April 2021

WHITE PAPER

STRATEGIC THREAT INTELLIGENCE: PREPARING FOR THE NEXT "*SOLARWINDS*" EVENT

H-ISAC™
HEALTH - ISAC

www.h-isac.org

American Hospital Association™
Advancing Health in America

www.aha.org

Introduction

As the impact of the SolarWinds incident is still being investigated and discussed, the American Hospital Association (AHA) and Health-ISAC collaborated on this strategic intelligence analysis to identify what other “SolarWinds” like issues might be lurking in enterprise networks. The paper is meant for all audiences, non-technical and technical, as we present strategic level decision elements that senior leaders including C-Suite Executives can use to help understand the risks involved with certain enterprise IT systems in their network environment. We then provide detailed technical analysis and recommendations for IT and information security teams to help address immediate concerns by providing tactical mitigations and recommendations. For our technical audience, this paper presents a detailed analysis of characteristics that allowed the SolarWinds incident to affect multiple industries, organizations, and systems.

The ability to extract the characteristics and features of SolarWinds could allow organizations to predict and hopefully prevent the next “SolarWinds”-like event in their enterprise environments.

SHARING SINCE 2010 H-ISAC™ HEALTH - ISAC

American Hospital Association™ Advancing Health in America

How Health-ISAC and AHA Work Together

The AHA and Health-ISAC have urged for more ways to improve cyber security in a global approach to defend against cyber threats. Hospitals and health systems, and the patients they care for every day, are heavily targeted by cyber adversaries, including sophisticated nation-states. Defenders have made great strides to protect their networks, secure patient data, preserve health care services’ efficient delivery and, most importantly, ensure patient safety. However, it cannot be done alone. Hospitals and health systems need more active support from the public and private sector to defend patients from cyber threats.

Health-ISAC and AHA partner in a variety of ways. Highlighting just a few examples regarding information sharing, Health-ISAC shares many threat and vulnerability reports with AHA for the benefit of their 5,000 member hospitals. AHA and Health-ISAC will continue to work together to ensure tactical threat and vulnerability intelligence is broadly shared with this community. Health-ISAC and AHA will also continue to collaborate on strategic threat analyses, much like this report, in the future.

Executive Summary

The SolarWinds incident that began to unfold in mid-December 2020 is yet another reminder of the on-going risks lurking in enterprise networks. SolarWinds is the company that makes the Orion platform which is used by tens of thousands of businesses globally to help manage their networks, systems, and information technology infrastructure. As Orion runs with privileged access to the assets it manages, the SolarWinds breach meant those enterprise assets could now easily be compromised by the adversary. It is these supply-chain dependencies and inherent trust models that must be carefully reviewed before, during and after any implementation to ensure unwanted risks are not introduced into the enterprise network.

As senior leaders responsible for overall risk management of your firm, you should be asking the right questions of your technical experts about new and existing technologies which provide broad access into your IT infrastructure, including access to data and sensitive information. Information security principles including least privileged access, network segmentation and on-going monitoring should be used in concert to minimize risk during implementation and production of enterprise management systems. What controls are in place? Establish and maintain a dynamic inventory process for all IT systems (you can't secure what you don't know about) and implement appropriate audit and control processes. Monitoring should also include establishing a baseline of "normal" network traffic and looking for anomalies outside that baseline for potential issues.

(continued on following page)

SHARING SINCE 2010 H-ISAC™ HEALTH - ISAC

Organizations should be active with their respective critical infrastructure Information Sharing & Analysis Center (ISAC). Health-ISAC, for example, shares timely threat intelligence, indicators of compromise (IOC), technical guidance, situational awareness, mitigation strategies and best practices. The ISAC also coordinates and collaborates on sector response. On Monday morning, December 14, 2020, just hours after the SolarWinds breach was announced, Health-ISAC alerted its members about the incident, provided an analysis including IOCs and detailed recommendations to address the issue. Health-ISAC also provided an Executive Summary PowerPoint that members could use internally within their organizations to explain to senior leadership what happened, the implications of the breach and what needed to be done to mitigate the compromise. Health-ISAC updated the advisory and communications in subsequent releases based on member feedback, especially from our Threat Intelligence Committee. The sharing was invaluable to the entire health sector.

Executive Summary *(continued)*

As part of the risk management process, you should also understand the types of sensitive data you have in your environment as it relates to customers, patients and your firm’s strategic priorities and intellectual property. Should there be a breach of your network, do you have an up-to-date inventory of data to understand the possible compromise exposures, including exposure to legal and regulatory risk? Could you determine what was stolen? Do you have an understanding of the vendors/third party suppliers you use so that when vulnerabilities arise you can assess risks? What is the future value of that data (ie, is it part of an R&D project to develop a new product, that if exposed, could provide another firm a competitive advantage or other sensitive data like patient information)? Are there future reputational, economic or national security implications because of the breach? These are just some of the questions you should be asking your internal subject matter experts.

American Hospital Association™

Advancing Health in America

The AHA, which represents over 5,000 hospitals and health systems and 43,000 individual members, understands that cyber risk is a now a top enterprise risk issue impacting not only data, but impacting patient care and safety. The AHA through its senior advisor for cybersecurity and risk, John Riggi, a former FBI cyber executive, continues to serve as a platform to collect, analyze and share cyber threat intelligence from the field, the government and Health-ISAC . During the SolarWinds breach, the AHA worked with all public and private partners to understand the scope of the breach, its impact and rapidly disseminate related technical and strategic threat information. In the realm of cyber defense, there is no competitive advantage between organizations. We all face the same cyber threats and the same potential consequences to data and to patients. Thus, the AHA strongly believes in the necessity of rapid and robust cyber threat information sharing - between organizations, sectors and the government in a truly “whole of nation” approach to cybersecurity.

Technical Analysis

In mid-December 2020, news of a major cyber security breach began to unfold. Victims from several US Government agencies, Microsoft and cyber security firm FireEye, were all impacted by the SolarWinds attacks. This sophisticated attack campaign likely also compromised multiple unnamed business systems and resources, occupied multiple days of news coverage, and instigated large-scale business responses still months later to mitigate the event.

Before the wide-spread coverage and analysis, malicious actors gained access to the build versions of the network monitoring software named Orion, designed by Texas-based company SolarWinds. Access to the Orion build version was possibly caused by a vulnerable Microsoft Office 365 account. The cause of this initial breach is still unknown, but could have possibly been due to complex phishing attacks, weak passwords or unsecure account hardening practices. The attackers then established a foothold in the software update publishing infrastructure somewhere before September 2019. Next, the malicious actors surreptitiously modified software updates provided by the SolarWinds corporation, which was then directly applied to legitimate users updating their Orion platform to the latest version.

The first known modification, occurring in October 2019, was merely a proof of concept. Once the proof had been established, the attackers spent December 2019 to February 2020 setting up a command-and-control (C2) infrastructure to further weaponize the supply-chain structure of the Orion update function. In March 2020, the attackers began to plant remote access tool malware into Orion updates, thereby effectively trojanizing them. Once weaponized, the update was sent to enterprise security administrators, who automatically applied the relevant security fixes, not knowing the update was malicious.

The malware would stay dormant from 12 to 14 days before attempting to communicate with one or more of several C2 servers, trying to mimic and masquerade as legitimate Orion outbound traffic sent back to SolarWinds. If the outbound traffic was able to contact one of the C2 servers, an alert would be sent to the attackers of a successful malware deployment and would offer the attackers a backdoor that the attackers could choose to utilize if they wished to exploit the system further. The SolarWinds Orion Platform incident is certainly one of the most significant cyber security compromises from the past few years, especially because its complex supply chain exploitation and propagation. But this event is not the only cyber incident to have the identical, distinguishable characteristics that made the attack so meaningful and so successful.

SolarWinds – Characteristics Broken Down

In order to first compare SolarWinds characteristics to similar events in the past, the underlying attributes must be identified. At its core, the reason why the SolarWinds incident could compromise so many organizations around the globe relies on the simplicity and wide scale adoption of managed services for enterprise organizations. Managed service providers and software, products that can control and manage multiple systems and software from a centralize service, offer simplicity when onboarding new systems and a scalable growth mechanism for managing dynamic business systems. Their rise in popularity over the past 15 plus years, and the subsequent security incidents, reveals three distinguishable characteristics that makes these enterprise software systems such appealing targets to malicious actors:

- The centralized system easily controls multiple subsystems, networks, or products, requiring little interaction or no activation from the controlled system.
- The system possesses an undisclosed, unpatched, or unknown opening that attackers can exploit for a degree of administrative control.
- The exploited opening of the centralized product can affect, in either a limited or total ability, the subsystem it controls.

These first characteristics exist for several reasons, mainly for ease-of-use and onboarding control of systems. The second characteristic, the undisclosed, unpatched, or unknown opening, is also uncontrollable, but can be mitigated by vulnerability testing, quality assurance, least privilege operations and Privileged User Monitoring and Access control discipline. The last characteristic lies in the relationship between the controlling software and the controlled devices/products. The SolarWinds attackers exploited all of the above characteristics to achieve their attack goals -- and we discuss four more incidents in this document where attackers exploited the same factors -- the 2003 HP OpenView vulnerability, WannaCry (2017), Petya/NotPetya (2017) and the 2021 SAP Solution Manger incident.

HP OpenView (2009)

When applying this threat model to the 2009 HP OpenView incident, and comparing it to SolarWinds, all three characteristics match. HP OpenView is a now legacy system management and network monitoring software system which was used to manage a variety of HP and non-HP affiliated devices, such as virtual machines, servers, databases, and networking devices, thus matching the first characteristic. Two undisclosed vulnerabilities, designated CVE-2009-0920 and CVE-2009-0921, allowed remote attackers to execute remote malicious code via specially crafted HTTP requests on the vulnerable system, satisfying the second requirement. The last shared characteristic is the combination of the previous two points, where the utilization of CVE-2009-0920 and CVE-2009-0921 is paired with a vulnerable HP OpenView to cause significant damage to any connected service or device. At the time, the combination of CVE-2009-0920 and CVE-2009-0921 potentially affected millions of organizations utilizing HP OpenView in business environments, and numerous business entities appropriately responded, much like they did in the current SolarWinds incident.

WannaCry (2017)

Probably one of the most significant vulnerabilities to ever affect the online connected ecosystem, EternalBlue, an exploit reportedly discovered by the United States National Security Agency (NSA) for older Windows operating systems versions, affected millions of outdated and unpatched systems. While coverage and analysis of this vulnerability was widespread, systems that were unavailable or otherwise unable to upgrade legacy Windows systems were subject to the weaponization of the EternalBlue vulnerability through the WannaCry ransomware, which has been attributed to the North Korean government.

By using WannaCry ransomware on central administrative systems, such as a domain controller or server, this incident satisfies the first and second characteristics, by having a centralized system that controls a variety of services directly impacted by an unpatched vulnerability. The combination of these two components directly leads to the third and final characteristic, which could potentially cause large-scale destruction and disruption of critical systems not only in the healthcare sector, but any system worldwide that had failed to upgrade its legacy Windows systems

Petya and NotPetya (2017)

A continuation of the EternalBlue vulnerability described in the WannaCry section above, Russian-backed state actors utilized the legacy Windows flaw to encrypt the boot records of systems, centralized services, and other critical machines across a wide variety of business sectors. While the original Petya malware variant was primarily used to target Ukrainian entities and worldwide legacy systems, another variant, deemed NotPetya, utilized different keys for encryption and possessed a unique reboot style different from its predecessor. The discovery and investigation of NotPetya found that a Ukraine-based tax accounting software firm named Intellect Service, which developed the M.E.Doc tax accounting software was corrupted by Russian nation state actors. M.E.Doc had more than 400,000 customers across Ukraine, representing about 90% of the country's domestic firms and prior to the attack was installed on an estimated one million computers in Ukraine.

By abusing the automatic update features of M.E.Doc, state actors pushed a corrupted update that included the newly discovered NotPetya variant. The attack affected systems primarily in Ukraine, but also impacted entities across the globe, with estimated damages caused by the attack measured to be over $10 billion (US). This incident remains highly notable because of the similarities when compared to the aforementioned SolarWinds attack, which utilized a compromised updater to spread malware across a variety of business systems across the globe. SolarWinds' methodologies, such as its techniques, tactics and procedures, might have either been inspired by, or directly influenced by, the initial attack and intrusion vector of the Russian NotPetya malware strain.

The impacts across the globe – while perhaps unintended by the attackers – left many organizations reeling from the attack. Unaffected entities that were, in fact, not vulnerable to the Petya and NotPetya strains were indirectly affected by vulnerable third-party services providers. For example, a large medical operation outsourcer was compromised by Petya and NotPetya-enabled attacks, and healthcare providers globally that relied on that service provider were operationally affected by the loss of service.

With both malware variants, centralized medical management systems were impacted across the globe, as these complex systems provided lifesaving services that could not have been deactivated or upgraded to the most current versions of the Windows operating system. These centralized, targeted medical systems, which affected multiple medical devices across hospitals and health centers, were directly impacted by an unpatched and weaponized vulnerability, which satisfies the first, second and third characteristics of the SolarWinds shared-characteristics model.

(continued on following page)

SAP Solution Manager (SolMan) (2021)

Another example to apply the SolarWinds exploitation model is to the 2021 SAP Solution Manager incident. Solution Manager (SolMan) is a widely used software module created by SAP that provides integrated content, methodologies, and tools to implement, operate, monitor, and support enterprises' SAP and, to a limited extent, non-SAP solutions.

SolMan closely resembles HP OpenView, has properties of SolarWinds Orion products, and satisfies the first exploitation characteristic, by easily controlling multiple subsystems. A discovered vulnerability, tracked as CVE-2020-6207, was assessed a CVSS base score of 10.0, the highest severity rating available. The issue was addressed by SAP as part of its March 2020 updates, but a public release of a proof-of-concept by security researchers could allow attackers to target unpatched systems. The unpatched opening meets the second distinguishable characteristic. While not unknown, undiscovered, or left unpatched by developers, a lack of coordinated response by unaware security and system administrators allowed for numerous SAP-enabled systems to be left open for attackers to exploit. A successful exploitation of the vulnerability would allow a remote unauthenticated actor to execute highly privileged administrative tasks in the connected SAP Solution Manager Diagnostics toolset used to analyze and monitor SAP systems via SolMan. The attack could shut down any connected SAP system, delete any data stored on connected devices, and read and extract any logs stored on connected systems. These capabilities closely resemble achieved capabilities via a SolarWinds Orion compromise, and also satisfies the third characteristic of the overall threat model outlined earlier.

Analysis: Summing It Up

As demonstrated by several examples, the SolarWinds incident -- still in the news three months after its discovery -- was not the first interconnected software failure that affects the devices it controls or has access to. Centralized administrative software and unknown vulnerabilities have, and always will be, a potential central point of compromise for system and security administrators. The rise and continued usage of managed service providers and software allows small and large businesses limitless scalability and easy onboarding. Their continued use and development represent a risk as these software systems create new opportunities for attackers and security researchers to find new openings in trusted enterprise software systems.

In conclusion, the SolarWinds incident is not the first incident of this type to occur, multiple types of centralized administrative software have been compromised in the past, by either motivated nation state actors, such as Russia, China, North Korea or Iran or by public disclosure of critical vulnerabilities. The rise of managed service providers into critical businesses has expedited the severity of the situation and will also continue to be compromised by the same attack vectors we described in this paper. Administrators should consider their critical data dependencies, business functions, and business relationships with these third-party firms, as their past history of central failure and data compromise will likely continue in the future and will directly and negatively impact an organization if an incident were to occur. The best countermeasure to ensure organizational security and protection from the next SolarWinds level event is the application of proper patch management, vulnerability awareness, and the use of reputable threat intelligence. With the analysis and recommendations provided, healthcare organizations should be able to utilize actionable threat intelligence and remain alert to potential vulnerabilities, thereby effectively preventing, or at least minimizing, the impacts from the next “SolarWinds-type” event.

Technical Recommendations

Simply put, the best ways to mitigate the next SolarWinds-level incident are having vulnerability awareness, applying proper patch application and management, implementing least privilege access, deploying Privileged User Monitoring & Access Control functions, and having access to reputable threat intelligence.

Software developers of centralized administrative software have, and always should, responsibly disclose actual or potential vulnerabilities and security breaches. The software vendors should respond with an appropriate patch or remediation in a timely, critical, short period. All parties in the examples and incidents listed previously disclosed their vulnerabilities or breaches publicly, openly explained the technical details and methodologies that allowed for success exploitation, and subsequently released a patch or update which mitigated the issues. Security and systems administrators must be aware of all potential openings via conducting proper and regular vulnerability scanning, testing and implementing patches across systems and continuing to verify that security controls remain effective against potential attackers.

In the case of a SolarWinds-level event, security administrators should also be aware of third-party recommendations and security practices that would help augment their traditional security infrastructure and development lifecycle. As SolarWinds impacted multiple sectors and organizations, third-party entities offered services, techniques, tactics, and procedures to help support and prevent future breaches utilizing this supply chain attack methodology. Microsoft released CodeQL queries to the general public, helping to mitigate potential damage to all potentially impacted developers utilizing a development rollout structure similar to the SolarWinds Orion platform. Using these queries, software developers can scan their source codebase for functionality or syntactic code elements that match those used by the malicious implants from the SolarWinds attack.

Security systems and administrators, though, cannot predict the occurrence of an unknown zero-day affecting their centralized administrative software, which leads to another area that organizations can use to mitigate the next SolarWinds-level event, having access to meaningful threat intelligence. Reputable and timely threat intelligence allows administrators and information security staff to become aware of urgent zero days discovered, potential or ongoing nation state campaigns, and direct threats that can affect their centralized administrative software that they would otherwise be unaware of. By using reliable threat intelligence, organizations can take action in their own environments to remediate vulnerabilities, implement countermeasures and other recommendations to minimize the likelihood of an attack.

Recommendations from Health-ISAC and AHA

- Continue to review and monitor Common Vulnerabilities & Exposures (CVEs) along with their criticality to ensure appropriate priorities are applied to software patch management of internal systems and satellite products of centralized administrative software.
  - Immediate testing of the patch and implementation where applicable.
  - Continuous review of current common vulnerabilities and exposures to infrastructure to reduce organizational attack surface.
- Administrators should identify and consider their critical data dependencies and business relationships with third-party firms who operate centralized administrative software in their environment.
  - Utilize a least access-privilege approach, giving only the necessary data and privileges that are needed to operate a service, thereby limiting potential openings for attackers to exploit.
    - When managing users who have elevated permissions and access to critical resources within your business environment, mandatory activation of two, or multi-factor authentication remains a top priority. Account access should also be immediately terminated upon the employee leaving the organization.
  - Use internal cyber security "hunt" teams to identify enterprise systems that meet the exploitation characteristics described above.
- Utilize the actionable threat intelligence disseminated from Health-ISAC, AHA and other threat intelligence sources.
  - Access to threat intelligence reports should be analyzed and potentially acted upon in a timely matter.
  - Communication between disseminators and recipients of threat intelligence should be maintained for familiarization, feedback and response, potential collaboration, and openness.
- Identify appropriate and known communications channels such as IP addresses and ports that such critical software and services should be communicating over and use that information to develop a baseline of what can be considered normal activity. Continuously monitor and design alerts for any deviation in communications from known communications channels.

(continued on following page)

Recommendations from Health-ISAC and AHA *(continued)*

Strategic Risk Management Considerations:

- Identify mission critical third party software, solutions and services utilized by the organization.
- Risk categorize and risk rank based upon scope of access to networks, volume and sensitivity of data.
- Risk rank based upon criticality to operations, revenue capture and most importantly, impact to patient care and safety.
- Utilize a vendor risk management program which incorporates cybersecurity, legal, compliance, clinical, finance and operations teams to assess risk in these types of mission critical third party, enterprise level applications.
- Ensure cybersecurity teams are involved in the scoping, purchase and acquisition of new technologies and have conducted appropriate cybersecurity due diligence on the product or service and the business associate organization.
- Develop business associate agreements which include and scale cybersecurity requirements proportionally with the risk ranking of the business associate organization and service being provided.
- Require business associates to notify within 72 hours of the discovery of any vulnerability, breach or compromise or which has the potential to impact the confidentiality, integrity and availability of your data, and or their services.
- Include cybersecurity insurance requirements in business associate agreements which scale proportionally with the identified risk ranking of the business associate.

Resources

- NIST: CVE-2003-0746: Various Distributed Computing Environment (DCE) for HP OpenView
- Network World: HP Patches OpenView Vulnerabilities
- Health-ISAC: SAP Solution Manager Flaw Weaponized with Proof of Concept Available
- Core Security: HP OpenView Buffer Overflows Advisory ID Internal CORE-2009-0122
- ZDNet: Microsoft: Petya Ransomware Attacks Were Spread by Hacked Software Updater
- Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients
- Microsoft Shares CodeQL Queries to Scan Code for SolarWinds-Like Implants
- SolarGate CodeQl Queries Github
- Microsoft Blog: Turning the Page on Solorigate and Opening the Next Chapter for the Security Community
- CISA Alert (AA20-352A) Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations
- CISA Issues Emergency Directive to Mitigate the Compromise of Solarwinds Orion Network Management Products
- DHS Emergency Directive 21-01 Mitigate SolarWinds Orion Code Compromise
- Health-ISAC: SolarWinds Breach Attributed to Latest US Agency Attacks
- Health-ISAC Cyber Threat Level Raised to Yellow (Elevated)

Conclusion

As we have described in this paper, the December 2020 SolarWinds incident was not the first and surely will not be the last trusted enterprise software solution to be leveraged in a complex global cyber-attack.

What is truly needed is close cooperation between governments, the healthcare sector and all critical infrastructure globally via a formal exchange of cyber threat information and combined cyber defenses – to create a truly global approach.

We urge organizations to use the strategic and tactical issues discussed in this paper as considerations for all trusted systems used, or planning to be used, in your environment.

As this paper was going through final editing, news broke of a major Microsoft Exchange compromise that has impacted hundreds of thousands of organizations globally. Researchers believe that four zero-day vulnerabilities were being actively exploited by Chinese nation-state actors, with other malicious cyber actors suspected as well, including ransomware groups. Exchange Servers, the crown jewel of espionage targeting, are the key to email across many enterprise networks. The ramifications of a Microsoft Exchange server being breached can be catastrophic for a business. While the Exchange compromise is extremely serious, it does not meet the three characteristics we discussed for puposes of this paper that make enterprise management systems an attractive target for threat actors.

We welcome your feedback and suggestions regarding this paper. Please contact the Health-ISAC Threat Operations Center via email at toc@h-isac.org or John Riggi, AHA senior advisor for cybersecurity and risk, at jriggi@aha.org

H-ISAC™
HEALTH - ISAC

www.h-isac.org

American Hospital Association™
Advancing Health in America

www.aha.org