SolarWinds and Related Supply Chain Compromise

TLP:WHITE - Lessons for the North American Electricity Industry

This joint white paper was prepared by the staff of the Federal Energy Regulatory Commission and the Electricity Information and Analysis Sharing Center (E-ISAC). **This report does not necessarily reflect the views of the Commission.**

Table of Contents

Executive Summary

This white paper, prepared jointly by Federal Energy Regulatory Commission (FERC) staff and the E-ISAC, emphasizes the need for continued vigilance by the electricity industry related to supply chain compromises and incidents and recommends specific cybersecurity mitigation actions to better ensure the security of the bulk-power system (BPS). While focusing primarily on the ongoing cyber event related to the SolarWinds Orion platform and related Microsoft's 365/Azure Cloud compromise, it also addresses related compromises in products such as Pulse Connect Secure. Two additional examples of compromises, Microsoft's on-premise Exchange servers and F5's BIG-IP are discussed to illustrate continued adversary interest and exploitation of ubiquitous software systems.

Because of SolarWinds' wide use and the adversarial tactics used, even entities that did not install SolarWinds on their networks could still be impacted. For example, the indicators of compromise (IOCs) have been found on networks without SolarWinds. In addition, although SolarWinds may not have been used by entities, their key suppliers may use the product. Should the suppliers be compromised, the supplier in turn could compromise their customers, including those without SolarWinds. In fact, there is evidence technology firms were targeted for this reason.

On December 13, 2020, FireEye Inc., a cybersecurity solutions and forensics firm, publicly posted details about an attack on certain software developed by SolarWinds Orion. For victims, this attack is particularly damaging because in order to function SolarWinds must have broad and privileged access to the networks it manages, including both the corporate and operational networks of an entity. The breach provides the opportunity for an adversary to monitor network traffic and compromise systems, which could result in disruption of their operations.

Underscoring the severity of the event, on December 13, 2020, the U.S. Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) issued Emergency Directive 21-01, which required Federal agencies to take action based on the DHS assessment that a successful compromise from the SolarWinds attack would have "grave" consequences. On December 15, 2020, the White House National Security Council (NSC) established a Cyber Unified Coordination Group (UCG) composed of multiple Federal agencies to coordinate the investigation and remediation of the "significant" cyber incident. On December 17, 2020, CISA issued Alert AA20-352A, directed toward the private sector, which described the attack for industry, the affected products and the mitigation recommendations.

In response to the breach, SolarWinds issued a new version of its software that eliminated the compromised code and addressed other vulnerabilities. At a minimum, users of the compromised software were advised to update their SolarWinds software with the updated version. CISA, however, has warned that operating even the updated version of SolarWinds may carry some risk, explaining that "…it is likely that the adversary is in a strong position to identify any potential … vulnerabilities in the SolarWinds Orion code that are unrelated to the inserted malicious code *and may therefore survive its removal*."[1]

Considering the sophistication, breadth, and persistence of the SolarWinds attack, it is recommended that electric industry stakeholders fully consider the available diagnostics and mitigation measures to affectively address the software compromise. Likewise, it is valuable for entities to consider the recommendations of both CISA Alerts. While CISA Emergency Directive 21-01 is directed to Federal agencies, private sector entities can benefit from the specific mitigation actions set forth in the document,

[1] DHS CISA, https://cyber.dhs.gov/ed/21-01/

including: disconnecting affected systems, conducting deep forensics, performing risk analyses, and consulting with CISA before reconnecting affected systems.

Next Steps – Recommended Industry Actions

FERC staff and the E-ISAC strongly recommend the following industry actions:

- Regardless of use of affected SolarWinds Orion products, forensically verify the existence of IOCs from Appendix B of CISA Alert AA20-352A.
  - Sources may include network flow data, Domain Name Services (DNS) logs, firewall logs, Endpoint Detection and Response (EDR) logs, host and server logs, and proxy logs. If not currently retaining *all* of the above log sources for a period of at least 180 days, consider the necessary resources to enhance your collection capability to that level.
- Fully considering the Emergency Directives to the federal agencies if their networks have shown compromise:
  - Disconnecting affected systems, conducting deep forensics, performing risk analyses, consulting with CISA before reconnecting affected systems and, re-building infected networks including identity management systems as necessary
- Require key vendors to report their use of SolarWinds and their actions to check for the TTPs/IOCs regardless of such use as well as any follow-up remediation actions recommend by DHS publications Alert AA20-352a and Emergency Directive 21-01.
- If continuing to operate SolarWinds in your on-premises or cloud hosted environment, apply the mitigation activities set forth in follow Appendix B of Emergency Directive 21-01 guidance, (Specific Conditions for Operating SolarWinds Orion).
  - For third-party hosted environments (e.g., cloud), inventory all information systems and inquire with service providers for status pertaining to compliance to CISA Emergency Directive 21-01 and Alert AA20-352A. Run log queries on IOCs from Appendix B of DHS AA20-352A regardless of use of affected SolarWinds products.
  - If not currently using advanced logging actions in cloud hosted environments, in addition to log retention of at least 180 days, and centralized out-of-band logging either on-premises or to a separate cloud instance, consider the necessary resources to enhance your capability to that level.
- Revalidate the implementation of least-privilege principle for host and network permissions, specifically surrounding local administrative privilege, service accounts and delegation under Active Directory.
- Consider a systemic risk-based approach for protecting the most critical of the critical assets.
- Implement the National Institute of Standards and Technology (NIST) Cybersecurity Framework and baseline critical access and administrative privileges.
- Consider participating in the Cyber Mutual Assistance Program with peer utilities, to ensure a collective response during cyber events.[2]
- Exercise cyber and physical security response plans with third-party vendors, partners, and government. Review and update cyber plans, as necessary, to include Lessons Learned from these supply chain attacks.
- Consider conducting security assessments or penetration tests to ensure security baseline.[3]
- Increase timeliness of voluntary reporting to the E-ISAC and CISA as well as mandatory CIP-008-6 reports.

[2] ESCC, https://www.electricitysubsector.org/-/media/Files/ESCC/Documents/CMA/Cyber-Mutual-Assistance-Program-One-Pager_013119.ashx?la=en&hash=F4D3445C75E3B9884458E403390DBBD120F9D8D4

[3] NIST Guide to Secure Web Services https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-95.pdf

Scope and Purpose

Scope

This joint white paper by FERC Staff and NERC's E-ISAC primarily focuses on the significant and ongoing cyber event related to the SolarWinds Orion platform and the related Microsoft 365/Azure Cloud compromise, it also addresses vulnerabilities in products such as Pulse Connect Secure, Microsoft's on-premise Exchange servers, and F5's BIG-IP. This white paper is derived from reputable sources and offers key actions to take and key questions to ask to ensure the electricity industry is taking all necessary steps to mitigate compromises related to these incidents and vulnerabilities.

Purpose

This whitepaper produced by FERC Staff, in consultation with the E-ISAC, highlights the need for continued vigilance by the electricity industry related to supply chain compromises and incidents, identifies key elements of adversary tradecraft, highlights specific malwares and tools to remediate, and recommends actions to ensure the reliability and security of the BPS. The whitepaper is intended for electric industry stakeholders and vendors as they consider their next steps in continued response to the SolarWinds cyberattack. Members of other critical infrastructure sectors may also find the white paper of interest.

Solar Winds Event Background and Electricity Industry Response

Event Background

Information published by the U.S. government and security vendor FireEye on December 13, 2020, revealed that the widely used SolarWinds Orion network management tool was compromised through a supply chain attack.[4] The Russian Foreign Intelligence Service (SVR) threat actor gained access to the SolarWinds production environment, "pushed" malicious code, dubbed SUNBURST (also known as Solorigate), through legitimate updates to customers and enabled adversary remote access.[5] Adjacent to the SolarWinds compromise, additional research revealed the actor used its initial access to gain network privileges on victim's system and manipulate identity and authentication mechanisms in Microsoft's 365 and Azure Cloud environments.[6] According to CISA:

> … the threat actor obtained initial access by password guessing, password spraying, and exploiting inappropriately secured administrative credentials via remote services… After gaining access to cloud environments, the actor established persistence mechanisms for Application Programming Interface (API)-based access and collected and exfiltrated data.[[7]]

The threat actor demonstrated sophisticated defense evasion skills, including:

- Obfuscating its Command and Control (C2) communications[8]
- Hiding its activity among legitimate user traffic
- Establishing difficult-to-detect persistence mechanisms (e.g., in API)

DHS CISA developed a network categorization taxonomy to guide organizational risk and impact assessments:

- **Category 1** includes networks that do not have the identified malicious binary code on their network and can forensically confirm that the binary was never present on their systems. This includes networks that do not and never did use the affected versions of SolarWinds Orion products.
- **Category 2** includes agency networks where the presence of the malicious binary has been identified, with or without beaconing to avsvmcloud[.]com [adversary controlled infrastructure].

[4] DHS CISA, *Emergency Directive 21-01,* (Dec. 13, 2020), https://cyber.dhs.gov/ed/21-01/.

[5] White House Statement, *FACT SHEET: Imposing Costs for Harmful Foreign Activities by the Russian Government*, (Apr. 15, 2021). https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/.

[6] NSA, *Cybersecurity Advisory: Malicious Actors Abuse Authentication Mechanisms to Access Cloud Resources*, (Dec. 17, 2020). https://www.nsa.gov/News-Features/Feature-Stories/Article-View/Article/2451159/nsa-cybersecurity-advisory-malicious-actors-abuse-authentication-mechanisms-to/.

[7] DHS CISA, Remediating Networks Affected by the SolarWinds and Active Directory/M365 Compromise, April 15, 2021. https://us-cert.cisa.gov/remediating-apt-compromised-networks

[8] NIST defines Command and Control (C2) as "the exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission." In the context of cyber incidents, it refers to the infrastructure and communication methodologies that enable threat actors to gather data and execute commands on a target network.

- **Category 3** includes agency networks that used affected versions of SolarWinds Orion and have evidence of follow-on threat actor activity, such as binary beaconing to avsvmcloud[.]com [communicating with the adversary's infrastructure] and secondary C2 activity to a separate domain or IP address (typically but not exclusively returned in avsvmcloud[.]com Canonical Name record [CNAME[9]] responses).[10]

The reported compromise of nearly 18,000 SolarWinds customers triggered incident response across the public and private sectors, including the electricity industry.[11] Since the initial disclosure, additional related malware has been identified, providing additional information for responders to identify and mitigate.[12] In reaction to FireEye's report about the SolarWinds attack on December 13, DHS issued Emergency Directive 21-01 that same day, directing federal agencies to take action after assessing that a successful compromise from this attack would have "grave" consequences. In rapid succession, on December 15, 2020, the NSC set up a Cyber Unified Coordination Group (UCG) after finding that the event was "significant." This process was established under Presidential Policy Directive (PPD)-41 which was issued in July 2016. The process is intended to ensure that "cyber incidents that have significant impacts on an entity, our national security, or the broader economy" receive adequate response efforts. According to PPD-41, "[t]hese significant cyber incidents demand unity of effort within the Federal Government and especially close coordination between the public and private sectors."

In order to engage with the private sector, on December 17, 2020, CISA issued Alert AA20-352A. This comprehensive Alert described the breach, the affected SolarWinds products, other attack vectors and affected products, the TTPs, IOCs, hunting techniques and tools, and mitigation recommendations. In the Alert, CISA emphasized the extended time before discovery (at least March 2020), the difficulty in removing the adversary from compromised networks, the probability that the adversary has additional access vectors and TTPs that may not yet have been discovered, and other possible compromised applications such as Microsoft 365 and Microsoft Azure. The Alert discussed the range of actions from checking for the affected binary code affiliated with the SolarWinds Orion product through rebuilding the affected networks depending upon the category of exposure.

While the complexity and breadth of the compromise only became public on December 13, 2020, subsequent investigations demonstrated that the compromise persisted as far back as January 2019 and highlighted the patience and tradecraft of this Russian adversary.[13] The first public indication of the campaign initially emerged on December 8, 2020, when FireEye disclosed it was compromised. FireEye's investigation into the theft led to the source code review of a recent SolarWinds update and the initial detection of the larger breach as well as compromises that involved Microsoft products.[14]

[11] FBI, CISA, ODNI, and NSA, *Joint Statement*, (Jan 5, 2021). https://www.cisa.gov/news/2021/01/05/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure.

[12] DHS CISA AR21-105A, April 15, 2021. https://us-cert.cisa.gov/ncas/analysis-reports/ar21-105a

[13] Reuters, SolarWinds CEO says hackers may have struck in January 2019, months earlier than thought: https://www.reuters.com/business/energy/solarwinds-ceo-says-hackers-may-have-struck-january-2019-months-earlier-than-2021-05-19/

[14] FireEye Threat Research 'Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor." December 13, 2020. https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

In its Emergency Directive 21-01 of December 13, 2020, CISA directed Federal agencies to disconnect affected computer systems, conduct deep forensics, perform risk analyses, and consult with CISA before reconnecting or rebuilding affected systems. CISA explained:

> Operating even version 2020.2.1 HF2 of the SolarWinds Orion platform may still carry some risk. The adversary enjoyed longstanding, covert access to the build process that SolarWinds uses for Orion, including to the code underlying the Orion platform. While the immediate known consequence of this access was the insertion of the malicious code into the affected versions of SolarWinds Orion, there may be other unknown consequences as well. The adversary can be presumed to be familiar with at least some aspects of the SolarWinds development and coding practices, … Consequently, it is likely that the adversary is in a strong position to identify any potential (and as yet unknown) vulnerabilities in the SolarWinds Orion code that are unrelated to the inserted malicious code and may therefore survive its removal.[15]

Electricity Industry Response

Since December 2020, the U.S. government and cyber security vendors continue to investigate and share new findings, threat vectors, and remediation tips. On December 14, 2020, the E-ISAC published an all-points bulletin to highlight the SolarWinds compromise and its potential impact as well as highlighting several defense and detection tools produced by FireEye to aid industry in its response. In addition, on December 17, 2020, the E-ISAC hosted a Critical Broadcast Program call. In an effort to better understand the extent of condition of the SolarWinds Orion compromise impact on BPS security and reliability, NERC issued a private Level 2 NERC alert on December 22, 2020.

To support the ongoing and resource intensive industry response, the E-ISAC and the ESCC produced additional resources to aid utilities in their response and hosted a series of restricted webinars to provide additional insights to electric utilities with key vendors involved in the response. A publicly available curated list of resources is available www.eisac.com .

[15] DHS CISA, ED 21-02 Mitigate Microsoft Exchange On-Premises Product Vulnerabilities: https://cyber.dhs.gov/ed/21-02/

Recommended Key Actions for the Electric Industry

FERC and E-ISAC staff have reviewed the recent supply chain event, guidance provided by private software and hardware vendors, and the U.S. federal government, and recommend that electric industry stakeholders take the following actions to help minimize the potential of future supply chain attacks.

SolarWinds Orion Platforms

The SolarWinds Orion products (the affected versions are 2019.4 through 2020.2.1 HF1) that were exploited by the Russian-attributed actors were identified publicly on December 13, 2020. Investigation continues on this campaign, and the electricity industry is encouraged to view the information and take appropriate actions to assure the reliability and security of the BPS as new information becomes available. Although the following recommendations are based on CISA Emergency Directive 21-01 and tailored to federal agencies, CISA encourages critical infrastructure entities as well as and private sector organizations to review and apply as appropriate.

- Entities with the affected versions of the SolarWinds Orion software should immediately **disconnect or power down SolarWinds Orion products, versions 2019.4 through 2020.2.1 HF1, from their network**. Until such time as CISA directs affected federal entities to rebuild the Windows operating system and reinstall the SolarWinds software package Additionally: **Identify and remove** all threat actor-controlled accounts and identified persistence mechanisms.
- **Electric industry stakeholders should report as an incident** to CISA and the E-ISAC any evidence of computer system compromise as a result of the SolarWinds attack, either through direct purchase and application of the affected software, or indirect compromise through a third-part vendor or supplier.
- **After (and only after) all threat actor-controlled accounts and identified persistence mechanisms have been removed, electricity industry stakeholders should**:
  - Treat all hosts monitored by the SolarWinds Orion monitoring software as compromised by threat actors and assume that further persistence mechanisms have been deployed
  - Rebuild hosts monitored by the SolarWinds Orion monitoring software using trusted sources
  - Reset all credentials used by or stored in SolarWinds software (such credentials should be considered compromised).

Key Tools to Assist Network Defenders/Responders on SolarWinds Orion

The following is a list of key tools to help defenders ensure they have mitigated malware related to the SolarWinds Orion platform compromise.

- **SolarWinds Issues New Patches for Orion Platform to Address "SUPERNOVA" Malware**
  SolarWinds released an update to their security advisory that discussed the SUPERNOVA malware. SUPERNOVA is not malicious code embedded in SolarWinds's Orion but a webshell[16] that could be deployed through an exploitation of a vulnerability in the Orion platform.

[16] Microsoft defines a webshell as a "small piece of malicious code written in typical web development programming languages (e.g., ASP, PHP, JSP) that attackers implant on web servers to provide remote access and code execution to server functions. Webshells allow attackers to run commands on servers to steal data or use the server as launch pad for other activities like credential theft, lateral movement, deployment of additional payloads, or hands-on-keyboard activity, while allowing attackers to persist in an affected organization."

- **FireEye Releases Free Tool to Detect SolarWinds Hack Techniques**
  FireEye released a free tool on GitHub, dubbed Azure AD Investigator, which the company claims can help organizations detect techniques utilized by the group behind the SolarWinds (UNC2452).[17]

- **Microsoft 365 and Azure Cloud Malware Strains**
  As referenced previously, security researchers continue to uncover new malware strains and TTP used by the threat actor. The threat actors behind these intrusions have continued to focus heavily on remaining undetected in victims' environments.

Custom tools and C2 infrastructure continue to be released by security researchers and defenders investigating SolarWinds. Microsoft associated the three malware strains, "GoldMax," "Sibot," and "GoldFinder" with late-stage, post-infection activity. GoldMax, a C2 backdoor,[18] attempts to obfuscate malicious C2 network traffic by surrounding it with decoy traffic. This decoy traffic generator creates up to four random server requests to both legitimate and malicious addresses. Each URL is created from a combination of domain names or IP addresses taken from a list of 14 hardcoded URLs, many of which contain the top level domain (TLD)[19] of the malicious C2. Sibot connects to legitimate but compromised sites that are unique to each victim in order to download to the compromised system a visual basic script. The script is named after legitimate Windows tasks and is stored either in the compromised system's registry or in an obfuscated format on the disk. FERC and the E-ISAC expects these discoveries to persist. Network defenders are encouraged to remain vigilant of similar activity related to this campaign.

Actions to Take

The following are recommended general practices for system hardening to address the Microsoft 365 and Azure Cloud environment compromise:

- Maintain up-to-date antivirus signatures and engines
- Keep operating system patches up-to-date
- Disable file and printer sharing services (If these services are required, use strong passwords or Active Directory (AD) authentication.)
- Restrict users' ability (permissions) to install and run unwanted software applications and do not add users to the local administrators group unless required
- Enforce a strong password policy and implement regular password changes
- Exercise caution when opening e-mail attachments even if the attachment is expected and the sender appears to be known
- Enable a personal firewall on workstations configured to deny unsolicited connection requests
- Disable unnecessary services on workstations and servers
- Scan for and remove suspicious e-mail attachments and ensure that the scanned attachment is its "true file type" (i.e., the extension matches the file header)
- Monitor users' web browsing habits and restrict access to sites with unfavorable content
- Exercise caution when using removable media (e.g., USB thumb drives, external drives, compact disks, etc.)
- Scan all software downloaded from the Internet prior to executing

[17] FireEye/Mandiant, "Github: fireeye/Mandiant-Azure-AD-Investigator" https://github.com/fireeye/Mandiant-Azure-AD-Investigator

[18] NIST defines a backdoor as "an undocumented way of gaining access to computer system."

[19] A top-level domain refers to the last segment of a domain name, or the part that follows immediately after the "dot" symbol.

- Maintain situational awareness of the latest threats and implement appropriate access control lists (ACLs)[20]

Key Tools to Assist Network Defenders and Responders for Azure and Microsoft 365
The following is a list of key tools that can help defenders ensure that they have mitigated malware related to Microsoft products affected by the compromise.

- **Crowdstrike and CISA Released Tools for Hunting the Azure and Microsoft Office 365**
  CrowdStrike released the free CrowdStrike Reporting Tool for Azure to help organizations quickly and easily review excessive permissions in their Azure AD environments, determine configuration weaknesses, and provide advice to mitigate risk. The tool is intended to help defenders review excessive permissions in their Azure AD environments to help determine configuration weaknesses and provide advice to mitigate this risk. [21]

  On December 24, the DHS CISA publicly released a similar Microsoft PowerShell based tool called "Sparrow," to help detect possible compromised accounts and applications in the Azure/m365 environment. Per CISA, "The tool is intended for use by incident responders, and focuses on the narrow scope of user and application activity endemic to identity and authentication based attacks seen recently in multiple sectors. It is neither comprehensive nor exhaustive of available data, and is intended to narrow a larger set of available investigation modules and telemetry to those specific to recent attacks on federated identity sources and applications."[22] Guidance on how to use the CISA Sparrow tool to aid in detecting potentially compromised environments can be found in AA21-008A, and visualized through the "Aviary" tool, also developed by DHS CISA.[23]

- **CISA Alert CHIRP IOC Detection Tool**
  DHS CISA developed and publicly released a new tool intended to detect post-compromise threat activity using the CISA Hunt and Incident Response Program (CHIRP) IOC Detection Tool.[24] CHIRP is a forensics collection tool that CISA developed to help network defenders find IOC associated with the Orion products, threat activity in Microsoft cloud environments (Azure and Office 365), and threat activities associated with on-premise enterprise environments. CHIRP is most likely to benefit entities where the presence of the malicious binary has been identified but where evidence of follow-on threat activity has yet to be identified.

[20] DHS CISA, "CISA, CNMF Issue Malware Analysis Report of SolarWinds-Related Malware" https://us-cert.cisa.gov/ncas/analysis-reports/ar21-105a

[21] Crowdstrike, "CRT (Crowdstrike Reporting Tool for Azure," https://www.crowdstrike.com/resources/community-tools/crt-crowdstrike-reporting-tool-for-azure/

[22] DHS CISA, "Github: cisagov/Sparrow" https://github.com/cisagov/Sparrow

[23] DHS CISA, "AA21-008A Detecting Post-Compromise Threat Activity in Microsoft Cloud Environments" https://us-cert.cisa.gov/ncas/alerts/aa21-008a

[24] DHS CISA, "Github: cisagov/CHIRP" https://github.com/cisagov/CHIRP

Other Events - Background and Electricity Industry Response

In addition to the SolarWinds attack, other recently identified cybersecurity vulnerabilities have the potential to compromise electric industry cybersecurity. Below, we describe the following vulnerabilities: Pulse Connect Secure, email-based attacks by Nobelium, Microsoft's on-premise Exchange servers, and F5's BIG-IP.

Pulse Connect Secure

Pulse Connect Secure (recently acquired by Avanti) is a computer services provider. A vulnerability in Pulse Connect Secure VPN devices was disclosed on April 20, 2021, that could allow an un-authenticated user to gain remote access to the Pulse Connect Secure appliance that, if unpatched, could allow a threat actor to execute files on the Pulse Connect Secure gateway. Pulse Secure determined that threat actors have used this newly disclosed vulnerability and a combination of prior vulnerabilities identified in 2019 and 2020 to place webshells on the Pulse Connect Secure appliances for further access and persistence. These webshells can allow for a variety of functions, including authentication and multi-factor authentication bypass, password logging, and maintaining persistence. This vulnerability netted a Critical Vulnerability Scoring System (CVSS) score of 10, which is critical.

Active exploitation was observed in U.S. government agencies and the financial services sector. CISA published Alert *AA21-110A Exploitation of Pulse Connect Secure Vulnerabilities* on April 20, 2021, followed by Emergency Directive (ED) 21-03, *Mitigate Pulse Connect Secure Product Vulnerabilities* on April 20, 2021, in response to the discovery. While not seen actively in the electricity industry, the E-ISAC issued an All Points Bulletin (APB) and shared the immediate recommended solution to upgrade the software to version 9.1R.11.4.

Though not tied to the same APT as the SolarWinds Orion compromise, the exploitation of Ivanti's Pulse Connect Secure VPN appliances used the SolarWinds-related malware SUPERNOVA.[25] This demonstrated that previously used tools, tactics, and techniques could be used by other actors for different campaigns and brings to the forefront the importance of accurately identifying the threat actor.

Actions to Take

- The immediate recommended solution for this vulnerability is to upgrade the Pulse Connect Secure server software to version 9.1R.11.4.
- "To disable the Windows File Browser, Pulse Secure recommends users navigate to "User > User Role > Click Default Option > Click on General."
- A final patch was issued on May 3, 2021.[26]
- DHS CISA updated ED21-03 and AA-21-110A on May 27, 2021 with additional recommendations for using the Pulse Secure Integrity Checker to understand if a device has been compromised.

Key Tools to Assist Network Defenders/Responders

Pulse Secure's parent company, Ivanti, released mitigation for related exploitation activities and also recommends using the Pulse Connect Secure Integrity Tool to determine if customer systems are impacted.[27] The Pulse Connect Secure Integrity Tool can assist network defenders in identifying modifications or additions to a Pulse Connect Secure appliance file system.

[25] DHS CISA AA21-110A, April 20, 2021. https://us-cert.cisa.gov/ncas/alerts/aa21-110a

[26] Ivanti, https://kb.pulsesecure.net/articles/Pulse_Secure_Article/SA44784/

[27] Ivanti, https://kb.pulsesecure.net/articles/Pulse_Secure_Article/KB44755

Nobelium Threat Actor - New Email-Based Attack

The Microsoft Threat Intelligence Center posted a report on a recently uncovered wide-scale malicious email campaign operated by Nobelium, which is Microsoft's label for the threat actor behind the attacks against SolarWinds, the Sunburst backdoor, Teardrop malware, GoldMax malware, and other related components.[28] Microsoft initially observed and tracked the malicious email campaign in January 2021, and saw it evolve over a series of waves demonstrating significant experimentation. On May 25th, 2021, the campaign escalated as Nobelium leveraged legitimate mass-mailing service, Constant Contact, to masquerade as a U.S.-based development organization to distribute malicious URLs to a wide variety of organizations and industry verticals. Microsoft noted that this is still an "active incident," and they will post more details as they become available.

Actions to Take

- Turn on cloud-delivered protection in Microsoft Defender Antivirus or the equivalent for your antivirus product to cover rapidly evolving attacker tools and techniques. Cloud-based machine learning protections block a huge majority of new and unknown variants.
- Run Endpoint Detecting and Response in block mode so that Microsoft Defender for Endpoint can block malicious artifacts, even if your non-Microsoft antivirus doesn't detect the threat or when Microsoft Defender Antivirus is running in passive mode.
- Enable network protection to prevent applications or users from accessing malicious domains and other malicious content on the Internet.
- Enable investigation and remediation in full automated mode to allow Microsoft Defender for Endpoint to take immediate action on alerts to resolve breaches, significantly reducing alert volume.
- Use device discovery to increase your visibility into your network by finding unmanaged devices on your network and onboarding them to Microsoft Defender for Endpoint.
- Enable Multi Factor Authentication to mitigate compromised credentials.
- Turn on the following attack surface reduction rule to block or audit activity associated with this threat: Block all Office applications from creating child processes. NOTE: Assess rule impact before deployment.

Microsoft Exchange On-premise Vulnerabilities

On March 2, 2021, Microsoft announced the detection of multiple zero-day exploits[29] being used to attack on-premise versions of Microsoft Exchange Server (Exchange Online was not affected). Microsoft attributed the campaign that targeted the Exchange servers to HAFNIUM, a Chinese state-sponsored adversary. The vulnerabilities affected Exchange Server versions 2013, 2016, and 2019 while Exchange Server 2010 was also updated for defense-in-depth purposes.[30] Successful exploitation of vulnerabilities may have allowed remote, unauthorized access, arbitrary write-to-file paths, and potential exfiltration of data on vulnerable Exchange servers.[31]

The immediate recommended action was to apply the patch provided by Microsoft. While DHS CISA was unaware of active exploitation of these vulnerabilities, once notice of an update is publicly released, other

[28] Microsoft, https://www.microsoft.com/security/blog/2021/05/27/new-sophisticated-email-based-attack-from-nobelium/?utm_source=dlvr.it

[29] NIST defines a Zero-Day Exploit as a "previously unknown hardware, firmware, or software vulnerability."

[30] Microsoft, "HAFNIUM Targeting Exchange Servers with 0-day exploits," March 2, 2021. https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/

[31] DHS CISA, Emergency Directive 21-02 https://cyber.dhs.gov/ed/21-02

actors and cyber criminals have been known to take advantage of the underlying vulnerabilities before the patches are applied.[32] Although the guidance is tailored to federal agencies, CISA encourages critical infrastructure entities as well as state, local, and private sector organizations to review and apply it as appropriate. As of March 24, 2021, Microsoft reported 92% of vulnerable servers across the world were patched or mitigated.

Actions to Take

All affected entities should have already applied the March 2, 2021, patches provided by Microsoft.[33] In addition, CISA has recommended a number of hardening measures.[34] CISA also recommended the use of tools such as BloodHound to understand the possible attack path that starts with a compromise of the Microsoft Exchange infrastructure.

Key Tools to Assist Network Defenders and Responders

The following is a list of key tools can help defenders ensure they have mitigated malware related to Microsoft products affected by the compromise:

- *Microsoft released the new Microsoft Exchange On-Premises Mitigation Tool[35] to help customers who do not have dedicated security or IT teams to apply these security updates.* Microsoft tested this tool across Microsoft Exchange Server 2013, 2016, and 2019 deployments. This new tool is designed as an interim mitigation for customers who are unfamiliar with the patch or update process or who have not yet applied the on-premises Exchange security update.
- The Microsoft Safety Scanner[36] is a scan tool designed to find and remove malware from Windows computers. Simply download it and run a scan to find malware and try to reverse changes made by identified threats.
- Another option is to run Test-ProxyLogon.ps1 script[37] as an administrator to analyze Exchange and internet information server logs and discover potential attacker activity. This script checks targeted exchange servers for signs of the proxy logon compromise described in CVE-2021-26855, 26857, 26858, and 27065. This script is intended to be run via an elevated Microsoft Exchange Management Shell. If the script does not identify attacker activity, it outputs the message "Nothing suspicious detected." If attacker activity is identified, the script reports the vulnerabilities for which it found evidence of use and collects logs that it stores in the specified output path in the Test-ProxyLogonLogs directory.

F5 Networks, Inc. BIG-IP

On April 28, 2021, F5 Networks, Inc. (F5), a cloud services and security company, released an advisory on multiple security vulnerabilities, and advised the following steps to address the vulnerable versions:

[32] DHS CISA, Emergency Directive 21-02 "Mitigate Microsoft Exchange On-Premise Product Vulnerabilities, Updated April 13, 2021. https://cyber.dhs.gov/ed/21-02/#supplemental-direction-v2

[33] Microsoft Security Response Center, "On-Premises Exchange Server Vulnerabilities Resource Center, March 2, 2021. https://msrc-blog.microsoft.com/2021/03/02/multiple-security-updates-released-for-exchange-server/

[34] *See* CISA Emergency Directive 21-02. https://cyber.dhs.gov/ed/21-02/#supplemental-direction-v2

[35] https://aka.ms/eomt

[36] Microsoft, https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/safety-scanner-download

[37] Microsoft Threat https://msrc-blog.microsoft.com/2021/03/16/guidance-for-responders-investigating-and-remediating-on-premises-exchange-server-vulnerabilities/

The first vulnerability (CVE-2021-23008) enables a bypass of the Kerberos Key Distribution Center (KDC) security feature impacting application delivery services. According to Silverfort researchers, “the KDC Spoofing vulnerability allows an attacker to bypass the Kerberos authentication to BIG-IP Access Policy Manager (APM), bypass security policies and gain unfettered access to sensitive workloads.”[38]

The second vulnerability (CVE-2021-23009) may cause malformed HTTP/2[39] requests to have an infinite loop that causes a denial-of-service (DoS)[40] for Data Plane traffic. According to F5, “when this vulnerability is exploited, the system may experience a [DoS] attack, which can cause the [Traffic Management Microkernel] process to restart.”[41]

The third vulnerability (CVE-2021-23010) impacts BIG-IP Application Security Manager (ASM)/Advanced Web Application Firewall (WAF). According to F5, “when BIG-IP ASM/Advanced WAF system processes WebSocket requests with [JavaScript Object Notation] [42] payloads using the default [JavaScript Object Notation] content profile in the ASM security policy, the BIG-IP ASM bd process may produce a core file.” Furthermore, if this vulnerability is exploited, the BIG-IP ASM bd[43] process may produce a core file, interrupt traffic processing, and cause a failover event.[44]

The fourth vulnerability (CVE-2021-23015) is referred to as the Appliance Mode authenticated iControl RE presentational State Transfer (iControl REST)[45] vulnerability and an authenticated user assigned the “Administrator” role may be able to bypass Appliance Mode restrictions. According to F5, “In Appliance Mode, an authenticated user with valid user credentials assigned the Administrator role may be able to bypass Appliance mode restrictions and run arbitrary commands.”[46]

Action to Take

F5 has provided detailed information to assist entities running a version of F5 to determine whether the software has a known vulnerable and, if so, available fixes.[47]

[38] F5. Ask F5. “K51213246: BIG-IP APM AD authentication vulnerability CVE-2021-23008.” April 28, 2021. https://support.f5.com/csp/article/K51213246

[39] HTTP/2 is a revision to the original Hyertext Transfer Protocol (HTTP) that is the foundation of most data exchanges on the internet.

[40] NIST defines Denial of Service (DoS) as the “prevention of authorized access to resources or the delaying of time-critical operations.”

[41] F5. Ask F5. “K90603426: TMM with HTTP/2 vulnerability (CVE-2021-23009).” April 28, 2021. https://support.f5.com/csp/article/K90603426

[42] JavaScript Object Notation (**JSON**) is a standard text-based format for representing structured data based on JavaScript object syntax commonly used for transmitting data in web applications.

[43] ‘”d” is the traffic processing daemon that implements the BIG-IP ASM security policy on the HTTP requests it receives from TMM.

[44] F5. Ask F5. “K18570111: BIG-IP ASM and Advanced WAF WebSocket vulnerability CVE-2021-23010.” April 28, 2021. https://support.f5.com/csp/article/K18570111

[45] iControl REST is an interface used to manage F5 network appliances.

[46] F5. Ask F5. “K74151369: Appliance Mode authenticated iControl REST vulnerability CVE-2021-23015.” April 28, 2021. https://support.f5.com/csp/article/K74151369

Conclusion

As geopolitical competitors increasingly demonstrate intent to leverage cyber capabilities, including civilian critical infrastructure, to advance their interests, so too must vigilance against direct and indirect attacks against the electricity industry.[48] The December 2020 supply chain compromise using SolarWinds and adjacent technologies like Microsoft 365 and Azure cloud environments provide an important reminder to industry on the need for persistent and proactive collective defense. This white paper describes these major supply chain-related cyber security events and the key actions to take to secure systems.

The E-ISAC is working closely with its members, FERC, and other partners in the Canadian and United States governments to produce timely, actionable, and useful defense information for all segments of the electric industry. In the coming months, the E-ISAC anticipates supplementing its current information sharing with new CRISP capabilities, enhanced cross-border sharing, and collaboration with the U.S. Department of Energy's office of Cybersecurity, Energy Security and Emergency Response (CESER). Likewise, FERC staff stands ready to assist in the dissemination of actionable information that supports the electric industry in proactively responding to cyber attacks and other cyber vulnerabilities.

Next Steps – Recommended Industry Actions

The E-ISAC and FERC staff strongly recommend the following industry actions:

- Regardless of use of affected SolarWinds Orion products, forensically verify the existence of indicators of compromise (IOCs) from Appendix B of CISA Alert AA20-352A.
    - Sources may include network flow data, Domain Name Services (DNS) logs, firewall logs, Endpoint Detection and Response (EDR) logs, host and server logs, and proxy logs. If not currently retaining *all* of the above log sources for a period of at least 180 days, consider the necessary resources to enhance your collection capability to that level.
- Fully considering the Emergency Directives to the federal agencies if their networks have shown compromise:
    - disconnecting affected systems, conducting deep forensics, performing risk analyses, consulting with CISA before reconnecting affected systems and, re-building infected networks including identity management systems as necessary
- Require key vendors to report their use of SolarWinds and their actions to check for the TTPs/IOCs regardless of such use as well as any follow-up remediation actions recommend by DHS publications Alert AA20-352a and Emergency Directive 21-01.
- If continuing to operate SolarWinds in your on-premises or cloud hosted environment, apply the mitigation activities set forth in follow Appendix B of Emergency Directive 21-01 guidance, (Specific Conditions for Operating SolarWinds Orion).
    - For third-party hosted environments (e.g., cloud), inventory all information systems and inquire with service providers for status pertaining to compliance to CISA Emergency Directive 21-01 and Alert AA20-352A. Run log queries on IOCs from Appendix B of DHS AA20-352A regardless of use of affected SolarWinds products.
    - If not currently using advanced logging actions in cloud hosted environments, in addition to log retention of at least 180 days, and centralized out-of-band logging either on-premises or to a separate cloud instance, consider the necessary resources to enhance your capability to that level.

[48] DNI, 2021 Wordwide Threat Assessment, p. 4.

- Revalidate the implementation of least-privilege principle for host and network permissions, specifically surrounding local administrative privilege, service accounts and delegation under Active Directory.
- Consider a systemic risk-based approach for protecting the most critical of the critical assets.
- Implement the National Institute of Standards and Technology (NIST) Cybersecurity Framework and baseline critical access and administrative privileges.
- Consider participating in the Cyber Mutual Assistance Program with peer utilities, to ensure a collective response during a cyber event.[49]
- Exercise cyber and physical security response plans with third-party vendors, partners, and government. Review and update cyber plans, as necessary, to include Lessons Learned from these supply chain attacks.
- Consider conducting security assessments or penetration tests to ensure security baseline.[50]
- Increase the timeliness of voluntary reporting to the E-ISAC and CISA as well as mandatory CIP-008-6 reports.

[49] https://www.electricitysubsector.org/-/media/Files/ESCC/Documents/CMA/Cyber-Mutual-Assistance-Program-One-Pager_013119.ashx?la=en&hash=F4D3445C75E3B9884458E403390DBBD120F9D8D4

[50] NIST Guide to Secure Web Services https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-95.pdf

Appendix A: SolarWinds Supply Chain Compromise Key Terms

Table 1 summarizes the major terms for to the December 2020 Supply Chain Compromise.

Table 1: Key Terms

Primary Name	Associated Names[51]	Date	What it Does	Tools/Steps to Mitigate
Threat Actor				
Russian Foreign Intelligence Service	• APT29 (*FireEye*) • UNC2452 (*FireEye*), • The Dukes (*F-Secure*) • Yttrium (*Microsoft)* • Nobelium (*Microsoft)* • Stellar Particle (*Crowdstrike*) • CozyBear (*Crowdstrike*)	4/15/21	• SVR cyber operations have posed a longstanding threat to the United States. Prior to 2018, several private cyber security companies published reports about APT29 operations to obtain access to victim networks and steal information, highlighting the use of customized tools to maximize stealth inside victim networks and APT 29 actors' ability to move within victim environments undetected. • Beginning in 2018, the FBI observed the SVR shift from using malware on victim networks to targeting cloud resources, particularly e-mail, to obtain information. The exploitation of Microsoft Office 365 environments following network access gained through use of modified SolarWinds software reflects this continuing trend. Targeting cloud resources probably reduces the likelihood of detection by using compromised accounts or system misconfigurations to blend in	Review NSA, DHS CISA, FBI Cybersecurity Advisory: Russian SVR Targets U.S. and Allied Networks: https://media.defense.gov/2021/Apr/15/2002621240/-1/-1/0/CSA_SVR_TARGETS_US_ALLIES_UOO13234021.PDF Review DHS CISA Alert AA21-116A: https://us-cert.cisa.gov/ncas/alerts/aa21-116a

[51] NOTE: Given the complicated nature of cyber forensics, multiple vendors and government agencies may use different names for an activity group, threat actor, or activity cluster. Additionally, the individual names' TTPs and IOCs developed by each vendor/agency may not map 100 percent to another vendor/agency's name for the actor. As such, a certain vendor may not be able to prove with high confidence that their particular actor or activity cluster "is" the Russian SVR. For unity of message purposes, the E-ISAC uses U.S. and Canadian government attribution claims where possible. This list of associated names is provided for awareness only so when members hear them, they can begin to associate it with other names they may have read.

Table 1: Key Terms				
Primary Name	**Associated Names[51]**	**Date**	**What it Does**	**Tools/Steps to Mitigate**
			with normal or unmonitored traffic in an environment not well defended, monitored, or understood by victim organizations.[52]	
SolarWinds Orion Platform				
SUNBURST malware *FireEye*	Solorigate *Microsoft*	12/13/20	- A trojanized version of a digitally signed SolarWinds Orion plugin called: SolarWinds[.]Orion.Core.BusinessLayer[.]dll	Visit FireEye's GitHub Site for SUNBURST Countermeasures: https://github.com/fireeye/sunburst_countermeasures

[52] DHS CISA Alert (AA21-116A), "Russian Foreign Intelligence Service (SVR) Cyber Operations: Trends and Best Practices for Network Defenders," April 26, 2021 - https://us-cert.cisa.gov/ncas/alerts/aa21-116a

Table 1: Key Terms				
Primary Name	**Associated Names**[51]	**Date**	**What it Does**	**Tools/Steps to Mitigate**
			• The plugin contains a backdoor that communicates via HTTP to third party servers. • After an initial dormant period of up to two weeks, SUNBURST may retrieve and execute commands that instruct the backdoor to transfer files, execute files, profile the system, reboot the system, and disable system services. • The malware's network traffic attempts to blend in with legitimate SolarWinds activity by imitating the Orion improvement program protocol and persistent state data is stored within legitimate plugin configuration files. • The backdoor uses multiple obfuscated blocklists to identify processes, services, and drivers associated with forensic, and anti-virus tools.[53]	Review DHS CISA MAR (AR21-039A): https://us-cert.cisa.gov/ncas/analysis-reports/ar21-039a
TEARDROP malware *FireEye*		12/13/20	• TEARDROP is a loader designed to decrypt and execute an embedded payload on the target system. • The payload has been identified as the Cobalt Strike Beacon Implant (Version 4) and provides a remote operator command and control capabilities over a victim system through an encrypted network tunnel. • The capabilities include the ability to rapidly exfiltrate data,	Visit FireEye's GitHub Site for SUNBURST Countermeasures: https://github.com/fireeye/sunburst_countermeasures Review DHS CISA MAR (AR21-039B): https://us-cert.cisa.gov/ncas/analysis-reports/ar21-039b

[53] FireEye, "SUNBURST Additional Technical Details," December 24, 2020 - https://www.fireeye.com/blog/threat-research/2020/12/sunburst-additional-technical-details.html

Table 1: Key Terms

Primary Name	Associated Names[51]	Date	What it Does	Tools/Steps to Mitigate
			log keystrokes, take screenshots, and deploy additional payloads.[54]	
SUNSPOT malware *Crowdstrike*		1/11/21	• SUNSPOT is a malware used by the actor to insert the SUNBURST backdoor into software builds of the SolarWinds Orion IT management product. • SUNSPOT monitors running processes for those involved in compilation of the Orion product and replaces one of the source files to include the SUNBURST backdoor code. • Several safeguards were added to SUNSPOT to avoid the Orion builds from failing, potentially alerting developers to the adversary's presence.[55]	Review Crowdstrike Malware Technical Analysis Blog: https://www.crowdstrike.com/blog/sunspot-malware-technical-analysis/
Raindrop malware *Symantec*		1/18/21	• A loader that is designed to decrypt and execute an embedded payload on the target system. • The payload has been identified as the Cobalt Strike Beacon Implant (Version 4) and provides a remote operator command and control capabilities over a victim system through an encrypted network tunnel. • The capabilities include the ability to rapidly exfiltrate data, log keystrokes, take screenshots, and deploy additional payloads.	Review DHS CISA Alert (AA21-077A) and the use of the CHIRP Indicators of Compromise Detection Tool: https://us-cert.cisa.gov/ncas/alerts/aa21-077a
SUPERNOVA malware *FireEye*		1/27/21	• FireEye identified several malicious artifacts affecting the	Review DHS CISA MAR (AR21-027A): https://us-

[54] DHS CISA MAR (AR21-039B): https://us-cert.cisa.gov/ncas/analysis-reports/ar21-039b

[55] Crowdstrike, "SUNSPOT: An Implant in the Build Process," January 11, 2021: https://www.crowdstrike.com/blog/sunspot-malware-technical-analysis/

Table 1: Key Terms				
Primary Name	**Associated Names**[51]	**Date**	**What it Does**	**Tools/Steps to Mitigate**
			SolarWinds Orion product as SUPERNOVA. - According to a SolarWinds advisory, SUPERNOVA is not embedded within the Orion platform as a supply chain attack; rather, it is placed by an attacker directly on a system that hosts SolarWinds Orion and is designed to appear as part of the SolarWinds product. - CISA's assessment is that SUPERNOVA is not part of the SolarWinds supply chain attack.[56] - SolarWinds states that the SUPERNOVA malware has two distinct parts, "a harmful, unsigned webshell .dll" developed especially for the Orion Platform and the second is an exploitation of a vulnerability (CVE-2019-8917) to "enable deployment of the malicious code."[57]	cert.cisa.gov/ncas/analysis-reports/ar21-027a
Microsoft 365/ Azure Cloud Environment				
SUNSHUTTLE malware *FireEye*	GoldMax *Microsoft*	3/4/21	- In August 2020, an entity based in the United States uploaded a new backdoor named SUNSHUTTLE to a public malware repository. - SUNSHUTTLE is a second-stage backdoor written in GoLang that features some detection evasion capabilities. - FireEye observed SUNSHUTTLE at a victim that was compromised by UNC2452 and had indications	Review DHS CISA Alert (AR21—105A): https://us-cert.cisa.gov/ncas/analysis-reports/ar21-105a Visit DHS CISA's GitHub Site for M365/Azure Tools

[56] DHS CISA AR21-027A, January 27, 2021 - https://us-cert.cisa.gov/ncas/analysis-reports/ar21-027a

[57] SolarWinds. "SolarWinds Security Advisory," December 24, 2020 - https://www.solarwinds.com/securityadvisory#anchor2

Table 1: Key Terms				
Primary Name	**Associated Names[51]**	**Date**	**What it Does**	**Tools/Steps to Mitigate**
			that it was linked to UNC2452, but this connection has not been fully verified.[58]	like Sparrow and Aviary: https://github.com/cisagov/Sparrow
Sibot malware *Microsoft*	MISPRINT	3/4/21	- A dual-purpose malware implemented in Visual Basic Script (VBScript), it is designed to achieve persistence on the infected machine then download and execute a payload from a remote C2 server. - The VBScript file is given a name that impersonates legitimate Windows tasks and is either stored in the registry of the compromised system or in an obfuscated format on disk. The VBScript is then run via a scheduled task. - Sibot reaches out to a legitimate but compromised website to download a DLL to a folder under *System32*. - Sibot uses a simplistic implementation allowing a low footprint for the actor as they can download and run new code without changes to the compromised endpoint by just updating the hosted DLL. - The compromised website used to host the DLL is different for every compromised network and includes websites of medical device manufacturers and IT service providers.	Review the Microsoft Security Blog: https://www.microsoft.com/security/blog/2021/03/04/goldmax-goldfinder-sibot-analyzing-nobelium-malware/ Review DHS CISA Alert (AR21—105A): https://us-cert.cisa.gov/ncas/analysis-reports/ar21-105a

[58] FireEye, "New SUNSHUTTLE Second-Stage Backdoor Uncovered Targeint U.S.-Based Entity,; Possible Connection to UNC2452, March 4, 2021 - https://www.fireeye.com/blog/threat-research/2021/03/sunshuttle-second-stage-backdoor-targeting-us-based-entity.html

Table 1: Key Terms

Primary Name	Associated Names[51]	Date	What it Does	Tools/Steps to Mitigate
GoldFinder malware *Microsoft*	SOLARFLARE	3/4/21	• GoldFinder can identify all HTTP proxy servers and other redirectors such as network security devices that an HTTP request travels through inside and outside the network to reach the intended C2 server • "Inform the actor of potential points of discovery or logging of their other actions, such as C2 communication with GoldMax."	Review the Microsoft Security Blog: https://www.microsoft.com/security/blog/2021/03/04/goldmax-goldfinder-sibot-analyzing-nobelium-malware/