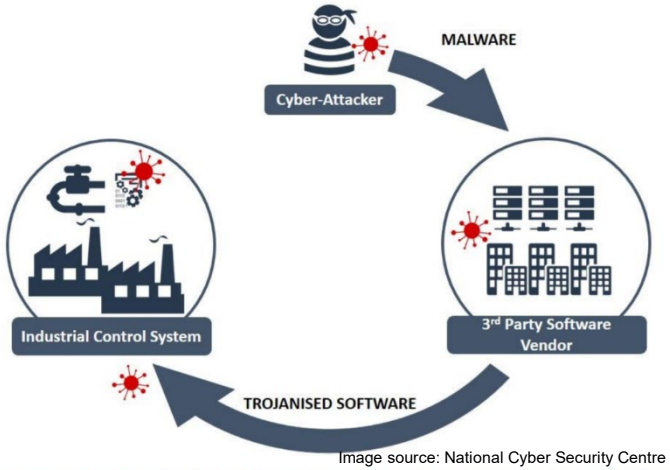


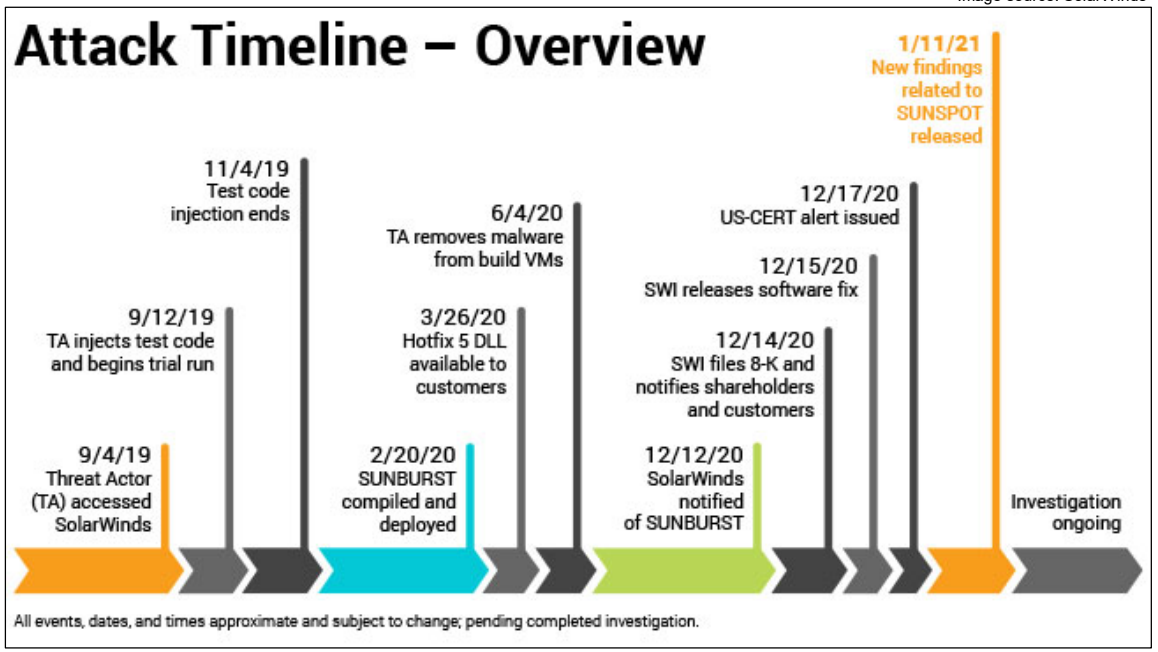
Image source: National Cyber Security Centre

SolarWinds: What Happened?

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 Solar Winds: 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

Image source: SolarWinds



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

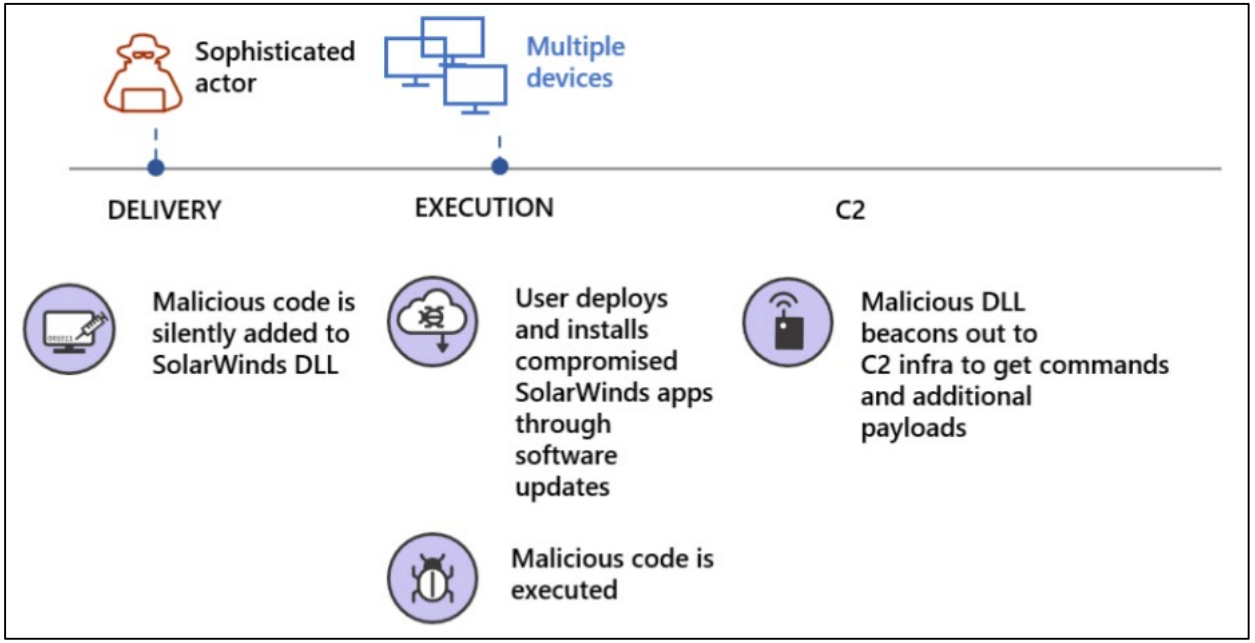


Image source: Microsoft

SolarWinds: Technical Summary

- Backdoor was included in malicious dynamic link library
  - Filename: SolarWinds.Orion.Core.BusinessLayer.dll (SUNBURST)
- 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: Who Was Impacted?

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

Image source: Government Technology

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:

https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/

Malwarebytes:

https://blog.malwarebytes.com/threat-analysis/2020/12/advanced-cyber-attack-hits-private-and-public-sector-via-supply-chain-software-update/

Protiviti:

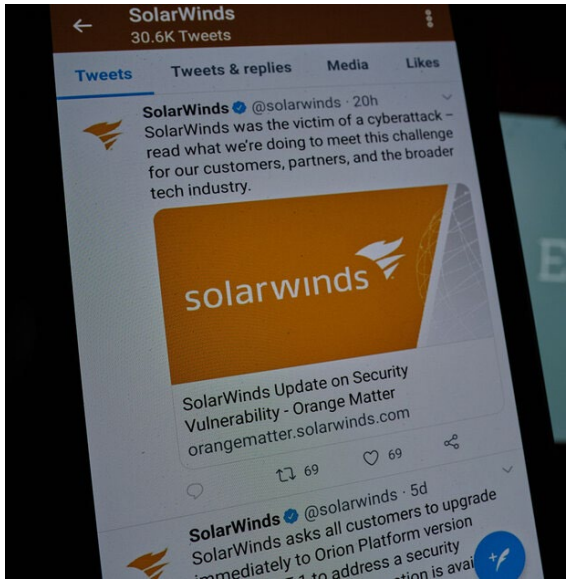
https://www.protiviti.com/US-en/solarwinds-vulnerability-update-resource-page

CISA:

https://us-cert.cisa.gov/ncas/alerts/aa20-352a

SolarWinds: Defense and Prevention

Image source: Government Technology



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/


```
rule CrowdStrike_SUNSPOT_01 : artifact stellarparticle sunspot {

    meta:
        copyright = "(c) 2021 CrowdStrike Inc."
        description = "Detects RC4 and AES key encryption material in SUNSPOT"

        version = "202101081448"
        last_modified = "2021-01-08"
        actor = "StellarParticle"
        malware_family = "SUNSPOT"

    strings:

        $key = {fc f3 2a 83 e5 f6 d0 24 a6 bf ce 88 30 c2 48 e7}
        $iv  = {81 8c 85 49 b9 00 06 78 0b e9 63 60 26 64 b2 da}

    condition:
        all of them and filesize < 32MB

}

rule CrowdStrike_SUNSPOT_02 : artifact stellarparticle sunspot
{

    meta:
        copyright = "(c) 2021 CrowdStrike Inc."
        description = "Detects mutex names in SUNSPOT"
        version = "202101081448"
        last_modified = "2021-01-08"
        actor = "StellarParticle"
        malware_family = "SUNSPOT"

    strings:
        $mutex_01 = "{12d61a41-4b74-7610-a4d8-3028d2f56395}" wide ascii
        $mutex_02 = "{56331e4d-76a3-0390-a7ee-567adf5836b7}" wide ascii

    condition:
        any of them and filesize < 10MB

}

rule CrowdStrike_SUNSPOT_03 : artifact logging stellarparticle sunspot

{

    meta:
        copyright = "(c) 2021 CrowdStrike Inc."
        description = "Detects log format lines in SUNSPOT"
        version = "202101081443"
        last_modified = "2021-01-08"
        actor = "StellarParticle"
        malware_family = "SUNSPOT"

    strings:
        $s01 = "[ERROR] ***Step1('%ls','%ls') fails with error %#x***\x0A" ascii
        $s02 = "[ERROR] Step2 fails\x0A" ascii
        $s03 = "[ERROR] Step3 fails\x0A" ascii
        $s04 = "[ERROR] Step4('%ls') fails\x0A" ascii
        $s05 = "[ERROR] Step5('%ls') fails\x0A" ascii
        $s06 = "[ERROR] Step6('%ls') fails\x0A" ascii
        $s07 = "[ERROR] Step7 fails\x0A" ascii
        $s08 = "[ERROR] Step8 fails\x0A" ascii
        $s09 = "[ERROR] Step9('%ls') fails\x0A" ascii
        $s10 = "[ERROR] Step10('%ls','%ls') fails with error %#x\x0A" ascii
        $s11 = "[ERROR] Step11('%ls') fails\x0A" ascii
        $s12 = "[ERROR] Step12('%ls','%ls') fails with error %#x\x0A" ascii
        $s13 = "[ERROR] Step30 fails\x0A" ascii
        $s14 = "[ERROR] Step14 fails with error %#x\x0A" ascii
        $s15 = "[ERROR] Step15 fails\x0A" ascii
        $s16 = "[ERROR] Step16 fails\x0A" ascii
        $s17 = "[%d] Step17 fails with error %#x\x0A" ascii
        $s18 = "[%d] Step18 fails with error %#x\x0A" ascii
        $s19 = "[ERROR] Step19 fails with error %#x\x0A" ascii
        $s20 = "[ERROR] Step20 fails\x0A" ascii
        $s21 = "[ERROR] Step21(%d,%s,%d) fails\x0A" ascii
        $s22 = "[ERROR] Step22 fails with error %#x\x0A" ascii
        $s23 = "[ERROR] Step23 fails with error %#x\x0A" ascii
        $s24 = "[%d] Solution directory: %ls\x0A" ascii
        $s25 = "[%d] %04d-%02d-%02d %02d:%02d:%02d:%03d %ls\x0A" ascii
        $s26 = "[%d] + '%s' " ascii

    condition:
        2 of them and filesize < 10MB
}}
```

SolarWinds: Formal Guidance and Recommendations

The following alerts, guidance and background information may prove helpful:

- **DHS: Emergency Directive 21-01**
  https://cyber.dhs.gov/ed/21-01/
- **DHS: Supplemental Guidance for ED 21-01 (version 1)**
  https://cyber.dhs.gov/ed/21-01/#supplemental-guidance
- **DHS: Supplemental Guidance for ED 21-01 (version 2)**
  https://cyber.dhs.gov/ed/21-01/older-supplemental-guidance/
- **DHS: Supplemental Guidance for ED 21-01 (version 3)**
  https://cyber.dhs.gov/ed/21-01/#supplemental-guidance-v3
- **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 Security Advisory**
  https://www.solarwinds.com/securityadvisory
- **Microsoft: Understanding "Solorigate"'s Identity IOCs - for Identity Vendors and their customers**
  https://techcommunity.microsoft.com/t5/azure-active-directory-identity/understanding-quot-solorigate-quot-s-identity-iocs-for-identity/ba-p/2007610
- **National Security Agency: Russian State-Sponsored Actors Exploiting Vulnerability in VMware WorkspaceONE Access Using Compromised Credentials**
  https://media.defense.gov/2020/Dec/07/2002547071/-1/-1/0/CSA_VMWARE%20ACCESS_U_OO_195076_20.PDF

The following tools may prove helpful:

- **CISA Sparrow:**
  https://github.com/cisagov/Sparrow
- **CrowdStrike Reporting Tool for Azure (CRT)**
  https://github.com/CrowdStrike/CRT
- **Using Microsoft 365 Defender to protect against Solorigate**
  https://www.microsoft.com/security/blog/2020/12/28/using-microsoft-365-defender-to-coordinate-protection-against-solorigate/

A managed service provider is the outsourcing of IT services:

Common Types of Managed Services

MANAGED NETWORKS & INFRASTRUCTURE	These services include managed IP VPNs, which are widely used for secure, high-performance and cost-effective networking. Also, managed hosting and storage services falls 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).
MANAGED SECURITY SERVICES	This type of managed service provides a broad range of solutions from patch management to antivirus, malware and other remote security updates.
MANAGED COMMUNICATIONS SERVICES	This managed service merges data, voice, and video services on the same IP network. It also can include a managed contact center that combines traditional call center features with intelligent IP call routing and integrates e-mail, phone, Web, instant messaging, fax, and other human or automated forms of customer contact.
MANAGED WIRELESS & MOBILE COMPUTING SERVICES	Like managed hosting and storage, this service enables wireless capabilities without the capital expenditure and implementation.
MANAGED PRINT SERVICES	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.
MANAGED SUPPORT SERVICES	This service handles traditional help desk responsibilities, including trouble ticketing for IT problems among employees and resolution mechanisms.
BUSINESS INTELLIGENCE/DATA ANALYTICS SERVICES	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.
MANAGED CLOUD INFRASTRUCTURE SERVICES	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, ecommerce 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 to role of "cloud orchestrator."
MANAGED SOFTWARE AS A SERVICE	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.

Image source: CompTIA

Managed Service Providers: Brief Review

Managed service providers:

- Pros:
  - Cost
  - Scalability
  - Technology
  - Expertise
- Cons:
  - Control
  - Flexibility/customization of services
  - Communication/management issues

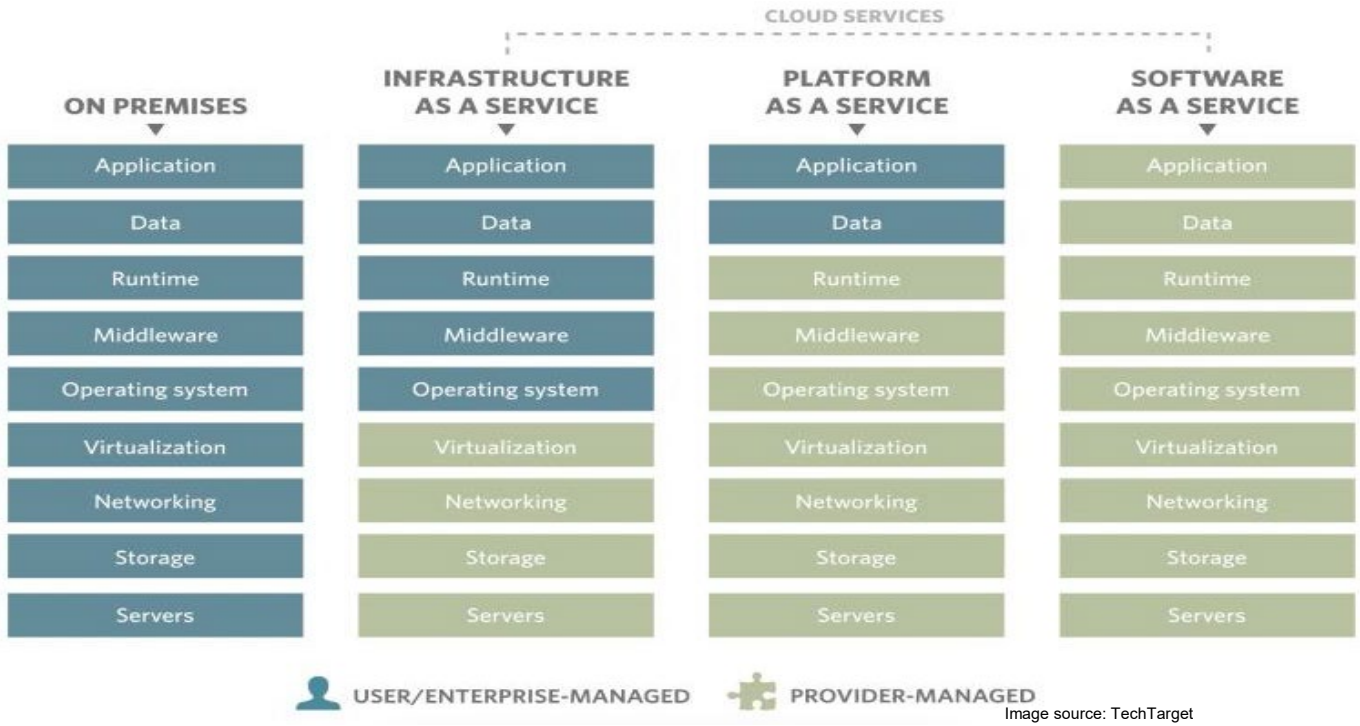
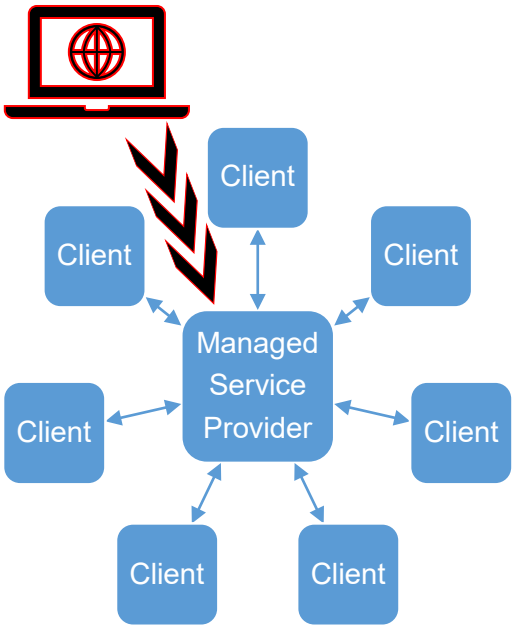
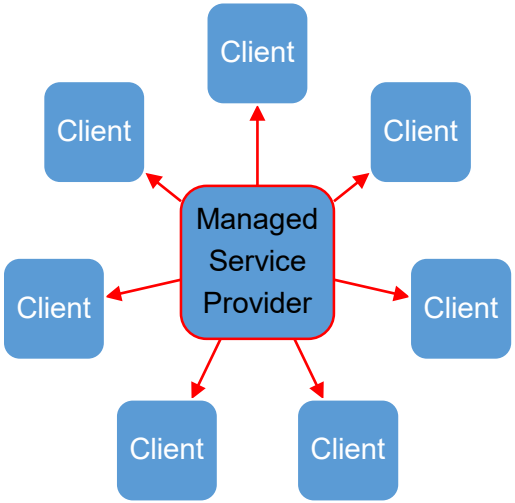


Image source: TechTarget

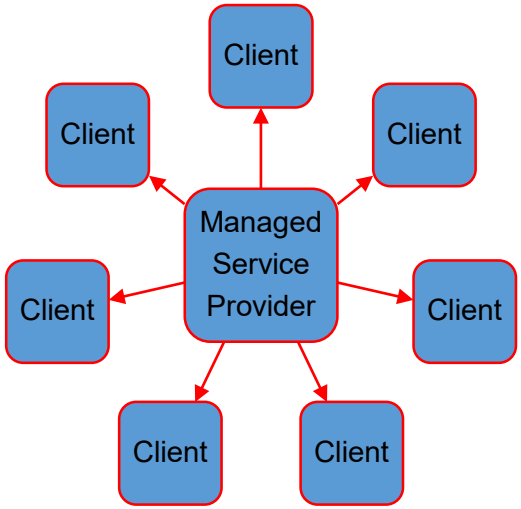
How does a managed service provider attack occur?



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:
  - Forbes: Leading Employer for Diversity
  - Fortune: 56 Companies Changing the World
  - 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

Blackbaud: Healthcare Organizations 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

Organization Name	Records breached
Medical center in Kansas	315,811
Hospital in Michigan	52,711
Hospital in Michigan	95,000
Hospital in North Carolina	Unknown
Hospital in California	39,881
Healthcare provider in Ohio	118,874
Health center in Pennsylvania	3,320,726
Healthcare network in Virginia	1,045,270
Health service provider in Maine	657,392
Health service provider in Washington State	300,000
Health service provider in Pennsylvania	60,595
Healthcare providers in Illinois	55,983

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:

DEFENSE/MITIGATION/COUNTERMEASURE	405(d) HICP REFERENCE
Provide social engineering and phishing training to employees.	[10.S.A], [1.M.D]
Develop and maintain policy on suspicious e-mails for end users; Ensure suspicious e-mails are reported.	[10.S.A], [10.M.A]
Ensure emails originating from outside the organization are automatically marked before received.	[1.S.A], [1.M.A]
Apply patches/updates immediately after release/testing; Develop/maintain patching program if necessary.	[7.S.A], [7.M.D]
Implement Intrusion Detection System (IDS); Keep signatures and rules updated.	[6.S.C], [6.M.C], [6.L.C]
Implement spam filters at the email gateways; Keep signatures and rules updated.	[1.S.A], [1.M.A]
Block suspicious IP addresses at the firewall; Keep firewall rules are updated.	[6.S.A], [6.M.A], [6.L.E]
Implement whitelisting technology to ensure that only authorized software is allowed to execute.	[2.S.A], [2.M.A], [2.L.E]
Implement access control based on the principal of least privilege.	[3.S.A], [3.M.A], [3.L.C]
Implement and maintain anti-malware solution.	[2.S.A], [2.M.A], [2.L.D]
Conduct system hardening to ensure proper configurations.	[7.S.A], [7.M.D]
Disable the use of SMBv1 (and all other vulnerable services and protocols) and require at least SMBv2.	[7.S.A], [7.M.D]

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
- **<u>Think in terms of distributed attacks when developing/implementing your risk management approach!</u>**

Reference Materials

References

Differentiate supply chain attacks (part of the compromise vice the target of the compromise)
https://healthsectorcouncil.org/09-20-2020-health-sector-publishes-guidance-on-supply-chain-cybersecurity-risk-management/

Modern Attacks Include Supply Chain "Hopping" and Reversing Agile Environments
https://www.infosecurity-magazine.com/news/attacks-hopping-reversing-agile/

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

In wake of SolarWinds and Vietnam, more supply chain attacks expected 2021
https://www.scmagazine.com/home/security-news/cyberattack/in-wake-of-solarwinds-and-vietnam-more-supply-chain-attacks-expected-2021/

Vietnam targeted in complex supply chain attack
https://www.zdnet.com/article/vietnam-targeted-in-complex-supply-chain-attack/

North Korean software supply chain attack targets stock investors
https://www.bleepingcomputer.com/news/security/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

References

The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies
https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

Managed Security Services Provider (MSSP) News: 24 December 2020
https://www.msspalert.com/cybersecurity-news/updates-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
https://blog.paloaltonetworks.com/2017/12/2018-predictions-recommendations-era-software-supply-chain-attacks-begun/

SolarWinds hackers have a clever way to bypass multi-factor authentication
https://arstechnica.com/information-technology/2020/12/solarwinds-hackers-have-a-clever-way-to-bypass-multi-factor-authentication/

~18,000 organizations downloaded backdoor planted by Cozy Bear hackers
https://arstechnica.com/information-technology/2020/12/18000-organizations-downloaded-backdoor-planted-by-cozy-bear-hackers/

DHS, State, NIH join list of federal agencies – now five – hacked in major Russian cyberespionage campaign
https://www.seattletimes.com/nation-world/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
https://blogs.microsoft.com/on-the-issues/2020/12/13/customers-protect-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
https://documentation.solarwinds.com/en/Success_Center/orionplatform/Content/Core-How-Orion-Works-sw1625.htm

FireEye, Microsoft create kill switch for SolarWinds backdoor
https://www.bleepingcomputer.com/news/security/fireeye-microsoft-create-kill-switch-for-solarwinds-backdoor/

Continue Clean-up of Compromised SolarWinds Software
https://www.tripwire.com/state-of-security/security-data-protection/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
https://www.washingtonpost.com/national-security/russia-is-behind-the-broad-ongoing-cyber-spy-campaign-against-the-us-government-and-private-sector-pompeo-says/2020/12/19/8c850cf0-41b3-11eb-8bc0-ae155bee4aff_story.html

Microsoft to quarantine compromised SolarWinds binaries tomorrow
https://www.bleepingcomputer.com/news/security/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
https://www.bleepingcomputer.com/news/security/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
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/

Sunburst: connecting the dots in the DNS requests
https://securelist.com/sunburst-connecting-the-dots-in-the-dns-requests/99862/

SolarWinds hackers breached US Treasury officials' email accounts
https://www.bleepingcomputer.com/news/security/solarwinds-hackers-breached-us-treasury-officials-email-accounts/

References

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
https://www.finance.senate.gov/ranking-members-news/wyden-statement-following-treasury-and-irs-briefing-on-solarwinds-hack

Russia's FireEye Hack Is a Statement—but Not a Catastrophe
https://www.wired.com/story/russia-fireeye-hack-statement-not-catastrophe/

SolarWinds Campaign Focuses Attention on 'Golden SAML' Attack Vector
https://www.darkreading.com/attacks-breaches/solarwinds-campaign-focuses-attention-on-golden-saml-attack-vector/d/d-id/1339794

UK privacy watchdog warns SolarWinds victims to report data breaches
https://www.bleepingcomputer.com/news/security/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
https://www.cyberscoop.com/solarwinds-white-house-national-security-council-emergency-meetings/

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

11/16/2020: Healthcare Supply Chain Security: Updated Guidance
https://healthsectorcouncil.org/11-16-2020-healthcare-supply-chain-security-updated-guidance/

References

Partial lists of organizations infected with Sunburst malware released online
https://www.zdnet.com/google-amp/article/partial-lists-of-organizations-infected-with-sunburst-malware-released-online/

NSA, CISA Warn of Attacks on Federated Authentication
https://www.darkreading.com/vulnerabilities---threats/advanced-threats/nsa-cisa-warn-of-attacks-on-federated-authentication/d/d-id/1339776

Massive Russian hack attack threatens national security and fuels disinformation warfare
https://news.yahoo.com/massive-russian-hack-attack-threatens-143009174.html

White House confirms cyberattack report on U.S. Treasury by foreign government
https://www.foxbusiness.com/technology/u-s-treasury-breached-by-hackers-backed-by-foreign-government-report

Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor
https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

Malicious Domain in SolarWinds Hack Turned into 'Killswitch'
https://krebsonsecurity.com/2020/12/malicious-domain-in-solarwinds-hack-turned-into-killswitch/

SolarWinds Hack Victims: From Tech Companies to a Hospital and University
https://www.wsj.com/articles/solarwinds-hack-victims-from-tech-companies-to-a-hospital-and-university-11608548402

Cisco, Intel, Deloitte Among Victims of SolarWinds Breach: Report
https://www.darkreading.com/threat-intelligence/cisco-intel-deloitte-among-victims-of-solarwinds-breach-report/d/d-id/133978

References

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
https://www.zdnet.com/article/partial-lists-of-organizations-infected-with-sunburst-malware-released-online/

Kevin Mandia: 50 Firms 'Genuinely Impacted' By SolarWinds Attack
https://www.crn.com/news/security/kevin-mandia-50-firms-genuinely-impacted-by-solarwinds-attack

SVR cyberespionage updates—other victims, avenues of approach. US AG calls out Moscow. Emotet's back. Big Tech vs. NSO Group.
https://thecyberwire.com/newsletters/daily-briefing/9/245

IT giants VMware, Cisco confirmed as victims of SolarWinds hack
https://www.itproportal.com/news/it-giants-vmware-cisco-confirmed-as-victims-of-solarwinds-hack/

Kremlin officially rejects involvement in US hacker attacks
https://en.mehrnews.com/news/167452/Kremlin-officially-rejects-involvement-in-US-hacker-attacks

Bear tracks all over the US Government's networks. Pandas and Kittens and Bears, oh my... Emotet's back. Spyware litigation. A few predictions.
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
https://www.tripwire.com/state-of-security/security-data-protection/continue-clean-up-of-compromised-solarwinds-software/

The List of Known SolarWinds Breach Victims Grows, as Do Attack Vectors
https://www.datacenterknowledge.com/security/list-known-solarwinds-breach-victims-grows-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
https://www.cisa.gov/news/2020/12/17/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
https://news.sophos.com/en-us/2020/12/21/how-sunburst-malware-does-defense-evasion/

References

Best Practice: Identifying And Mitigating The Impact Of Sunburst
https://blog.checkpoint.com/2020/12/21/best-practice-identifying-and-mitigating-the-impact-of-sunburst/

CISA releases CISA Insights and creates webpage on ongoing APT cyber activity
https://www.securitymagazine.com/articles/94232-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
https://www.cisa.gov/sites/default/files/publications/CISA%20Insights%20-%20What%20Every%20Leader%20Needs%20to%20Know%20About%20the%20Ongoing%20APT%20Cyber%20Activity%20-%20FINAL_508.pdf

SUPERNOVA SolarWinds .NET Webshell Analysis
https://www.guidepointsecurity.com/supernova-solarwinds-net-webshell-analysis/

Sunburst: Supply Chain Attack Targets SolarWinds Users
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/sunburst-supply-chain-attack-solarwinds

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
https://uk.reuters.com/article/uk-global-cyber-usa/suspected-russian-hackers-made-failed-attempt-to-breach-crowdstrike-company-says-idUKKBN28Y1BY

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
https://securityboulevard.com/2020/12/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
https://event.on24.com/eventRegistration/EventLobbyServlet?target=reg20.jsp&referrer=https%3A%2F%2Ft.co%2F&eventid=2942412&sessionid=1&key=783AEE47BD24CA13386B5C7AFC354433&regTag=&V2=false&sourcepage=register

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-5PuCl80

Microsoft has discovered yet more SolarWinds malware
https://www.techradar.com/news/microsoft-has-discovered-yet-more-malware-affecting-solarwinds-orion

The Sunburst attack, a second strain of malware and strengthening your security
https://www.cybertalk.org/2020/12/21/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
https://www.crn.com/news/security/top-treasury-email-accounts-exposed-in-solarwinds-hack-report?itc=refresh

CrowdStrike releases free Azure security tool after failed hack
https://www.bleepingcomputer.com/news/security/crowdstrike-releases-free-azure-security-tool-after-failed-hack/

CISA Releases Free Detection Tool for Azure/M365 Environment
https://us-cert.cisa.gov/ncas/current-activity/2020/12/24/cisa-releases-free-detection-tool-azurem365-environment

Russian hackers compromised Microsoft cloud customers through third party, putting emails & other data at risk
https://www.washingtonpost.com/national-security/russia-hack-microsoft-cloud/2020/12/24/dbfaa9c6-4590-11eb-975c-d17b8815a66d_story.html

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
https://www.reuters.com/article/global-cyber-usa-solarwinds/experts-who-wrestled-with-solarwinds-hackers-say-cleanup-could-take-months-or-longer-idINL1N2J31BN

SolarWinds Hackers "Impacting" State and Local Governments
https://www.infosecurity-magazine.com/news/solarwinds-hackers-impacting/

SolarWinds releases updated advisory for new SUPERNOVA malware
https://www.bleepingcomputer.com/news/security/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
https://www.csoonline.com/article/3601007/how-to-avoid-subdomain-takeover-in-azure-environments.html

SUNBURST, TEARDROP and the NetSec New Normal
https://research.checkpoint.com/2020/sunburst-teardrop-and-the-netsec-new-normal/

SolarWinds roundup: Fixes, new bad actors, and what the company knew
https://www.networkworld.com/article/3602090/solarwinds-roundup-fixes-new-bad-actors-and-what-the-company-knew.html

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
https://blog.shiftleft.io/visual-notes-solarwinds-supply-chain-compromise-using-sunburst-backdoor-detected-by-fireeye-561e097fff3c

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

Best Practice: Identifying And Mitigating The Impact Of Sunburst
https://blog.checkpoint.com/2020/12/21/best-practice-identifying-and-mitigating-the-impact-of-sunburst/

CISA releases CISA Insights and creates webpage on ongoing APT cyber activity
https://www.securitymagazine.com/articles/94232-cisa-releases-cisa-insights-and-creates-webpage-on-ongoing-apt-cyber-activity

References

50 orgs 'genuinely impacted' by SolarWinds hack, FireEye chief says
https://gcn.com/articles/2020/12/22/solarwinds-hack-impact.aspx

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

SolarWinds Orion API authentication bypass allows remote comand 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
https://www.tipranks.com/news/solarwinds-makes-fixes-to-address-supernova-attack-street-sees-34-upside/

Best Practice: Identifying And Mitigating The Impact Of Sunburst
https://blog.checkpoint.com/2020/12/21/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.
https://techcommunity.microsoft.com/t5/azure-active-directory-identity/understanding-quot-solorigate-quot-s-identity-iocs-for-identity/ba-p/2007610

Microsoft: Important steps for customers to protect themselves from recent nation-state cyberattacks
https://blogs.microsoft.com/on-the-issues/2020/12/13/customers-protect-nation-state-cyberattacks/

What Every Leader Needs to Know About the Ongoing APT Cyber Activity
https://www.cisa.gov/insights

References

CISA Releases Free Detection Tool for Azure/M365 Environment
https://us-cert.cisa.gov/ncas/current-activity/2020/12/24/cisa-releases-free-detection-tool-azurem365-environment

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

SolarWinds releases updated advisory for new SUPERNOVA malware
https://www.bleepingcomputer.com/news/security/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
https://www.schneier.com/blog/archives/2020/12/russias-solarwinds-attack.html

SolarWinds roundup: Fixes, new bad actors, and what the company knew
https://www.networkworld.com/article/3602090/solarwinds-roundup-fixes-new-bad-actors-and-what-the-company-knew.html

Using Microsoft 365 Defender to protect against Solorigate
https://www.microsoft.com/security/blog/2020/12/28/using-microsoft-365-defender-to-coordinate-protection-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.**

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

Contact

Health Sector Cybersecurity Coordination Center (HC3)

202-691-2110

HC3@HHS.GOV