IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 7, July 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307134|

The Weakest Link: A Case Study of the Solar Winds Cyber Attack

Varadharaj Varadhan Krishnan

Independent Researcher, Washington, USA

ABSTRACT: The SolarWinds cyberattack of 2020 is one of the most sophisticated and wide-reaching supply chain attacks in history. It served as a stark demonstration of the vulnerabilities inherent within software supply chains and its profound implications. This paper presents a comprehensive analysis of the SolarWinds security incident, examining the sequence of events, the tactics, techniques, and procedures (TTPs) employed by the attackers, and the subsequent global response. The paper also discusses the significant impact on numerous high-profile government and private sector entities and the pressing need for enhanced cybersecurity measures. By doing a thorough exploration of the incident and technical analysis the paper aims to actionable insights that any organizations can use to reinforce their defenses against similar future threats. This case study sheds light on the details of the SolarWinds attack and the importance of broader supply chain security.

KEYWORDS: SolarWinds, Cybersecurity, Supply Chain Attack, Solarigate, Nobelium, Suburst.

I. INTRODUCTION

SolarWinds, is a U.S. based software company that develops software for large enterprises to manage their computer networks, systems, and IT infrastructure. One of its flagship products, the SolarWinds Orion Platform, is widely used across various sectors for infrastructure monitoring and management, primarily manage IT operations across on-premises, hybrid, and SaaS environments. In March 2020, a routine software update of the SolarWinds Orion management platform became the conduit for one of the most sophisticated cyberattacks in history. Dubbed as "Solorigate" by Microsoft and known as "SUNBURST" from FireEye's investigations, this attack was facilitated through a compromised software update that installed a malicious code library into the Orion platform. This code created a backdoor for hackers into the systems of approximately 18,000 organizations worldwide, including top-tier government agencies and Fortune 500 companies. The entities impacted include, but are not limited to, the Pentagon, the U.S. Departments of Homeland Security, State, and Energy, as well as private sector giants like Microsoft, Cisco, and Intel. This paper will delve into the details of this critical capturing the sequence of events, the tactics, techniques, and procedures (TTPs) used by the attackers, and the overall implications the attack. This study will dissect the events that led up to the incident, discovery and global response and offer actionable insights that can be used by organizations to improve their defenses against similar future threats. Through this case study, the paper aims to highlight the significance of software supply chain security and how something that's has been discussed theoretically for many years has become urgent problem globally. The documented lessons from the SolarWinds incident will serve as a reminder and a wakeup call for cybersecurity communities globally to enhance software supply chain security posture.

.

II. SOFTWARE SUPPLY CHAIN ATTACK (SSCA)

ENISA defines SSCA as "a compromise of a particular asset, e.g. a software provider's infrastructure and commercial software, with the aim to indirectly damage a certain target or targets, e.g. the software provider's clients." In other words, a Software Supply Chain Attack refers to activity targeting the software supply chain, aiming to compromise and introduce vulnerabilities or malicious elements into the software development and distribution process. This attack capitalizes on the interconnected and often complex network of processes, tools, and entities involved in creating and delivering software. Figure 1 shows a simple illustration of an SSCA.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307134|

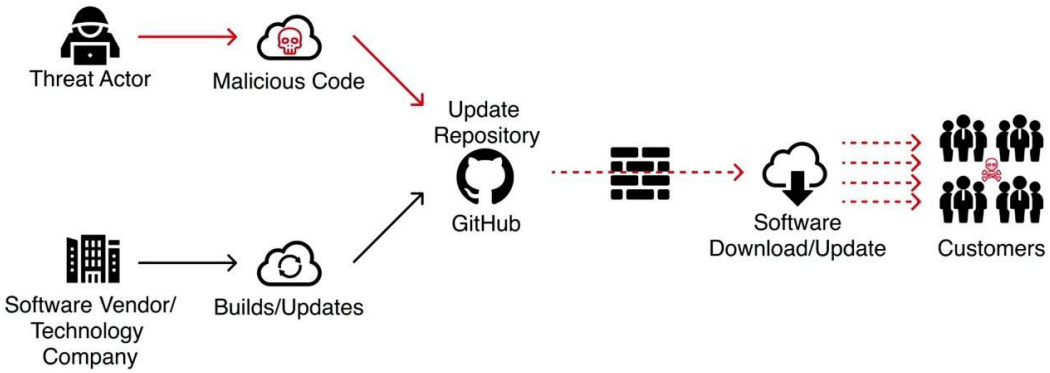

Figure 1 Anatomy of a software supply chain attack

As depicted in the illustration, SSCA typically follow a multi-stage process where the threat actor first inserts malicious code into the software build or update process managed by a software vendor. The initial step involves a threat actor, who may be an external or an insider, developing malicious code designed to compromise the software's functionality, steal data, or gain unauthorized access to network resources. This malicious code is then introduced into the software's codebase, often through manipulation of the software development tools or direct modification of source code. Once the malicious code is embedded within the software, the compromised build is then pushed to becomes part of the software updates or new builds that are distributed to customers. Unsuspecting customers download and install these updates, unknowingly executing the malicious code within their own IT environments. This attack vector is dangerous because it exploits the trust relationship between software vendors and their customers. Users generally assume software updates and patches are safe to install, given that they are directly provided by the vendor. However, once a software supply chain is compromised, every customer that update or installs the affected software inadvertently becomes part of the attack surface.

III. THE INCIDENT

On 13th Dec 2020, in a report published by FireEye, it said, it identified a significant global intrusion campaign designated as UNC2452, involving a sophisticated supply chain attack. They disclosed that the attack was centered around the distribution of a trojanized update for SolarWinds Orion business software, through a malicious component named *SolarWinds.Orion.Core.BusinessLayer.dll*. This component was engineered to act as a backdoor, facilitating covert communications with third-party servers using HTTP, mimicking normal SolarWinds API communications. The Solarigate campaigns was initiated in early Spring 2020, attacker targeted a diverse array of public and private organizations worldwide, spanning sectors such as government, technology, telecom, consulting, and extraction industries across North America, Europe, Asia, and the Middle East.

The attackers employed the SUNBURST backdoor to remain dormant for up to two weeks before activating to execute commands, transfer files, gather system profiles, and even reboot systems while cleverly disguising its activities within legitimate SolarWinds traffic. The attackers were sophisticated and created custom malwares that avoided detection by using advanced evasion techniques. Microsoft initially referred to the threat actor responsible for the SolarWinds intrusion as 'Solorigate'. However, to emphasize the group more accurately behind these sophisticated cyberattacks, the Microsoft Threat Intelligence Center (MSTIC) renamed the actor as NOBELIUM. The entire campaign including the SUNBURST backdoor, TEARDROP malware, and other related malicious components were attributed back to NOBELIUM threat actor.

Sep 2019	Attacker accessed SolarWinds network and compromised Orion product development environment and injects Sunburst malware.
Feb 2020	Sunburst (Trojanized version of a digitally signed SolarWinds Orion plugin) compiled and deployed for March update.
Jun 2020	Attacker removes infrastructure to compile and inject malware to avoid detection.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307134|

Dec 2020	FireEye detects anomalous user login and traces it back to Sunburst. Microsoft, FireEye and Solarwinds worked on publishing detection signals and patched were released.
Jan 2021	Additional malwares Teardrop, Sunspot, and Raindrop detected and published.
Feb 2021	A second of round attacker activity detected and additional Orion vulnerabilities published.

Table 1 Incident Timeline

.

IV. MALWARES USED

When the SolarWinds incident was first uncovered, the primary mechanism of breach was identified as a malicious backdoor known as Sunburst. However, it soon became clear that Sunburst was not working alone. Other malware such as Teardrop, Sunspot, and Raindrop also played significant roles in this complex cyber intrusion.

Teardrop: Further analysis by FireEye revealed Teardrop, a previously unrecognized malware, deployed through the Sunburst backdoor. Unlike earlier malware, Teardrop showed no similarities in its code to previously identified threats. Masquerading as a benign JPG file named "gracious_truth.jpg," this memory only dropper was designed for covert network infiltration, seamlessly delivering, and executing a tailored Cobalt Strike Beacon. This allowed it to mimic various sophisticated cyber threats and execute actions within the compromised network.

Sunspot: CrowdStrike's research shed light on Sunspot, the malware responsible for initially facilitating the Sunburst insertion into SolarWinds' software. In September 2019, Sunspot was meticulously implanted to monitor and modify the Orion product's build process undetected, inserting the Sunburst backdoor.

Raindrop: Discovered by Broadcom's Symantec division, Raindrop was another variant involved in the SolarWinds breach. It acted as a loader with capabilities similar to Teardrop. However, unlike Teardrop, Raindrop was not directly deployed by Sunburst. Symantec's findings showed it spreaded across networked computers via the management software, using PowerShell commands to propagate itself further, and configuring network communications via server message block (SMB).

V. ATTACKER UNIQUE BEHAVIOURS

After the revelation of Solorigate, in an in-depth analysis, Microsoft detailed the operational security methods used during the Sunburst, Teardrop, and Raindrop attacks, which involved:

- Camouflaging malicious files within directories by mimicking existing file names.
- Strategically enabling and disabling event logging to evade detection.
- Modifying firewall rules to facilitate the transmission of sensitive data.
- Executing lateral movements with extreme caution.
- Employing techniques like DLL-implant obfuscation to hide their tracks.

A notable target within the SolarWinds breach was Microsoft 365. According to FireEye's analysis, the attackers employed specific tactics against Microsoft services, including:

- Compromising the AD FS token-signing certificate to generate fraudulent tokens.
- Altering Azure AD trusted domains to establish attacker-controlled identity providers.
- Capturing credentials of users with high privileges linked to Microsoft 365
- Integrating backdoors within Microsoft 365 systems to maintain remote access.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307134|

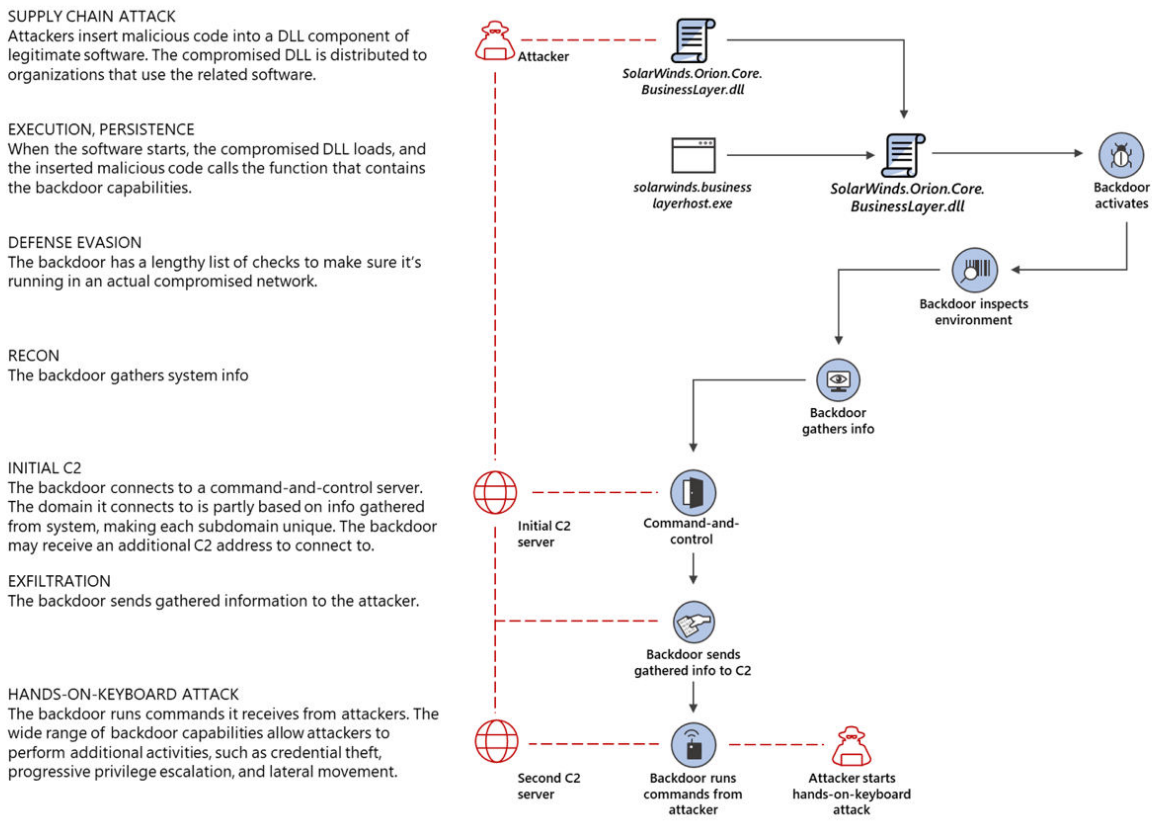

Figure 2 SolarWinds Attack Anatomy

Initial Access

The exact method by which the backdoor code was integrated into SolarWinds' library remains unclear. Crowdstrike's extensive research showed that the Sunspot malware was used to compromise the Orion platform build environment. With the help of the Sunspot malware, the attacker was able to embed malicious code into a legitimate library named SolarWinds.Orion.Core.BusinessLayer.dll. This compromised library was then disseminated across various networks via automatic update mechanisms.

Execution

During the update process of the SolarWinds application, the embedded malicious code within the SolarWinds.Orion.Core.BusinessLayer.dll library is executed prior to any legitimate code. This early execution misleads organizations into believing that the update is proceeding normally and that there is no malicious activity. To further evade detection, the attackers compromised libraries that were signed with the digital certificates of the target companies. Microsoft has since revoked these compromised certificates to prevent further misuse. Details of one such certificate include:

Signer: "Solarwinds Worldwide, LLC"
SignerHash: "47d92d49e6f7f296260da1af355f941eb25360c4"

Post-installation, the malicious DLL is loaded from the SolarWinds application's installation directory. Subsequently, the malware is set up as a Windows service and as a DLL file, residing in variable paths such as:

Standard Installation Path: %PROGRAMFILES%\SolarWinds\Orion\SolarWinds.Orion.Core.BusinessLayer.dll

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307134|

.NET Assembly Cache Path (when compiled): %WINDIR%\System32\config\systemprofile\AppData\Local\assembly\tmp<VARIES>\SolarWinds.Orion.Core.BusinessLayer.dll

Microsoft's security researchers have reported that this malicious code becomes active when run under the process context of SolarWinds.BusinessLayerHost.exe. This targeted execution strategy is part of the attackers' method to remain undetected while establishing a foothold within the network.

Command-and-control (C2)

The C2 mechanism in the SolarWinds attack was a sophisticated setup utilizing a Domain Generation Algorithm (DGA) to create and resolve subdomains of avsvmcloud[.]com for command-and-control operations. The DGA was initialized by cryptographic helpers, generating subdomains by encoding the victim's user ID and local machine domain name. These dynamically created subdomains allowed the attackers to adjust their targeting and control mechanisms discretely. To maintain stealth, the malware scanned for and identified security analysis tools and antivirus engines using hashed process, service name, and driver path listings. These were checked against a hardcoded blocklist; if any block listed items were detected, the update routine would halt, and the malware would attempt to execute again later. This evasion tactic also extended to disabling block listed services by altering registry entries, effectively suppressing potential alerts.

For network communication control, the malware performed connectivity checks and then proceeded to generate domains at random intervals. If the resolved IP addresses for these domains fell within certain specified ranges, the malware would deactivate, updating its configuration to prevent further execution. Successful domain resolution led to the spawning of a new HTTP communication thread, which handled all data transmissions using HTTP GET or POST requests. The data payloads, often containing detailed operational commands and structured in JSON format, were meticulously crafted to mimic benign network traffic. These payloads included detailed timestamps, event types, and encoded messages, which were camouflaged within HTTP response bodies that superficially appeared to be related to benign .NET assembly XML data. The use of steganography in HTTP responses, hiding command data within GUID and HEX strings shows the level of sophistication in the malware design and execution strategy by NOBELIUM.

Key Actions

In the Microsoft 365 environment, attackers achieved their objectives by gaining administrative access through two main methods: using compromised privileged account credentials or by forging SAML tokens with compromised SAML token signing certificates. In instances where SAML token signing certificates were compromised, the precise methods of access varied. Some confirmed breaches involved the use of common hacking tools to infiltrate databases supporting the SAML federation server, utilizing administrative and remote execution privileges. In other situations, attackers gained administrative privileges via service account credentials or by exploiting vulnerabilities in ADFS servers. Once in possession of a SAML token signing certificate, attackers forged SAML tokens to include any claims and set any desired validity period. These forged tokens were then used to authenticate and gain access to various resources that trust the SAML framework, including creating tokens that impersonate highly privileged accounts within Azure AD.

Attackers were able to gain administrative privileges in Azure AD using compromised credentials, especially in scenarios where the accounts were not secured with multi-factor authentication. With such access, the attackers conducted various malicious activities leveraging these privileges, which included establishing long-term access and extracting significant amounts of data.

Persistence or Long-Term Access

Once the attackers established a strong presence within the on-premises environment, they proceeded to manipulate Azure Active Directory settings to secure long-term access. The attackers added new federation trusts or altered the properties of existing ones within Azure Active Directory. These modifications allowed the trusts to accept tokens that were signed with certificates controlled by the attackers, thereby authenticating malicious activities as legitimate operations. In addition to manipulating federation trusts, the attackers added credential such as x509 keys or password credentials to existing OAuth Applications or Service Principals. The applications they target had typically permissions

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307134|

like Mail.Read or Mail.ReadWrite, which enabled the reading of mail content from Exchange Online via Microsoft Graph or Outlook REST APIs.

MITRE ATT&CK Techniques Observed

ID	Description
T1012	Query Registry
T1027	Obfuscated Files or Information
T1057	Process Discovery
T1070.004	File Deletion
T1071.001	Web Protocols
T1071.004	Application Layer Protocol: DNS
T1083	File and Directory Discovery
T1105	Ingress Tool Transfer
T1132.001	Standard Encoding
T1195.002	Compromise Software Supply Chain
T1518	Software Discovery
T1518.001	Security Software Discovery
T1543.003	Windows Service
T1553.002	Code Signing
T1568.002	Domain Generation Algorithms
T1569.002	Service Execution
T1584	Compromise Infrastructure

Table 2 MITRE ATT&CK Techniques Observed

Recommended Security Posture Improvements

Blocking Command and Control (C2) Traffic: Organizations should implement measures to block all known C2 endpoints using their network infrastructure to malicious communications going out and enabling threat actor to control assets inside the network.

Securing SAML Token Signing Certificates: Organizations should adhere to the best practices recommended by the identity federation technology provider for securing SAML token signing keys. Wherever possible, hardware security modules should be used for storing SAML token signing certificates.

Administrative Access Controls: Organizations should ensure that user accounts with administrative privileges are managed in accordance with best practices. This includes the use of Privileged Access Workstations and Just-In-Time (JIT) strategies, and robust authentication mechanisms. Organizations should also reduce the number of users with high-level directory roles such as Global Administrator, Application Administrator, and Cloud Application Administrator.

Service Account Security: Service accounts and service principals with administrative privileges should use strong, high-entropy secrets, such as certificates and they should be stored securely. Organizations should continuously monitor any changes to these secrets as part of security operations. More importantly unusual activities involving service accounts and new sign-ins from unexpected locations should be investigated. Tools like Microsoft Azure AD and Microsoft Cloud App Security provide functionalities to detect such unusual session activities.

Reducing Exposure: Decrease potential attack surfaces by disabling or removing unnecessary or unused applications and service principals. Organizations should review and restrict the permissions assigned to active applications and service principals, particularly those that have application-only

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307134|

Embracing Zero Trust Principles: The concept of Zero Trust revolves around the shift from implicit trust where everything within a corporate network is presumed secure to a stance where a breach is assumed, and security verification is mandatory for identities, endpoints, networks, and other resources. This approach leverages all available signals and data to continuously validate the security status within an environment.
Protection of Privileged Credentials: Securing credentials is the single most important thing organizations should focus on, especially in environments that bridge on-premises infrastructure with cloud services. It is vital for organizations to excel in identity management in the cloud to mitigate risks associated with on-premises compromises affecting cloud services.

Actions Taken and Global Response

In response to the SolarWinds cybersecurity incident, a series of measures were initiated by SolarWinds, various U.S. government agencies, and international bodies to mitigate the impact and enhance security protocols. Initial steps included widespread alerts and emergency directives issued by entities such as the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the National Security Agency (NSA), focusing on immediate threat identification and mitigation. The urgency of the situation led to the deployment of Emergency Directive 21-01 by CISA on December 13th 2020, mandating federal agencies to disconnect or shut down SolarWinds Orion products. That directive was part of a broader effort to secure federal networks and assess the extent of the intrusion. Concurrently, SolarWinds responded by releasing multiple software updates aimed at patching the vulnerabilities exploited by the attackers, advising all users to update their systems to prevent further breaches.

The incident sparked a global response, with the UK's National Cyber Security Centre (NCSC) and other international entities assessing the potential impact on their networks and initiating protective measures. Legislative and executive branches in the U.S. actively participated, with senators demanding detailed assessments of the incident's impact and the administration taking steps to address and potentially retaliate against the perpetrators. This period also saw significant collaboration between the public and private sectors. Microsoft and other tech companies collaborated actively to neutralize threats by seizing and sink holing malicious domains. Into early 2021, CISA continued to release updated guidance and tools designed to assist organizations in detecting and mitigating any compromises.

VI. CONCLUSION

The SolarWinds cyberattack a poster child of sophisticated supply chain compromise, has served as a critical wake-up call to the global cybersecurity community about the profound implications of such breaches. Through an extensive dissection of this incident, this paper has explored the finer details of the attack, including the deployment of Sunburst, Teardrop, and other malicious components, and their substantial effects on a wide range of high-profile targets. This case study has highlighted the necessity for organizations to adopt a robust cybersecurity framework that emphasizes a Zero Trust approach, rigorous monitoring, and the safeguarding of privileged access. Also, in this paper we delved into the measures taken by SolarWinds, alongside U.S. government agencies and international partners, demonstrate the effectiveness of a coordinated response to mitigate such threats. As we move forward, it is evident that the SolarWinds attack is not just a singular event but a warning signal of the evolving threat landscape that requires advanced strategies to defend and protect. Organizations must adapt to this changing environment by continually updating their security protocols, engaging in active threat hunting, and employing comprehensive detection tools to respond to incidents with agility and precision. By doing so, they can better protect their assets from the increasingly sophisticated nation state actors too.

REFERENCES

[1] SolarWinds. (2020, December 24). SolarWinds Security Advisory. Retrieved from https://www.solarwinds.com/sa-overview/securityadvisory
[2] Cash, D. et al. (2020, December 14). Dark Halo Leverages SolarWinds Compromise to Breach Organizations. Retrieved from https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/
[3] CrowdStrike. (2022, January 27). Early Bird Catches the Wormhole: Observations from the StellarParticle Campaign. Retrieved from https://www.crowdstrike.com/blog/observations-from-the-stellarparticle-campaign/

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307134|

[4] Unit 42. (2020, December 23). SolarStorm Supply Chain Attack Timeline. Retrieved from https://unit42.paloaltonetworks.com/solarstorm-supply-chain-attack-timeline/

[5] MSTIC. (2020, December 18). Analyzing Solorigate, the compromised DLL file that started a sophisticated cyberattack, and how Microsoft Defender helps protect customers . Retrieved from https://www.microsoft.com/en-us/security/blog/2020/12/18/analyzing-solorigate-the-compromised-dll-file-that-started-a-sophisticated-cyberattack-and-how-microsoft-defender-helps-protect/

[6] Sudhakar Ramakrishna . (2021, January 11). New Findings From Our Investigation of SUNBURST. Retrieved from https://orangematter.solarwinds.com/2021/01/11/new-findings-from-our-investigation-of-sunburst/

[7] FireEye. (2020, December 13). Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor. Retrieved from https://www.mandiant.com/resources/blog/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor

[8] MSRC Team. (2021, February 18). Microsoft Internal Solorigate Investigation – Final Update. Retrieved from https://msrc.microsoft.com/blog/2021/02/microsoft-internal-solorigate-investigation-final-update/

[9] NSA, FBI, DHS. (2021, April 15). Russian SVR Targets U.S. and Allied Networks. Retrieved from https://media.defense.gov/2021/Apr/15/2002621240/-1/-1/0/CSA_SVR_TARGETS_US_ALLIES_UOO13234021.PDF/CSA_SVR_TARGETS_US_ALLIES_UOO13234021.PDF

[10] MSRC. (2020, December 13). Customer Guidance on Recent Nation-State Cyber Attacks. Retrieved from https://msrc.microsoft.com/blog/2020/12/customer-guidance-on-recent-nation-state-cyber-attacks/

[11] Symantec Threat Hunter Team. (2021, January 18). Raindrop: New Malware Discovered in SolarWinds Investigation. Retrieved from https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/solarwinds-raindrop-malware

[12] CrowdStrike Intelligence Team. (2021, January 11). SUNSPOT: An Implant in the Build Process. Retrieved from https://www.crowdstrike.com/blog/sunspot-malware-technical-analysis/

[13] Microsoft 365 Defender Team. (2020, December 28). Using Microsoft 365 Defender to protect against Solorigate. Retrieved from https://www.microsoft.com/en-us/security/blog/2020/12/28/using-microsoft-365-defender-to-coordinate-protection-against-solorigate/

[14] Symantec Threat Hunter Team. (2021, January 22). SolarWinds: How Sunburst Sends Data Back to the Attackers. Retrieved from https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/solarwinds-sunburst-sending-data

[15] Stephen Eckels, Jay Smith, William Ballenthin. (2020, December 24). SUNBURST Additional Technical Details. Retrieved from https://www.mandiant.com/resources/blog/sunburst-additional-technical-details

[16] Check Point Research. (2020, December 22). SUNBURST, TEARDROP and the NetSec New Normal. Retrieved from https://research.checkpoint.com/2020/sunburst-teardrop-and-the-netsec-new-normal/

[17] eSecurity Planet. (2017, October 19). The secure supply chain: Where security starts. Retrieved from https://www.esecurityplanet.com/networks/the-secure-supply-chain-where-security-starts/

[18] Mandiant. (2023, December 13). Evasive attacker leverages SolarWinds supply chain compromises with SUNBURST backdoor. Retrieved from https://www.mandiant.com/resources/blog/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor

[19] Microsoft Threat Intelligence Center. (2021, October 25). NOBELIUM targeting delegated administrative privileges to facilitate broader attacks. Retrieved from https://www.microsoft.com/en-us/security/blog/2021/10/25/nobelium-targeting-delegated-administrative-privileges-to-facilitate-broader-attacks/

[20] Nafisi, R., Lelli, A. (2021, March 4). GoldMax, GoldFinder, and Sibot: Analyzing NOBELIUM's layered persistence. Retrieved from https://www.microsoft.com/en-us/security/blog/2021/03/04/goldmax-goldfinder-sibot-analyzing-nobelium-malware/

[21] Smith, L., Leathery, J., Read, B. (2021, March 4). New SUNSHUTTLE Second-Stage Backdoor Uncovered Targeting U.S.-Based Entity; Possible Connection to UNC2452. Retrieved from https://www.mandiant.com/resources/blog/sunshuttle-second-stage-backdoor-targeting-us-based-entity

[22] MSTIC, CDOC, 365 Defender Research Team. (2021, January 20). Deep dive into the Solorigate second-stage activation: From SUNBURST to TEARDROP and Raindrop . Retrieved from https://www.microsoft.com/en-

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307134|

us/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/

[23] NCSC, CISA, FBI, NSA. (2021, May 7). Further TTPs associated with SVR cyber actors. Retrieved from https://www.ncsc.gov.uk/files/Advisory-further-TTPs-associated-with-SVR-cyber-actors.pdf
[24] UK NCSC. (2021, April 15). UK and US call out Russia for SolarWinds compromise. Retrieved from https://www.ncsc.gov.uk/news/uk-and-us-call-out-russia-for-solarwinds-compromise
[25] Mandiant. (2020, April 27). Assembling the Russian Nesting Doll: UNC2452 Merged into APT29. Retrieved from https://www.mandiant.com/resources/blog/unc2452-merged-into-apt29
[26] FBI, CISA, ODNI, NSA. (2022, January 5). Joint Statement by the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the Office of the Director of National Intelligence (ODNI), and the National Security Agency (NSA). Retrieved from https://www.cisa.gov/news-events/news/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure
[27] Microsoft Threat Intelligence Center (MSTIC). (2021, May 27). New sophisticated email-based attack from NOBELIUM. Retrieved from https://www.microsoft.com/en-us/security/blog/2021/05/27/new-sophisticated-email-based-attack-from-nobelium/
[28] Secureworks CTU. (n.d.). IRON RITUAL. Retrieved from https://www.secureworks.com/research/threat-profiles/iron-ritual

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details