Investigative Plan

Case Number: CYBER-21-0019-I
Case Title: Lazy Fortnite
Case Agent: (b) (6), (b) (7)(C) Special Agent
Judicial Venue: Criminal Division, CCIPS (Federal)
Case Category: ☒ Criminal ☐ Civil ☐ Administrative
Cooperating Agencies: N/A
Cooperating IG Offices: N/A

Synopsis of Allegations
Malicious software was introduced to the Treasury Department's information systems.

Possible Violation(s) of Law, Rule or Regulation
(b) (5) [redacted]

Focus and Objectives of the Investigation
The objective is to identify who was responsible for the introduction of malware on Treasury information systems. The focus is on those who were victimized and any potential loss of information incurred as a result.

(b) (5) [redacted]

Resources Necessary to Meet Investigative Requirements
Forensic equipment.

MEMORANDUM OF ACTIVITY

Case Number:	Reporting Office:	Type of Activity:
CYBER-21-0019-I	Investigations	LEO Activity - Record/Information Review
Date of Activity:	**Date Report Drafted:**	**Location of Activity:**
June 30, 2021	June 30, 2021	875 15th Street, NW, Washington DC
Subject of Activity:		**Activity Conducted By (Name(s) and Title(s)):**
Cybersecurity and Infrastructure Security Agency written directives		(b) (6), (b) (7)(C) Senior Special Agent

On December 13, 2021, Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) issued Emergency Directive 21-01, "Mitigate SolarWinds Orion Code Compromise". CISA describes the order as a binding operational directive requiring action by certain federal agencies. The US Department of the Treasury is one of the agencies bound by the directive. The directive is located at uniform resource locator cyber.dhs.gov/ed/21-01 (Attachment 1). Key requirements from the directive are summarized below.

The directive cites statutory authority stating CISA can direct agencies to take certain measures when there is an information security threat, and federal agencies are required to comply. The emergency directive included a list of five required actions. In order, they are:

1. Agencies with expertise should immediately

- forensically image affected SolarWinds products;
- capture memory of affected devices;
- look for new user or service accounts; and
- review stored network traffic for indicators of compromise.

CISA defines "expertise" as trained personnel equipped with tools needed to image a machine and collect its memory. Agencies without expertise were directed to proceed to step 2 below.

2. The second directive applied to all affected agencies, irrespective of expertise. Any affected SolarWinds products should be disconnected or powered down, and any account that was controlled by the threat-actor should be removed. All traffic to

or from an affected SolarWinds product should be blocked.

3. Agencies were required to report to CISA by December 14, 2020 if they had any of the following:

- a particular SolarWinds Orion Business Layer dll with a given hash value;
- the netsetupsvc dll in the SysWOW64 directory; or
- any other indicator of compromise.

4. After an agency removed threat-actor controlled accounts and removed any identified persistence mechanisms, they were to reset all credentials used by or stored in SolarWinds software, rebuild hosts monitored by affected SolarWinds products, and take actions to remediate kerberoasting.

5. The final step mandated Department-level Chief Information Officers submit a report attesting that all affected SolarWinds products have either been disconnected or powered down. The report was due to CISA December 14, 2020.

On January 6, 2021, CISA issued Supplemental Guidance v3. It superseded two previous iterations. The guidance provided a list of all affected SolarWinds products. It reiterated the categories of compromised networks. The three categories of compromised networks are:

- Category 1. Networks that never utilized the affected versions of SolarWinds.

- Category 2. Networks that used the affected SolarWinds products but show no indications, aside from beaconing, that threat actor conducted follow-on activity.

- Category 3. Networks that used the affected SolarWinds products and show evidence of follow-on threat actor activity.

In respect to Category 2 and Category 3 networks, agencies were required to keep hosts that ran affected versions of SolarWinds disconnected. CISA defined "disconnected" as disconnected from the network and powered on if the agency has or is seeking the capability to collect forensics images, or disconnected from the

network and powered off if there is no such capability.

CISA issued Supplemental Guidance v4 publicly on May 14, 2021. It provided additional required actions for agencies with networks showing evidence of follow-on threat-actor activity. An agency with a Category 3 network is required to complete pre-eviction instructions which were provided to the agency by CISA. Affected agencies were required to submit a status report to CISA by July 16, 2021.

Attachments:
1. Emergency Directive 21-01.pdf

Emergency Directive 21-01

Updated April 15, 2021: The U.S. Government attributes this activity to the Russian Foreign Intelligence Service (SVR). Additional information may be found in a statement from the White House. For more information on SolarWinds-related activity, go to https://us-cert.cisa.gov/remediating-apt-compromised-networks and https://www.cisa.gov/supply-chain-compromise.

See updated supplemental direction for the latest.

December 13, 2020

Mitigate SolarWinds Orion Code Compromise

This page contains a web-friendly version of the Cybersecurity and Infrastructure Security Agency's Emergency Directive 21-01, "*Mitigate SolarWinds Orion Code Compromise*".

Section 3553(h) of title 44, U.S. Code, authorizes the Secretary of Homeland Security, in response to a known or reasonably suspected information security threat, vulnerability, or incident that represents a substantial threat to the information security of an agency, to "issue an emergency directive to the head of an agency to take any lawful action with respect to the operation of the information system, including such systems used or operated by another entity on behalf of an agency, that collects, processes, stores, transmits, disseminates, or otherwise maintains agency information, for the purpose of protecting the information system from, or mitigating, an information security threat." 44 U.S.C. § 3553(h)(1)–(2)

Section 2205(3) of the Homeland Security Act of 2002, as amended, delegates this authority to the Director of the Cybersecurity and Infrastructure Security Agency. 6 U.S.C. § 655(3).

Federal agencies are required to comply with these directives. 44 U.S.C. § 3554 (a)(1)(B)(v)

These directives do not apply to statutorily-defined "national security systems" nor to systems operated by the Department of Defense or the Intelligence Community. 44 U.S.C. § 3553(d), (e)(2), (e)(3), (h)(1)(B).

Background

SolarWinds Orion products (affected versions are 2019.4 through 2020.2.1 HF1) are currently being exploited by malicious actors. This tactic permits an attacker to gain access to network traffic management systems. Disconnecting affected devices, as described below in Required Action 2, is the only known mitigation measure currently available.

CISA has determined that this exploitation of SolarWinds products poses an unacceptable risk to Federal Civilian Executive Branch agencies and requires emergency action. This determination is based on:

- Current exploitation of affected products and their widespread use to monitor traffic on major federal network systems;
- High potential for a compromise of agency information systems;
- Grave impact of a successful compromise.

CISA understands that the vendor is working to provide updated software patches. However, agencies must wait until CISA provides further guidance before using any forthcoming patches to reinstall the SolarWinds Orion software in their enterprise.

Please refer to the MITRE ATT&CK framework for possible tactics the threat actors are using to maintain persistence in the environment.

Required Actions

This emergency directive requires the following actions:

1. *Agencies that have the expertise to take the following actions immediately must do so before proceeding to Action 2.* ***Agencies without this capability shall proceed to Action 2.***

a. Forensically image system memory and/or host operating systems hosting all instances of SolarWinds Orion versions 2019.4 through 2020.2.1 HF1]. Analyze for new user or service accounts, privileged or otherwise.

b. Analyze stored network traffic for indications of compromise, including new external DNS domains to which a small number of agency hosts (e.g., SolarWinds systems) have had connections.

2. Affected agencies shall 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 entities to rebuild the Windows operating system and reinstall the SolarWinds software package, **agencies are prohibited from (re)joining the Windows host OS to the enterprise domain**. Affected entities should expect further communications from CISA and await guidance before rebuilding from trusted sources utilizing the latest version of the product available. Additionally:

   a. **Block all traffic** to and from hosts, external to the enterprise, where *any version of* SolarWinds Orion software has been installed.

   b. **Identify and remove** all threat actor-controlled accounts and identified persistence mechanisms.

3. **By 12pm Eastern Standard Time on Monday December 14, 2020 agencies shall report as an incident** to CISA (at https://us-cert.cisa.gov/report) the existence of any of the following:

   a. [SolarWinds.Orion.Core.BusinessLayer.dll] with a file hash of [b91ce2fa41029f6955bff20079468448]

   b. [C:\WINDOWS\SysWOW64\netsetupsvc.dll]

   c. Other indicators related to this issue to be shared by CISA

4. **After (and only after) all threat actor-controlled accounts and identified persistence mechanisms have been removed**:

   a. Treat all hosts monitored by the SolarWinds Orion monitoring software as compromised by threat actors and assume that further persistence mechanisms have been deployed.

   b. Rebuild hosts monitored by the SolarWinds Orion monitoring software using trusted sources.

   c. Reset all credentials used by or stored in SolarWinds software. Such credentials should be considered compromised.

   d. Take actions to remediate kerberoasting, including, as necessary or appropriate, engaging with a 3rd party with experience eradicating APTs from enterprise networks. For Windows environments, refer to the following:

      - See Microsoft's documentation on kerberoasting: https://techcommunity.microsoft.com/t5/microsoft-security-and/detecting-ldap-based-kerberoasting-with-azure-atp/ba-p/462448
      - Require use of long and complex passwords (greater than 25 characters) for service principal accounts and implement a good rotation policy for these passwords.
      - Replace the user account by Group Managed Service Account (gMSA). See https://docs.microsoft.com/en-us/windows-server/security/group-managed-service-accounts/group-managed-service-accounts-overview and Implement Group Managed Service Accounts: https://docs.microsoft.com/en-us/windows-server/security/group-managed-service-accounts/group-managed-service-accounts-overview.
      - Set account options for service accounts to support AES256_CTS_HMAC_SHA1_96 and not support DES, RC4, or AES128 bit encryption
      - Define the Security Policy setting, for Network Security: Configure Encryption types allowed for Kerberos. Set the allowable encryption types to AES256_HMAC_SHA1 and Future encryption types. https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-security-configure-encryption-types-allowed-for-kerberos
      - See Microsoft's documentation on how to reset the Kerberos Ticket Granting Ticket password, twice: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/ad-forest-recovery-resetting-the-krbtgt-password

5. By 12pm Eastern Standard Time on Monday December 14, 2020, **submit a report to CISA** using the provided template. Department-level Chief Information Officers (CIOs) or equivalents must submit completion reports attesting to CISA that the affected devices were either disconnected or powered down.

These requirements apply to any agency network utilizing the SolarWinds Orion product. This includes any information system used or operated by another entity on behalf of an agency, that collects, processes, stores, transmits, disseminates, or otherwise maintains agency information.

CISA Actions

- CISA will continue to work with our partners to monitor for active exploitation associated with this vulnerability. CISA will release additional indicators of compromise as they become available.
- CISA will provide additional guidance to agencies via the CISA website, through an emergency directive issuance coordination call, and through individual engagements upon request (via CyberDirectives@cisa.dhs.gov).

Duration

This emergency directive remains in effect until all agencies have applied the forthcoming patch or the directive is terminated through other appropriate action.

Additional Information

- General information, assistance, and reporting – CyberDirectives@cisa.dhs.gov
- Reporting indications of potential compromise – Central@cisa.dhs.gov

Frequently Asked Questions

Answers to common questions appear below.

What does the directive mean by "expertise"?

By "expertise", we mean that you have staff or supporting personnel that are properly trained in taking a forensic image of system memory and have tooling readily-available to immediately do so.

What does the supplemental guidance mean by "disconnected"?

By "disconnected" we mean *disconnected from the network and powered **on*** if the agency has the capability- or is seeking a capable service provider- to collect forensics images (system memory, host storage, network) off of the host or virtual machine, or *disconnected from the network and powered **off*** if there is no such capability.

Supplemental Guidance v3

January 6, 2021

This guidance supersedes the Emergency Directive (ED) 21-01 Supplemental Guidance v1 issued on December 18, 2020 and ED 21-01 Supplemental Guidance v2 issued on December 30, 2020. This version also supersedes Required Action 4 of ED 21-01. All other provisions of ED 21-01 remain in effect.

For reference, see older Emergency Directive 21-01 supplemental guidance.

Summary of Required Actions

This supplemental guidance v3 requires (1) agencies that ran affected versions conduct forensic analysis, (2) agencies that accept the risk of running SolarWinds Orion comply with certain hardening requirements, and (3) reporting by agency from department-level Chief Information Officers (CIOs) by Tuesday, January 19, and Monday, January 25, 2021.

Table Summarizing Conditions for Operating SolarWinds Orion

SolarWinds Orion Platform Version	Continued use of SolarWinds Orion permitted	Hardening required	Rebuild or upgrade	If rebuilding or continuing use of SolarWinds, configurations can be restored from backups
Affected versions: 2019.4 HF5, 2020.2 RC1, 2020.2 RC2, 2020.2, 2020.2 HF1	Yes, if network falls into Category 1 or 2[1]. If network is in Category 3, consult CISA before continuing use	Yes (Except SAML-based authentication on MS AD FS)	Full **rebuild**[2] of SolarWinds Orion infrastructure and reset of all accounts that are currently—or have been—used by the system	Yes, but only following the SolarWinds restore guidance [3]
Unaffected versions: All other versions	Yes	Yes–may require rebuild or reinstallation of SolarWinds components	**Upgrade** to latest version of SolarWinds Orion (at least version 2020.2.1HF2) and host OS (Windows Server 2016 or later)	Yes

Background

This document provides supplemental guidance v3 on the implementation of CISA Emergency Directive (ED) 21-01, to include an update on affected versions; guidance for ensuring all federal agencies operating unaffected platforms are using at least SolarWinds Orion platform version 2020.2.1HF2; guidance for agencies using third-party service providers; and additional clarity on required actions. CISA provides this guidance as the minimum required guidance for Federal Executive Branch Agencies subject to CISA's emergency directive authority.

This v3 supplemental guidance, which supersedes both v1 and v2 of the supplemental guidance and Required Action 4 of ED 21-01, is provided pursuant to ED 21-01.[4] All other provisions specified in ED 21-01 remain in effect.

ED 21-01 directed agencies to immediately disconnect or power down certain SolarWinds Orion platform versions from their network. Based on developing information, on December 18, 2020, CISA provided supplemental guidance listing a subset of versions that have been identified as containing a malicious backdoor AKA TEARDROP or SUNBURST ("affected versions"). All other versions of the SolarWinds Orion platforms, regardless of whether included in the original range identified in ED 21-01, have been identified as not containing that malicious backdoor ("unaffected versions").

Affected Versions

The following versions of SolarWinds Orion software are considered affected versions:

- Orion Platform 2019.4 HF5, DLL version 2019.4.5200.9083
- Orion Platform 2020.2 RC1, DLL version 2020.2.100.12219
- Orion Platform 2020.2 RC2, DLL version 2020.2.5200.12394
- Orion Platform 2020.2, DLL version 2020.2.5300.12432
- Orion Platform 2020.2 HF1, DLL version 2020.2.5300.12432[5]

Network Categorization

As it pertains to activity related to ED 21-01, federal networks fall into one of three categories, as defined in Activity Alert AA20-352A and briefly restated here for convenience.

- Category 1 – Networks that do not, and never did, utilize the affected versions of SolarWinds Orion.
- Category 2 – Networks that utilize or utilized affected versions of SolarWinds Orion but have forensically demonstrated[6] that, at most, only initial beaconing activity occurred, and the threat actor conducted no follow-on activity.
- Category 3 – Networks that utilized affected versions of SolarWinds Orion and have evidence of follow-on threat actor activity.

For the purposes of ED 21-01 and associated supplemental guidance, a network is defined as any computer network with hosts that share either a logical trust or any account credentials with SolarWinds Orion.

Networks with Affected Versions (Category 2 and 3)

Agencies that were using affected versions at any time prior to the issuance of ED 21-01[7] **must** comply with the following requirements:

1. **For Category 3 networks, agencies shall keep hosts that ran affected versions disconnected,**[8] as required by ED 21-01, and not rebuild or reimage the affected platforms and host operating systems (OS) **pending consultation with CISA.** This direction to keep such hosts disconnected also prohibits (re)joining the host OS to the enterprise domain. CISA's approval of the implementation of SolarWinds Orion may be conditioned on agencies observing safeguards that are specifically tailored to the unique architecture/threat profile of the agency's network. CISA will provide additional mitigation instructions to agencies in this category.

2. For Category 2 and 3 networks, take appropriate actions (e.g., labeling and isolating, and retaining as appropriate in accordance with applicable record retention requirements/with other cyber investigative records) with backups of affected versions to prevent accidental re-introduction of malicious code to the production environment.

3. For Category 2 and 3 networks, conduct forensic analysis as outlined in Appendix A - Required Forensics Investigation Actions.

4. For Category 2 networks, provide an update on the incident to CISA before returning affected versions of SolarWinds Orion to service. Rebuilding SolarWinds Orion shall occur only after a thorough forensic investigation has been conducted and the agency has confirmed that there is no observed adversary activity or secondary actions on objectives (AOOs),[9] confirming Category 2 activity only. The update to CISA shall list the mechanisms used to validate the absence of activity beyond Category 2 and recommend that the ticket be marked for closure. When resuming use of SolarWinds Orion in the environment after meeting these requirements, follow "Conditions for Operating SolarWinds Orion," below (including Appendix B).

Conditions for Operating SolarWinds Orion

All agencies that accept the risk of running SolarWinds Orion in their enterprises (regardless of whether they were required to disconnect their instance(s) pursuant to ED 21-01 and regardless of "Category") **must run at least version 2020.2.1 HF2** and meet additional conditions outlined in Appendix B - Specific Conditions for Operating SolarWinds Orion.[10] The National Security Agency (NSA) has examined this version and verified that it eliminates the previously identified malicious code. This version also includes updates to fix vulnerabilities unrelated to this malicious code, including vulnerabilities that SolarWinds has publicly disclosed.

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, as well as the SolarWinds Orion code itself (CISA is unable to assess the level of access the adversary may have had to other SolarWinds [non-Orion] code). 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. This adversary has demonstrated the capability and willingness to exploit SolarWinds Orion to compromise U.S. government agencies, critical infrastructure entities, and private organizations. Agencies considering the use of the SolarWinds Orion platform should balance these risks against benefits of using these products to support agency network visibility.

As noted in CISA's Activity Alert AA20-352A, CISA has evidence that the threat actor that inserted the SolarWinds backdoor also utilized initial access vectors that are unrelated to the SolarWinds Orion platform. Agencies should therefore also hunt for the tactics, techniques, and procedures (TTPs) as well as indicators of compromise (IOCs) related to this activity published in Activity Alert AA20-352A. Agencies should also consult any additional guidance related to this activity published by CISA or provided by the information security community. After completing the requirements of ED 21-01 and this supplemental guidance, agencies should focus on identifying potential account access abuse as well as identity impersonation as outlined in Activity Alert AA20-352.

Reporting Agency Status

For each agency, department-level Chief Information Officers (CIOs) or equivalents shall submit two additional status reports to CISA using the provided template by Tuesday, January 19, and Monday, January 25, 2021. Given the threat actor's interest in compromising identity, CISA is requiring agencies to provide additional details in order to map the possible threat space that was impacted as part of the compromise.

Federal Information Systems Hosted in Third-Party Environments (such as Cloud)

CISA is working closely with FedRAMP to coordinate the response to ED 21-01 with FedRAMP Authorized cloud service providers (CSPs). FedRAMP Authorized CSPs have been informed to coordinate with their agency customers. CISA is also aware of third parties providing services for federal information systems subject to ED 21-01 that may not be covered by a FedRAMP authorization.

Each agency is responsible for inventorying all their information systems hosted in third-party environments (FedRAMP Authorized or otherwise) and contacting service providers directly for status pertaining to, and to ensure compliance with, ED 21-01. If instances of affected versions have been found in a third-party environment, reporting obligations will vary based on whether the provider is another federal agency or a commercial provider.

- If the affected third-party service provider is another federal entity: The provider agency itself is responsible for reporting the incidents to CISA and the customer agency does not need to report anything further to CISA.
- If the affected third-party service provider is a commercial provider (FedRAMP Authorized or otherwise): If the provider confirms presence of affected versions (listed above), this is a cybersecurity incident per 44 U.S.C. § 3552(b)(2); the customer agency is responsible for reporting to CISA through https://us-cert.cisa.gov/report.

Incident reports must identify:

a) Category, per Mitigations section of CISA Activity Alert AA20-352A;

b) Name of affected third-party service (FedRAMP Authorized or otherwise);

c) Name(s) of affected FISMA information systems; and

d) Additional details on what data was exposed to the third-party service provider.

All other provisions specified in ED 21-01 remain in effect.

CISA Actions

- CISA will continue to work with our partners to respond to this activity. CISA will release additional IOCs as they become available.
- CISA will provide additional guidance to agencies via the CISA website, through an emergency directive issuance coordination call and through individual engagements upon request (via CyberDirectives@cisa.dhs.gov).

Additional Information

- General information, assistance, and reporting – CyberDirectives@cisa.dhs.gov
- Reporting indications of potential compromise – Central@cisa.dhs.gov

---

Supplemental Direction v4

April 22, 2021
(Publicly released on May 14, 2021)

This document provides supplemental direction on the implementation of CISA Emergency Directive (ED) 21-01, issued on December 13, 2020, and Supplemental Guidance v3 issued on January 3, 2021. All other provisions of ED 21-01 and Supplemental Guidance v1 through v3, to the extent not previously superseded, remain in effect. This direction provides agencies with specific instructions for incident triage and remediation.

In particular, this document provides additional required actions for agencies with networks that used affected versions of SolarWinds Orion and have evidence of follow-on threat actor activity. CISA provides this direction as the minimum additional required actions for Federal Executive Branch agencies subject to CISA's emergency directive authority.

Background

ED 21-01 and Supplemental Guidance v1 through v3 directed agencies to immediately disconnect or power down certain SolarWinds Orion platform versions from their network, conduct forensic investigation, and, for all SolarWinds Orion platforms that remained in operation, update the version and implement hardening requirements.

For the purposes of ED 21-01 and associated supplemental direction, a network is defined as any computer network with hosts that share either a logical trust or any account credentials with SolarWinds Orion. For example, systems within a shared identity boundary are within the same "network."

Required Actions

Agencies that have or had networks that used affected versions of SolarWinds Orion and have evidence of follow-on threat actor activity, such as binary beaconing to avsvmcloud[.]com and secondary C2 activity to a separate domain or IP address (typically but not exclusively returned in avsvmcloud[.]com CNAME responses), including networks hosted by third parties on behalf of federal agencies, must comply with the applicable requirements below for each network meeting these conditions.

Agencies must complete these actions by noon Eastern Daylight Time on Friday, July 16, 2021 or within 90 days of any future discovery of follow-on threat actor activity.

1. Execute and complete CISA-detailed *pre-eviction* instructions (to be provided by CISA directly to applicable agencies), and document and justify, deviations from the guidance, if any.

   Agencies that find evidence of additional adversarial activities based on the pre-eviction instructions described above must execute and complete CISA-detailed *eviction and post-eviction instructions* (to be provided by CISA directly to applicable agencies), and document and justify deviations from the eviction guidance, if any.

   If unable to complete all applicable requirements above by the applicable deadline, create and provide to CISA a detailed plan of action with scheduled completion date for the remaining requirements.

2. Submit a report to CISA using the provided reporting template. Department-level Chief Information Officers (CIOs) or equivalents must submit this report attesting agency status to CISA.

   Agencies must report their status to CISA upon request until all actions have been completed.

CISA Actions:

- CISA will work directly with applicable agencies to support their eviction efforts and confirm the completion of all required actions.

Additional Information

- For questions about required actions, and to request CISA assistance contact central@cisa.dhs.gov,
- General information, assistance, and reporting – CyberDirectives@cisa.dhs.gov,
- Reporting indications of potential compromise – https://us-cert.cisa.gov/report.

Appendix A – Required Forensics Investigation Actions

Agencies that ran affected versions of SolarWinds Orion platform (Category 2 and Category 3) at any time prior to the issuance of ED 21-01 must conduct system memory, host storage, network, and cloud forensic analysis and hunt for indicators of compromise (IOCs) or other evidence of threat actor activity, such as secondary actions on objectives (AOO)[11] as outlined in AA20-352A, such as user impersonation, privilege escalation, and data exfiltration.

1. Agencies running affected versions that have no capability to conduct forensic analysis (system memory, host storage, network, and cloud) shall, at minimum, hunt for IOCs or other evidence of threat actor activity published in ED 21-01, Activity Alert AA20-352A, and future associated guidance. Agencies that, through hunting and/or forensic analysis, find

these IOCs or evidence of threat actor activity, such as secondary AOO, shall assume breach and must report it as an incident to CISA through https://us-cert.cisa.gov/report. If a reporting agency already submitted incident information to CISA, please send updates to CISA as you discover new evidence.

2. Agencies running affected versions that have no capability to conduct forensic analysis and no capability to hunt for IOCs shall assume breach, report the incident to CISA through https://us-cert.cisa.gov/report, and contact Central@cisa.dhs.gov to coordinate finding a qualified service provider capable of conducting forensics. Agencies whose forensics service provider's analysis finds IOCs or evidence of threat actor activity, such as secondary AOO, shall update the incident report to CISA through https://us-cert.cisa.gov/report.

Appendix B - Specific Conditions for Operating SolarWinds Orion

Agencies that decide to run SolarWinds Orion platform may continue or resume doing so ***only if each of the following conditions are met:***

1. The agency assesses the risk of operating the SolarWinds Orion platform in agency production environments, and the agency accepts the residual risk.

2. All incoming and outgoing communications outside of the agency device network management enclave are denied, with additional assurance that communications to the public internet to and from hosts running SolarWinds Orion products has been blocked (as required by ED 21-01).

3. Cloud instances of Orion can only monitor cloud resources in that cloud infrastructure.

4. On premises instances of Orion must not be permissioned with any cloud/hosted identity accounts.

5. In cases where a rebuild is required, restoration of SolarWinds configuration may be done from the legacy database by following the SolarWinds restore guidance. Restoration for affected versions will differ from restoration for unaffected versions—agencies must ensure that they are following the correct restoration guidance.

6. Networks using affected versions of SolarWinds Orion, where permitted to rebuild, must take the following additional steps before rebuilding their SolarWinds Orion platform:

   a) Change all account credentials, or other shared secrets (such as SNMP strings) that are—or had been—utilized by the affected SolarWinds Orion device being rebuilt.

      i. Enable multi-factor authentication (MFA) for these credentials whenever possible;

      ii. Provide service accounts with the minimum level of privilege necessary for the role performed whenever possible; and

      iii. For accounts where MFA is not possible, require use of randomly generated long and complex passwords (greater than 25 characters) and implement a maximum 90-day rotation policy for these passwords.

   b) Remove all inbound trust relationships to the SolarWinds Orion device being rebuilt.

7. The agency updates the SolarWinds Orion platform to at least version 2020.2.1 HF2 and install and update the host to the latest supported build of Windows Server 2019 (preferred) or Windows Server 2016, hardened to agency standards.

8. The SolarWinds Orion server, the web server, and the database server instances must be installed on separate and dedicated hosts.

9. Agencies must follow the SolarWinds secure configuration (hardening) guidelines provided by the vendor, which can be found at: https://documentation.solarwinds.com/en/Success_Center/orionplatform/content/core-secure-configuration.htm, ***EXCEPT*** agencies shall ***not*** configure the SolarWinds software to implement SAML-based authentication that relies on Microsoft's Active Directory Federated Services. This configuration is currently being exploited by the threat actor associated with this activity.

10. The agency configures logging to ensure that all logs from the host OS, SolarWinds platform, and associated network logs are being captured and stored for at least 180 days in a separate, centralized log aggregation capability.

11. The agency ensures that the SolarWinds logs are being actively monitored by the agency SOC.
12. The agency implements subsequent SolarWinds Orion platform updates and security advisories within 48 hours of release.

Footnotes for Supplemental Guidance

1. For category definitions see Mitigations Section of https://us-cert.cisa.gov/ncas/alerts/aa20-352a. ↩
2. A new OS (the latest supported build, at least Windows 2016) and fresh installation of Orion (at least version 2020.2.1 HF2) from trusted media must be used for all affected versions. ↩
3. https://solarwinds.com/upgrading-your-environment/ ↩
4. On December 13, 2020, CISA issued ED 21-01 to mitigate the SolarWinds Orion code compromise. As noted in ED 21-01, CISA continues to work with our partners to monitor for active exploitation associated with this compromise and will continue providing updated guidance to agencies as new information becomes available. ED 21-01 also indicated that agencies must wait until CISA provides further guidance before using any forthcoming patches to reinstall the SolarWinds Orion software in their enterprise. CISA subsequently issued supplemental guidance v1 and v2, which, respectively, updated ED 21-01 to provide guidance on affected versions and clarify requirements for agencies using third-party service providers, and directed agencies continuing to use unaffected versions of SolarWinds Orion to update to version 2020.2.1 HF2 by December 31, 2020. ↩
5. V1 of this guidance included a single bullet that listed two platform versions for the same DLL. For clarity, v3 lists these platform versions that share the same DLL version number separately, as both are considered affected versions. ↩
6. See Appendix A for additional information ↩
7. This includes instances that may have been rolled back, rebuilt, or reimaged to unaffected version but that, at one time prior to the issuance of ED 21-01, used an affected version. ↩
8. By “disconnected” we mean disconnected from the network and powered on if the agency has the capability—or is seeking a capable service provider—to collect forensics images (system memory, host storage, network) off of the host or virtual machine, or disconnected from the network and powered off if there is no such capability. ↩
9. https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Seven_Ways_to_Apply_the_Cyber_Kill_Chain_with_a_Threat_Intelligence_Platform.pdf ↩
10. Per v2 of the guidance, agencies continuing to operate unaffected versions of SolarWinds Orion as of December 30, 2020 were required to update to version 2020.2.1HF2 by December 31, 2020. All agencies resuming use of SolarWinds Orion after this date are required to update before reintroducing to the environment. ↩
11. https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Seven_Ways_to_Apply_the_Cyber_Kill_Chain_with_a_Threat_Intelligence_Platform.pdf ↩

Return to top

MEMORANDUM OF ACTIVITY

Case Number:	Reporting Office:	Type of Activity:
CYBER-21-0019-I	Investigations	Interview - Victim
Date of Activity:	**Date Report Drafted:**	**Location of Activity:**
January 12, 2021	January 12, 2021	1500 Pennsylvania Avenue, NW, Washington DC
Subject of Activity:		**Activity Conducted By (Name(s) and Title(s)):**
(b) (6), (b) (7)(C) Sanctions Investigator, Office of Foreign Assets Control, (b) (6), (b) (7)(C)		(b) (6), (b) (7)(C), Senior Special Agent (b) (6), (b) (7)(C), Senior Special Agent

On January 12, 2021, Department of the Treasury, Office of Inspector General (TIG) Senior Special Agents (SSA) (b) (6), (b) (7)(C) and (b) (6), (b) (7)(C) interviewed (b) (6), (b) (7)(C) Sanction Investigator with the Office of Foreign Assets Control (OFAC), regarding the compromise of his government email address (b) (6), (b) (7)(C). Mr. (b) (6), (b) (7)(C) provided the following information during the interview.

(b) (6), (b) (7)(C) In (b) (6), (b) (7)(C), (b) (6), (b) (7)(C) served as an intern with the United States Treasury Department. He was provided the email address (b) (6), (b) (7)(C) for use during his internship but has not had access to it since. (b) (6), (b) (7)(C). When (b) (6), (b) (7)(C) joined Treasury in (b) (6), (b) (7)(C) he was assigned the email address (b) (6), (b) (7)(C).

(b) (6), (b) (7)(C) is assigned to OFAC's Office of Global Targeting (OGT). Under OGT is the Global Mid-Eastern and Russia Team and within this team, (b) (6), (b) (7)(C) is a subject matter expert for the Russia and Ukraine component. His supervisor is Section Chief (b) (6), (b) (7)(C) and her deputy is (b) (6), (b) (7)(C). There are nine people on the team. The others include:

- (b) (6), (b) (7)(C)
-
-
-
-

Case Number:	Subject of Activity (*Brief Description*):	Date of Activity:
CYBER-21-0019-I	(b) (6), (b) (7)(C)	January 12, 2021

- (b) (6), (b) (7)(C)
-

About four to five employees work the Russian and Ukraine group and four or five work Syria and Belarus issues.

A sanctions investigator is involved in targeting individuals or groups as a result of certain activity. The sanctions investigator gathers evidence and documents findings. The results are included in a legal document called an Evidentiary Memorandum, although it goes by other names in OFAC. A sanction can block assets and prohibit a person's access to the financial system.

A sanctions investigator also conducts research and is responsible for delisting. The latter is an investigative process which provides evidence needed to remove a sanctioned person or entity from the sanction's list.

Since joining OFAC in (b) (6), (b) (7)(C) (b) (6), (b) (7)(C) said he has worked on several themes. These include sanction efforts involving Russia, Ukraine, (b) (6), (b) (7)(C), a Russia and Ukraine cyber action, and Belarus.

On about June, 2019, (b) (6), (b) (7)(C) began working the (b) (6), (b) (7)(C) and En+ investigation. It had predated his arrival but he spends about 30% to 40% of his time on the investigation. (b) (6), (b) (7)(C) monitors compliance to ensure (b) (6), (b) (7)(C) is not controlling En+.

From January to March, 2020, (b) (6), (b) (7)(C) worked on the (b) (6), (b) (7)(C) and En+ investigation. Then, from March to July, 2020, (b) (6), (b) (7)(C) conducted actions aimed at (b) (6), (b) (7)(C), a wealthy Russian who (b) (6), (b) (7)(C) described as a proxy actor for the Russian government. (b) (6), (b) (7)(C) owns and controls the Internet Research Agency, funds the Private Military Contract (PMC), and is engaged in mining activity in Africa.

From July 2020 to September 2020, (b) (6), (b) (7)(C) looked into sanctions involving Belarus and he continued work on (b) (6), (b) (7)(C) and En+ compliance. The Belarus investigation concerns the suppression of those who protested the August 2020 election in Belarus.

Case Number:	Subject of Activity (*Brief Description*):	Date of Activity:
CYBER-21-0019-I	(b) (6), (b) (7)(C)	January 12, 2021

Between September 2020 through the end of the year, (b) (6), (b) (7)(C) continued to look at Belarus, Russian and Ukrainian issues, and he assisted the State Department on a sale of Russian military equipment to Turkey.

(b) (6), (b) (7)(C) was not sure when his government email transitioned to Office 365 but believed it may have been the summer of 2020, but he could not say for certain. (b) (6), (b) (7)(C) and his coworkers do not use the Microsoft communications platform "Teams" but they upload documents to SharePoint. These are often final versions of their products. They also have a local share drive. They communicate by their unclassified email and sometimes send attachments. They also email links to the aforementioned share drive. When information is classified they use the appropriate system to communicate information.

(b) (6), (b) (7)(C) was asked if he knew or communicated with the following people:

- (b) (6), (b) (7)(C)
- "Forensic Examiner" or any individual who may do computer forensics

(b) (6), (b) (7)(C) said he knew and works with (b) (6), (b) (7)(C) and believed he heard the name (b) (6), (b) (7)(C). He did not recognize any of the other names.

(b) (6), (b) (7)(C) joined (b) (6), (b) (7)(C) team in (b) (6), (b) (7)(C). Although Ms. (b) (6), (b) (7)(C) worked on a different Treasury entity before joining OFAC, (b) (6), (b) (7)(C) and (b) (6), (b) (7)(C) worked the (b) (6), (b) (7)(C) investigation together since June, 2019.

(b) (6), (b) (7)(C) has a Facebook account but rarely uses it. He believes it may have two photos on it but none of the information or photos relate him to his position at Treasury. He signed up for the account with his legal name but it is linked to an old (b) (6), (b) (7)(C) address. (b) (6), (b) (7)(C) has a LinkedIn account and it once included an entry referencing his (b) (6), (b) (7)(C) internship with Treasury, but (b) (6), (b) (7)(C) deleted the information

about 14 months ago. His LinkedIn profile lists (b) (6), (b) (7)(C) as his current employer.

(b) (6), (b) (7)(C) does not have a Twitter account but he once signed up for Instagram, even though he does not use it. His Gmail account is his first name and last name. (b) (6), (b) (7)(C) does not attend conferences and has never sent out a subpoena, which could have his name on it. He has handed out two business cards. One was to a US person who provided it to a Lithuanian contact, (b) (6), (b) (7)(C) believes.

(b) (6), (b) (7)(C) also said an OFAC investigation can be obtained via the Freedom of Information Act (FOIA). Normally, the lawyer for the sanctioned investigator requests the report but it will be redacted before sent out. Moreover, it does not include (b) (6), (b) (7)(C) name and it is scrubbed of metadata that may include information linking the reports to him. When the report is transmitted by email, it uses a generic OFAC group account email address.

Finally, (b) (6), (b) (7)(C) said he does not know how his email account would have been targeted.

MEMORANDUM OF ACTIVITY

Case Number:	Reporting Office:	Type of Activity:
CYBER-21-0019-I	Investigations	Interview - Witness
Date of Activity:	**Date Report Drafted:**	**Location of Activity:**
October 12, 2021	October 13, 2021	875 15th Street, NW, Washington DC
Subject of Activity: (b) (6), (b) (7)(C) Departmental Offices (b) (6), (b) (7)(C)		**Activity Conducted By (Name(s) and Title(s)):** (b) (6), (b) (7)(C), Senior Special Agent

On October 12, 2021, Department of the Treasury, Office of Inspector General (TIG) Senior Special Agent (SSA) (b) (6), (b) (7)(C) interviewed (b) (6), (b) (7)(C) regarding Treasury's Departmental Offices (DO) incident response plans and activities. (b) (6), (b) (7)(C) DO's Computer Security Incident Response Center (CSIRC) and was the primary coordinator of DO's incident response to the SolarWinds breach. (b) (6), (b) (7)(C) also serves as (b) (6), (b) (7)(C). He provided the following information.

The CSIRC team at DO is comprised of ten members and (b) (6), (b) (7)(C) overseas the team. The team was established in April 29, 2020. The CSIRC team, however, is not a full time position. It is fully implemented when a security incident occurs, such as the case of the SolarWinds breach, but is not otherwise staffed with full time personnel.

(b) (6), (b) (7)(C) said he is not the incident responder who sits behind the keyboard collecting evidence or reviewing log files. His principal activity is the coordination all computer incident response activities. Operations personnel conduct hands-on incident response activities but are based upon (b) (6), (b) (7)(C) efforts and guidance. He often sits in on many meetings, phone calls, and other communication efforts to ensure the CISRC is fulfilling its mission.

(b) (6), (b) (7)(C) said a principal takeaway from the SolarWinds breach concerns DOs ability to conduct computer incident response activities and day to day work activities. (b) (6), (b) (7)(C) believes DO is fully prepared and capable of handling a major cybersecurity incident. DO is also fully capable of conducting its day to day Information Technology (IT) responsibilities. However, DO is not capable of responding to a major

cybersecurity incident and conducting its day to day work activities at the same time. The principal limiting factor in conducting both activities concurrently is personnel.

(b) (6), (b) (7)(C) said the incident response plan currently in effect is adequate and did everything it needed to. (b) (6), (b) (7)(C) is concerned the success of the current response plan may cause it to be overburdened with extra items in effort to address any unforeseen cybersecurity concern. The plan, (b) (6), (b) (7)(C) said, is prescriptive enough to give direction on what needs done but not so overly detailed as to overburden response personnel with checklists or tasks that may not be needed or necessary for every cybersecurity incident.

As for the response to the computer breach itself, (b) (6), (b) (7)(C) said the response effort was "fantastic." DO was prepared and ready for a major incident. Their posture, planning, training, and other factors made them well prepared for a major cybersecurity incident. Once the breach was identified, the response went well because the team was ready.

(b) (6), (b) (7)(C) added more should have been done to detect the network breach. DO does not currently have a person who is dedicated to reviewing computer log files in effort to identify anomalous or suspicious computer activity. Had there been one, (b) (6), (b) (7)(C) argued, the network traffic caused by the infected SolarWinds appliances could have been identified and stopped earlier than it was. If Treasury collects more logs, there needs to be a person reviewing them, otherwise there is little value in collecting something that is never looked at. Logs can be collected and be useful in proving activity after a breach is found, but a person reviewing them on a routine basis can identify problems before they become worse.

Treasury's Shared Services Security Operations Center (TSSOC) collects and reviews logs but (b) (6), (b) (7)(C) said each network is different and the TSSOC is not familiar with what normal traffic looks like on DO's network. TSSOC reviewing log files is a possible solution but their understanding of other bureau's networks may make finding threats more challenging.

Microsoft and Mandiant both had incident response teams augment Treasury's incident response. (b) (6), (b) (7)(C) said both are great at a specific task but need direction

from the requesting party. Moreover, the contracted companies do not know the network like an agency's own personnel do. (b) (6), (b) (7)(C) said Treasury personnel were not sure what to expect from Mandiant and Microsoft. (b) (6), (b) (7)(C) believes Treasury can benefit by having its own full time, in-house incident response team, even if the team is small. (b) (6), (b) (7)(C) offered the team can be augmented with contracted incident response companies, like Mandiant, when a major incident arises. In this scenario, Treasury's incident response team would facilitate the integration of additional incident responders, provide direction to all participating personnel, and look for threats and other indicators of compromise when not actively responding to a cybersecurity incident.

Lastly, (b) (6), (b) (7)(C) said there is not a magical piece of software or hardware DO did not have when responding to the SolarWinds breach. What was lacking most is the personnel needed to respond to an incident. As organizations purchase more hardware and software, people are needed to manage them. (b) (6), (b) (7)(C) said the investment is being made into technology but the shortage is in people who can manage the technology.

MEMORANDUM OF ACTIVITY

Case Number:	Reporting Office:	Type of Activity:
CYBER-21-0019-I	Investigations	Interview - Witness
Date of Activity:	**Date Report Drafted:**	**Location of Activity:**
August 26, 2021	August 26, 2021	875 15th Street NW, Washington DC
Subject of Activity:		**Activity Conducted By (Name(s) and Title(s)):**
(b) (6), (b) (7)(C), TSSSOC (b) (6), (b) (7)(C)		SSA (b) (6), (b) (7)(C)

On August 26, 2021, Department of the Treasury, Office of Inspector General (TIG) Senior Special Agent (SSA) (b) (6), (b) (7)(C) interviewed (b) (6), (b) (7)(C) regarding Treasury's incident response plans and activities. (b) (6), (b) (7)(C) is (b) (6), (b) (7)(C) with the Treasury Shared Services Security Operations Center (TSSSOC), formerly the Government Security Operations Center (GSOC). (b) (6), (b) (7)(C) was asked about Treasury policies and procedures and actions taken in response to the SolarWinds compromise. He provided the following information.

(b) (6), (b) (7)(C) said TSSSOC and his team did a very good job addressing the SolarWinds breach. His biggest surprise occurred when the incident first came to light, an inability to communicate quickly and easily. The email system was known to be compromised so communications were not sent over email. The team began using Signal, an encrypted form of messaging, to communicate securely. Some in the Department of Homeland Security's Cybersecurity and Infrastructure Agency (CISA) followed suit. While the communications were slow at first, (b) (6), (b) (7)(C) noted TSSSOC was still able to fulfill its mission.

TSSSOC is the central authority for cybersecurity incidents in Treasury. They serve as the enterprise's security operations center and have a sort of supervisory responsibility over the other Treasury bureaus. Each bureau is responsible for its own response but all reporting funnels through TSSSOC. The TSSSOC provides guidance and assistance to bureaus as needed or requested. One of TSSSOC's main functions is analysis and monitoring of network traffic coming into and out of Treasury's computer network. TSSSOC monitors traffic in order to keep Treasury's network safe. Each bureau has its own Security Operations Center or Incident Response team that responds to incidents.

Case Number:	Subject of Activity (*Brief Description*):	Date of Activity:
CYBER-21-0019-I	(b) (6), (b) (7)(C)	August 26, 2021

TSSSOC was made aware of a possible security incident when Microsoft alerted Treasury of a problem in mid-December, 2020. TSSSOC was unaware of any intrusion activity prior to this notification. Once notified, (b) (6), (b) (7)(C) and his team immediately knew it was a major incident. They reported it to CISA almost immediately and were one of the first government agencies to know of a breach and report it. CISA later followed with a government wide directive action that Treasury was obligated to comply with. (b) (6), (b) (7)(C) addressed each of the requirements and said each was complied with.

Among the CISA directives was the requirement to collect forensic images and a memory capture of affected SolarWinds devices. This was done but took a couple months or so to complete in its entirety. (b) (6), (b) (7)(C) explained the reasons it took time. First, each bureau is responsible for collecting data from its own systems, and different bureaus have different capabilities. Second, Mandiant was brought in to assist in the response and that added additional coordination effort. CISA also came in and added yet another party to coordinate with. Third, the devices which hosted the SolarWinds products had been shut down, as per CISA directive, and so imaging took more effort. The devices running SolarWinds products are dispersed and in different data centers and cloud environments. The guidance on which machines could have been infected with the malicious code evolved over time as well. Finding and getting to each of the victim machines took time.

A memory capture was made of many machines but its analysis did not prove too fruitful. The malicious software likely ran many months prior and was no longer resident in memory, and since machines had been powered down to avoid further compromise, information which could have been resident was lost.

(b) (6), (b) (7)(C) said TSSSOC followed all the other CISA requirements such as looking through new user and service accounts, reviewing traffic for indicators of compromise, and notifying CISA if malicious files were found. (b) (6), (b) (7)(C) said each of these were done and TSSSOC was able to provide CISA even more information. In the course of its incident response activities, TSSSOC was able to identify other strains of malware and indicators of compromise. They provided this to CISA and Mandiant and it furthered other entities knowledge of the compromise.

(b) (6), (b) (7)(C) also said all SolarWinds machines were powered down and, to his knowledge, have not been brought up. He added he has not been involved in resurrecting SolarWinds products so it is possible some non-infected devices may have been brought up recently. (b) (6), (b) (7)(C) further said all SolarWinds products were shut down, even those which did not have the malicious software on them. This was done out of caution.

When Microsoft notified Treasury in mid-December 2020, the TSSSOC was in an all-hands mode and ran operations 24 hours a day, seven days a week for at least two straight months, to include weekends and the Christmas and New Year's holidays. (b) (6), (b) (7)(C) said everyone worked tirelessly from the moment they first got word of a problem. When asked what were some of the biggest challenges, (b) (6), (b) (7)(C) said log files. Treasury has a contract with Microsoft and the package Treasury paid for may not have include extended log file retention. Also, it was sometimes difficult getting logs from Microsoft.

Finally, (b) (6), (b) (7)(C) said Treasury Departmental Offices (DO) was the only entity which showed evidence of further adversarial activity, like lateral movement. He said other bureaus had been infected but no evidence was found to indicate they were further exploited. DO has its own incident response team and it is led by (b) (6), (b) (7)(C). (b) (6), (b) (7)(C) said (b) (6), (b) (7)(C) would have information concerning specific actions DO took in response to the intrusion.

MEMORANDUM OF ACTIVITY

Case Number:	Reporting Office:	Type of Activity:
CYBER-21-0019-I	Investigations	Interview - Victim
Date of Activity:	**Date Report Drafted:**	**Location of Activity:**
March 16, 2021	March 17, 2021	US Department of the Treasury, 1500 Pennsylvania Avenue NW, Washington DC
Subject of Activity:		**Activity Conducted By (Name(s) and Title(s)):**
(b) (6), (b) (7)(C)		(b) (6), (b) (7)(C), Senior Special Agent

On March 16, 2021, Department of the Treasury, Office of Inspector General (TIG) Senior Special Agent (SSA) (b) (6), (b) (7)(C) interviewed (b) (6), (b) (7)(C) (b) (6), (b) (7)(C) regarding the compromise of her government email address (b) (6), (b) (7)(C). (b) (6), (b) (7)(C) has served in her current position since (b) (6), (b) (7)(C) years of government service. Ms. (b) (6), (b) (7)(C) provided the following information during the interview.

(b) (6), (b) (7)(C) email address is (b) (6), (b) (7)(C) but her prior email address, which can still receive emails, is (b) (6), (b) (7)(C). The change from her earlier (b) (6), (b) (7)(C) account occurred about four years ago. (b) (6), (b) (7)(C) also has an older (b) (6), (b) (7)(C) account and this too can still receive emails. (b) (6), (b) (7)(C) does not have a classified email account.

In her capacity as (b) (6), (b) (7)(C), (b) (6), (b) (7)(C) schedules meetings, responds to emails, and answers phone calls. (b) (6), (b) (7)(C) said she has lots of interaction with White House staff members and the Secretary of the Treasury's office. (b) (6), (b) (7)(C) said one of her main efforts is scheduling meetings on behalf of the Deputy Secretary.

When meetings are scheduled, (b) (6), (b) (7)(C) uses generic titles. For example, during a dignitary visit, she might say, "Italian dignitary visit." (b) (6), (b) (7)(C) does not include many details in the meeting title. Also, (b) (6), (b) (7)(C) is not involved with any policy related issues. (b) (6), (b) (7)(C) does not send or receive emails concerning policy. She does not have access to the Deputy Secretary's email account but does have access to his calendar.

Currently, there is not a Senate confirmed Deputy Secretary. The last Deputy

Secretary that (b) (6), (b) (7)(C) worked with was Justin Muzinich. When he served as Deputy Secretary, he had a principal policy advisor named (b) (6), (b) (7)(C).

On or about late 2019 or early 2020, Deputy Secretary Muzinich assumed duties of Under Secretary when the former Under Secretary, Sigal Mandekler ((b) (6), (b) (7)(C) was not certain of the exact spelling), left the position. The responsibilities included overseeing Terrorist Financing and Intelligence. (b) (6), (b) (7)(C) said this effort created a significant amount of extra work for the Deputy Secretary and herself. It included matters she and the Deputy Secretary were not previously used to dealing with, like concerns regarding foreign entities and sanctions.

(b) (6), (b) (7)(C) left her physical office in room (b) (6), (b) (7)(C) of Main Treasury on or about March 18, 2020 due to health concerns and the COVID pandemic. She recently returned to the office for the first time in February, 2021. While she was away from her office, (b) (6), (b) (7)(C) had her Treasury issued laptop and phone so she was able to monitor her Treasury email account. However, (b) (6), (b) (7)(C), Muzinich's policy advisor, took care of most issues. After teleworking for some time, (b) (6), (b) (7)(C) said she had less to do and at one point did not have much at all to deal with.

(b) (6), (b) (7)(C) said she did not know her email account had been compromised and she had no idea why anyone would want to. (b) (6), (b) (7)(C) said she did not feel she was that important and did not understand what value would be in her emails. (b) (6), (b) (7)(C) also said she did not have social media accounts but did have a LinkedIn account. She was not sure if it was even active and she last accessed it a year and a half ago. Her LinkedIn account included references to her employment at the US Department of the Treasury.

(b) (6), (b) (7)(C) does not have any interaction with foreign citizens, outside of her official duties. (b) (6), (b) (7)(C) said she does not even know any outside of work.

MEMORANDUM OF ACTIVITY

Case Number:	Reporting Office:	Type of Activity:
CYBER-21-0019-I	Investigations	Records/Information - Obtained
Date of Activity:	**Date Report Drafted:**	**Location of Activity:**
December 14, 2020	December 15, 2020	Treasury OIG, 875 15th Street NW, Washington DC
Subject of Activity:		**Activity Conducted By (Name(s) and Title(s)):**
Treasury OIG Personnel		(b) (6), (b) (7)(C), Senior Special Agent

On December 14, 2020, multiple personnel from the Department of Treasury, Office of Inspector General (TIG) reviewed their phone and voicemail systems in effort to determine if TIG personnel had been notified of the breach of computer systems at the Department of the Treasury.

(b) (6), (b) (7)(C) reviewed the main telephone line and the hotline voicemail system but found no messages regarding a cyber breach or intrusion (Attachment 1).

(b) (6), (b) (7)(C), reviewed her voicemail inbox to search for any messages concerning a hack or data breach but she found none (Attachment 2).

Special Agent (b) (6), (b) (7)(C) was duty agent from December 7, 2020 to December 13, 2020. He did not receive a complaint or notification regarding a breach or computer intrusion at the Department of the Treasury (Attachment 3).

Attachments:
1. (b) (6), (b) (7)(C) Email
2. (b) (6), (b) (7)(C) Email
3. (b) (6), (b) (7)(C) Email

From: Luttrell, Sally
To: (b) (6), (b) (7)(C)
Subject: FW: Cyber Breaches
Date: Monday, December 14, 2020 11:31:30 AM

For your records

Sally Luttrell
Assistant Inspector General for Investigations
US Department of the Treasury
Office of Inspector General
Office of Investigations
(b) (6), (b) (7)(C)
875 15th ST NW
Washington, DC 20005

From: (b) (6), (b) (7)(C)
Sent: Monday, December 14, 2020 11:18 AM
To: McDowell, Sean A. (b) (6), (b) (7)(C) ; Luttrell, Sally (b) (6), (b) (7)(C)
Cc: (b) (6), (b) (7)(C) . (b) (6), (b) (7)(C)
Subject: Cyber Breaches

Good Morning,

I check the Office of Investigations main telephone line (202-927-5260) and the Hotline voicemail this morning for messages at 8:43 am, there were no messages regarding Cyber Breaches at that time. At 9:51am, I check the Office of Investigations main telephone line and Hotline voicemail again and there were no messages regarding Cyber Breaches. I than called (b) (6), (b) (7)(C) at the Front Office at 9:56am and I asked (b) (6), (b) (7)(C) to check her main telephone line voicemail, to see if there were any messages regarding Cyber Breaches left on the Front Office voicemail. At 10:21am (b) (6), (b) (7)(C) stated there were no messages left on the Front Office voicemail regarding Cyber Breaches.

Thank you

(b) (6), (b) (7)(C)
Department of the Treasury
Office of the Inspector General
Office of Investigations
875 15th Street NW
Washington, DC 20005

From: Luttrell, Sally
To: (b) (6), (b) (7)(C)
Subject: FW: Message concerning Data Breach
Date: Monday, December 14, 2020 12:33:53 PM

I have asked her who all has access to her VM.
I'll send her response once received.

Sally Luttrell
Assistant Inspector General for Investigations
US Department of the Treasury
Office of Inspector General
Office of Investigations
(b) (6), (b) (7)(C)
875 15th ST NW
Washington, DC 20005

From: (b) (6), (b) (7)(C)
Sent: Monday, December 14, 2020 12:30 PM
To: Luttrell, Sally (b) (6), (b) (7)(C)
Cc: Delmar, Richard K. (b) (6), (b) (7)(C)
Subject: Message concerning Data Breach

Hi Sally,

As requested, I went back into my voicemail box to see if we've received a message from anyone concerning the Hack/Data Breach to the U.S. Treasury Website. I found no message in the voicemail box, from last week or today. However, I must say, that I am not the only one with access to the voicemail box, but no one has reached out to me and said, that they've heard of any alert/message left concerning Treasury being hacked.

If you need to contact me, please do. I am still in the office for now.

You'll stay safe, take care, and enjoy your day.

Thanks,
(b) (6), (b) (7)(C)
Treasury, IG
1500 Pennsylvania Avenue, NW
MT - Room (b) (6), (b) (7)(C)
Washington, DC 20005
(b) (6), (b) (7)(C)

From: (b) (6), (b) (7)(C)
To: (b) (6), (b) (7)(C)
Subject: FW: Duty Agent Summary 07Dec20 -13Dec20
Date: Monday, December 14, 2020 12:58:36 PM

(b) (6), (b) (

Please see the below email from last week's Duty Agent. Thanks.

(b) (6), (b) (7)(C)
Assistant Special Agent in Charge
U.S. Department of the Treasury
Office of Inspector General
875 15th Street, NW
Washington, DC 20005
(b) (6), (b) (7)(C) desk
(b) (6), (b) (7)(C) cell

From: (b) (6), (b) (7)(C)
Sent: Monday, December 14, 2020 11:39 AM
To: (b) (6), (b) (7)(C) (b) (6), (b) (7)(C)
Cc: (b) (6), (b) (7)(C) (b) (6), (b) (7)(C)
Subject: Duty Agent Summary 07Dec20 -13Dec20

Sir,

As a follow up to our phone conversation, I can confirm that during my duty week the below is a summary of duty agent activity.

Complaint received via hotline intake. Complainant alleged that they were overcharged in the amount of $1,300 for a $20,000 CDFI funded loan. Complainant had already contacted USDA and their Congressional Representative regarding this complaint. A telephonic interview with the complainant was conducted and an MOA was uploaded into VIPER.

I received no additional complaints or notifications during my duty period.

Respectfully,

(b) (6), (b) (7)(C)
Special Agent
U.S. Department of the Treasury
Office of Inspector General
Office of Investigations
Washington, DC 20220
(W) (b) (6), (b) (7)(C)
(C) (b) (6), (b) (7)(C)

MEMORANDUM OF ACTIVITY

Case Number:	Reporting Office:	Type of Activity:
CYBER-21-0019-I	Investigations	Interview - Witness
Date of Activity:	**Date Report Drafted:**	**Location of Activity:**
December 15, 2020	December 15, 2020	US Department of the Treasury, 1500 Pennsylvania Avenue NW, Washington DC
Subject of Activity:		**Activity Conducted By (Name(s) and Title(s)):**
(b) (6), (b) (7)(C) [redacted] Information Systems (b) (6), (b) (7)(C) [redacted] Phone: (b) (6), (b) (7)(C) Email: (b) (6), (b) (7)(C) [redacted]		(b) (6), (b) (7)(C), Senior Special Agent

On December 15, 2020, Department of Treasury, Office of Inspector General (TIG) Senior Special Agent (SSA) (b) (6), (b) (7)(C) interviewed (b) (6), (b) (7)(C) regarding the breach notification process by Treasury personnel. (b) (6), (b) (7)(C) is the (b) (6), (b) (7)(C) [redacted]. She provided the following information.

(b) (6), (b) (7)(C) contacted TIG on December 13, 2020 for an emergency meeting concerning the breach of Treasury's computer systems. (b) (6), (b) (7)(C) said she called TIG's (b) (6), (b) (7) [redacted], at 5:53 p.m. at phone number (b) (6), (b) (7)(C). The mailbox was full, according to an automated recording. (b) (6), (b) (7)(C) notified (b) (6), (b) (7)(C) [redacted] that she was unable to get ahold of TIG's CIO, and (b) (6), (b) (7)(C) [redacted] replied that he could not either.

In addition, given security considerations at the time, use of email was limited. (b) (6), (b) (7)(C) attempted to contact all CIOs by phone. She was unable to get ahold of a different CIO in another Treasury entity. He replied to her later saying he was on a boat when he missed her call.

Notification was made to Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) within 24 hours of the incident, as per established protocol. The next notification, which is currently being addressed, is to Congress. It is due seven days after the incident. The FBI was not contacted, contrary to newspaper articles which indicated they had been.

Case Number:	Subject of Activity (*Brief Description*):	Date of Activity:
CYBER-21-0019-I	(b) (6), (b) (7)(C)	December 15, 2020

Aside from the breach notifications, (b) (6), (b) (7)(C) said there are eight accounts which were compromised in the breach. (b) (6), (b) (7)(C) did not recall all of them by memory but said she believed two or three of the compromised accounts were related to sanction investigations, another for an executive assistance to a deputy secretary, and some are IT accounts.

(b) (6), (b) (7)(C) said she is available at any time for future questions and asked that SSA (b) (6), (b) (7)(C) reach out if TIG needed any additional information.

MEMORANDUM OF ACTIVITY

Case Number:	Reporting Office:	Type of Activity:
CYBER-21-0019-I	Investigations	Interview - Victim
Date of Activity:	**Date Report Drafted:**	**Location of Activity:**
January 13, 2021	January 13, 2021	875 15th Street, NW, Washington DC
Subject of Activity:		**Activity Conducted By (Name(s) and Title(s)):**
(b) (6), (b) (7)(C) IT Specialist, Office of Chief Information Officer, (b) (6), (b) (7)(C)		(b) (6), (b) (7)(C) Senior Special Agent (b) (6), (b) (7)(C) Senior Special Agent

On January 13, 2021, Department of Treasury, Office of Inspector General (TIG) Senior Special Agents (SSA) (b) (6), (b) (7)(C) and (b) (6), (b) (7)(C) interviewed (b) (6), (b) (7)(C) Information Technology Specialist for Treasury's Office of Chief Information Officer (OCIO), regarding the compromise of his government email address (b) (6), (b) (7)(C). Mr. (b) (6), (b) (7)(C) provided the following information during the interview.

(b) (6), (b) (7)(C) has worked at the United States Treasury for the last (b) (6), (b) (7)(C). He is a GS-14 Information Technology Specialist responsible for the administration of Treasury email servers. (b) (6), (b) (7)(C) works for (b) (6), (b) (7)(C). (b) (6), (b) (7)(C) is an email administrator assigned to the messaging team. The messaging team is responsible for unclassified email, Skype, the Zix encryption service, and fax services. (b) (6), (b) (7)(C) works with (b) (6), (b) (7)(C).

(b) (6), (b) (7)(C) described his work as a sort of system administrator for Treasury's email servers. He assigns permissions but does not create accounts. A different section is responsible for email account creation. (b) (6), (b) (7)(C) used the example of a departed Treasury employee as a permission activity he would be engaged in. In this situation, a departed employee does not have access to his or her email account. (b) (6), (b) (7)(C) would assign a different Treasury employee permission to access the departed employee's account. An example would be a FOIA request in which a supervisor must access the departed employee's email to review messages which may be subject to the FOIA request.

(b) (6), (b) (7)(C) said the ongoing transfer to Microsoft's Office 365 platform has changed some of his responsibilities. Under the old system, when Treasury ran their own email

servers, he had to patch and update the servers. Now, Microsoft is responsible for the updates, but he remains responsible for permissions and other actions.

On or about December 29, 2020, (b) (6), (b) (7)(C) called (b) (6), (b) (7)(C) who was on vacation at the time, to inform him his email address had been changed. (b) (6), (b) (7)(C) learned it had been compromised thus the reason for the change. His compromised email address is (b) (6), (b) (7)(C) and it was a normal user account. It did not have administrative permissions. His other account, (b) (6), (b) (7)(C) is (b) (6), (b) (7)(C) privileged account, which does have administrative privileges but does not have an associated Office 365 email account. (b) (6), (b) (7)(C) was assigned the new address (b) (6), (b) (7)(C) to replace his compromised, regular user account. The compromised email address was disabled but not deleted. It exists but it cannot be accessed.

(b) (6), (b) (7)(C) said he routinely gets emails related to email servers and email problems. If someone gained access to his email, they could learn about Treasury email issues. (b) (6), (b) (7)(C) said he gets automated emails from SolarWinds when there is a problem with a mail server. (b) (6), (b) (7)(C) said (b) (6), (b) (7)(C) would have more information on how a notification is sent when SolarWinds identifies an issue.

(b) (6), (b) (7)(C) said he had no idea how or why his email account would have been targeted. He said he has a Facebook account but it is tied to a personal email account and does not include any information regarding his position at Treasury. He has an old LinkedIn account but he rarely accesses it. It does indicate (b) (6), (b) (7)(C) works for Treasury IT. (b) (6), (b) (7)(C) also has a Twitter and WhatsApp account but none of his accounts link to his Treasury email address.

(b) (6), (b) (7)(C) did not notice any suspicious emails or personal contacts of recent. He said he has not traveled overseas since Christmas of 2019, when he went to Nigeria.

MEMORANDUM OF ACTIVITY

Case Number:	Reporting Office:	Type of Activity:
CYBER-21-0019-I	Investigations	Interview - Victim
Date of Activity:	**Date Report Drafted:**	**Location of Activity:**
January 28, 2021	January 29, 2021	1500 Pennsylvania Avenue, NW, Washington DC
Subject of Activity: (b) (6), (b) (7)(C) Office of International Affairs, (b) (6), (b) (7)(C)		**Activity Conducted By (Name(s) and Title(s)):** (b) (6), (b) (7)(C) Senior Special Agent; (b) (6), (b) (7)(C) Senior Special Agent

On January 28, 2021, Department of the Treasury, Office of Inspector General (TIG) Senior Special Agents (SSA) (b) (6), (b) (7)(C) and (b) (6), (b) (7)(C) interviewed (b) (6), (b) (7)(C) regarding the compromise of his government email address (b) (6), (b) (7)(C). (b) (6), (b) (7)(C) provided the following information during the interview. The interview was conducted over a secure phone to (b) (6), (b) (7)(C) assignment in Belgium.

(b) (6), (b) (7)(C) is in Treasury's Office of International Affairs. (b) (6), (b) (7)(C). (b) (6), (b) (7)(C) reports to the Deputy Assistance Secretary for Europe and Eurasia, acting supervisor (b) (6), (b) (7)(C).

In his position, (b) (6), (b) (7)(C) works with almost every part of Treasury. He works often with Terror Finance and Intelligence (TFI), Office of Foreign Assets Control (OFAC), and almost all offices in International Affairs. (b) (6), (b) (7)(C) said he is a Treasury liaison, of sorts, and handles any issue concerning the US Treasury Department.

(b) (6), (b) (7)(C) routinely interacts with European Union (EU) partners, NATO, and other foreign personnel. His unclassified Treasury email address, (b) (6), (b) (7)(C), is known to many of these individuals. He also uses his Department of State email address since his assignment to Belgium in (b) (6), (b) (7)(C), (b) (6), (b) (7)(C). It is common for (b) (6), (b) (7)(C) to hand out business cards with his Treasury email address on it.

(b) (6), (b) (7)(C) email communications since July, 2020 include any and all issues he works on, such as policy issues, reports that may be issued, and anything sent to Treasury's Office of International Affairs. This includes discussions or information concerning

possible sanctions. (b) (6), (b) (7)(C) said someone reading his emails would gain insight into financial issues, particularly those involving Europe.

Prior to (b) (6), (b) (7)(C) was the (b) (6), (b) (7)(C) in Treasury's Office of International Affairs. He served in this position for a little over (b) (6), (b) (7)(C). In this capacity, (b) (6), (b) (7)(C) worked with G7 partners and managed US participation in the multi-lateral development banks. (b) (6), (b) (7)(C) addressed World Bank issues and policies, specifically those concerning the five multi-national development banks. (b) (6), (b) (7)(C) said he worked a lot with the European Bank for Reconstruction and Development (EBRD), (b) (6), (b) (7)(C).

According to (b) (6), (b) (7)(C) the EBRD had a lot of Russian presence and the EBRD previously invested in Russia. It stopped when Russia invaded Crimea.

(b) (6), (b) (7)(C) added that over the last three years he has worked on more issues involving China then Russia. (b) (6), (b) (7)(C) work at Treasury is not focused on only one country.

When (b) (6), (b) (7)(C) was asked if had heard of the name (b) (6), (b) (7)(C) he said it was a name he knew well. He said he worked on issues concerning (b) (6), (b) (7)(C) while assigned to the EBRD. (b) (6), (b) (7)(C) went on to state he is currently dealing with sanctions issues concerning a different Russian individual, but he could not immediately recall the name. (b) (6), (b) (7)(C) was asked if the person was (b) (6), (b) (7)(C) and (b) (6), (b) (7)(C) stated that it was. (b) (6), (b) (7)(C) is addressing sanctions issues regarding (b) (6), (b) (7)(C) and coordinating with the EU on the matter.

(b) (6), (b) (7)(C) has social media accounts. His LinkedIn account contains information related to his current and past positions at Treasury. He does not use his Facebook account much, and it is not public. (b) (6), (b) (7)(C) has a Twitter account but it does not have his name, he has not posted with it, and uses it to read other Tweets. (b) (6), (b) (7)(C) rarely ever uses his Instagram account.

(b) (6), (b) (7)(C) personal email addresses are (b) (6), (b) (7)(C) and (b) (6), (b) (7)(C).

MEMORANDUM OF ACTIVITY

Case Number:	Reporting Office:	Type of Activity:
CYBER-21-0019-I	Investigations	Records/Information - Obtained
Date of Activity:	**Date Report Drafted:**	**Location of Activity:**
December 15, 2020	December 15, 2020	Treasury OIG, 875 15th Street NW, Washington DC
Subject of Activity:		**Activity Conducted By (Name(s) and Title(s)):**
(b) (6), (b) (7)(C) Information Technology Specialist, Government Security Operations Center (GSOC) (b) (6), (b) (7)(C)		(b) (6), (b) (7)(C), Senior Special Agent (b) (6), (b) (7)(C), Senior Special Agent

On December 15, 2020, Department of the Treasury, Office of Inspector General (TIG) Senior Special Agents (b) (6), (b) (7)(C) and (b) (6), (b) (7)(C) phoned into the Government Security Operations Center's (GSOC) initial incident briefing regarding the compromise of Treasury computer systems. The conference call, attended by many other individuals in Treasury, was hosted by GSOC and the callers identified themselves as (b) (6), (b) (7)(C) and (b) (6), (b) (7)(C). (b) (6), (b) (7)(C) provided most of the information, to include the following.

On late Friday evening, December 11, 2020, Microsoft contacted Treasury personnel to advise they had high confidence an actor exploited Security Assertion Markup Language (SAML) certificates to gain access to cloud infrastructure, presumably Microsoft's cloud infrastructure. A certificate had been stolen from Treasury's Active Directory Federation Services (ADFS). The account conducting this activity was believed to come from the Treasury network itself, indicating an actor had gained access to, and was operating on, Treasury's systems.

The SolarWinds Orion platform is the means by which access to Treasury's network was made. The investigation found the SolarWinds software of interest was downloaded on about March, 2020. Malicious activity from this download began in April, 2020. Public reports indicate the software remains dormant for at least 12 days before activating. GSOC does not know what causes the malicious software to activate. Moreover, the malicious versions of SolarWinds do not have to be activated. It remains unclear how this process occurs.

Once the malicious SolarWinds program is activated, further instructions are sent via Extensible Markup Language (XML) files. The files may look like normal SolarWinds

traffic, and have Universal Resource Identifiers (URIs) designed to look like SolarWinds traffic. The domain names in the traffic, however, are not SolarWinds's domains. The domains are controlled by the intruder. After the infected client receives the instructions via XML files, the adversary begins lateral movement into other computer systems, but the way in which this is done is not yet clear.

The "crown jewel", as the GSOC briefer stated, is for the adversary to obtain the ADFS signing certificate. With this certificate, the adversary can create its own certificates for future use. This creates a persistent problem across the network, allowing continued access to information, like Microsoft Office 365 email accounts.

The GSOC remains in a data collection phase. Several Bureaus have identified a compromise on their system, but the number and name of the Bureau was not provided on the call. The GSOC continues to try to understand the extent of the compromise. They advised, however, not to trust DO email at this time. The GSOC has moved to the Signal application as the preferred means of communication.

From an Incident Response (IR) perspective, GSOC has identified some traffic of interest, but most of it is stale. The team continues to look for fresh indicators of compromise. The last reported activity indicating compromise was November 3, 2020. The caller, believed to be (b) (6), (b) (7)(C) also said November 5, 2020, but it was unclear which date it was.

An IR contract was made with FireEye for incident response, and consideration for a contract with CrowdStrike is ongoing. The GSOC has been in consultation with CISA and personnel from Ft. Meade as well.

MEMORANDUM OF ACTIVITY

Case Number:	Reporting Office:	Type of Activity:
CYBER-21-0019-I	Investigations	Interview - Witness
Date of Activity:	**Date Report Drafted:**	**Location of Activity:**
December 16, 2020	December 16, 2020	875 15th Street, NW, Washington DC
Subject of Activity:		**Activity Conducted By (Name(s) and Title(s)):**
(b) (6), (b) (7)(C) [redacted] Phone: (b) (6), (b) (7)(C)		(b) (6), (b) (7)(C), Senior Special Agent

On December 16, 2020, Department of the Treasury, Office of Inspector General (TIG) Senior Special Agent (SSA) (b) (6), (b) (7)(C) interviewed (b) (6), (b) (7)(C), (b) (6), (b) (7)(C) [redacted], to determine if he received a missed call on Sunday evening, December 13, 2020. Previously, (b) (6), (b) (7)(C) advised she made telephonic notification to Bureau Chief Information Officers (CIOs) to inform them of an emergency briefing regarding the intrusion of Treasury's computer systems. (b) (6), (b) (7)(C) was included in the list of individuals (b) (6), (b) (7)(C) called.

(b) (6), (b) (7)(C) confirmed his work cell phone number is (b) (6), (b) (7)(C) and he holds (b) (6), (b) (b) (6), (b) (7)(C). (b) (6), (b) (7)(C) had not checked his work phone for missed calls recently but reviewed them during the interview and said he had a missed call on Sunday, December 13, 2020, at 5:53 p.m., from phone number (b) (6), (b) (7)(C). It was the only call (b) (6), (b) (7)(C) received on Sunday. The aforementioned phone number is used by (b) (6), (b) (7)(C) SSA (b) (6), (b) (7)(C) spoke to Ms. (b) (6), (b) (7)(C) at this number the day prior.

Following the interview, (b) (6), (b) (7)(C) checked his cellphone voicemail inbox to determine if it was full, as Ms. (b) (6), (b) (7)(C) said it was. (b) (6), (b) (7)(C) informed (b) (6), (b) (7)(C) his voicemail was indeed full. (b) (6), (b) (7)(C) was also asked if he had received a call from (b) (6), (b) (7)(C), to which (b) (6), (b) (7)(C) replied that he had not.

Lastly, (b) (6), (b) (7)(C) recommended future emergency notifications use the Ad-Hoc email notification system.

MEMORANDUM OF ACTIVITY

Case Number:	Reporting Office:	Type of Activity:
CYBER-21-0019-I	Investigations	Interview - Witness
Date of Activity:	**Date Report Drafted:**	**Location of Activity:**
January 21, 2021	January 21, 2021	1500 Pennsylvania Avenue, NW, Washington DC
Subject of Activity:		**Activity Conducted By (Name(s) and Title(s)):**
(b) (6), (b) (7)(C) Information Technology Specialist, (b) (6), (b) (7)(C)		(b) (6), (b) (7)(C) Senior Special Agent

On January 21, 2021, Department of the Treasury, Office of Inspector General (TIG) Senior Special Agent (SSA) (b) (6), (b) (7)(C) interviewed (b) (6), (b) (7)(C), Information Technology Specialist, regarding the compromise of the government email address (b) (6), (b) (7)(C). (b) (6), (b) (7)(C) provided the following information.

(b) (6), (b) (7)(C) Treasury email address is (b) (6), (b) (7)(C). He is also assigned the address (b) (6), (b) (7)(C). (b) (6), (b) (7)(C) said he never uses the (b) (6), (b) (7)(C) account and no one else does. Its purpose was for FOIA material, but he uses his official Treasury email address instead. (b) (6), (b) (7)(C) said he used the (b) (6), (b) (7)(C) account once, when he had to update the EnCase forensic tool software license. He said the (b) (6), (b) (7)(C) email account is tied to the EnCase license. It was the only time (b) (6), (b) (7)(C) used the account.

The (b) (6), (b) (7)(C) account has some low level privileges. It is not tied to (b) (6), (b) (7)(C) PIV. (b) (6), (b) (7)(C) uses a username and password to log into the (b) (6), (b) (7)(C) account.

The (b) (6), (b) (7)(C) account was used in 2016, when (b) (6), (b) (7)(C) predecessor managed it. The last time the account received an email was one year ago. The email was in regards to the EnCase license update. (b) (6), (b) (7)(C) surmised an intruder would use the (b) (6), (b) (7)(C) account as a test, since it is never used and is not tied to a specific user's name.

MEMORANDUM OF ACTIVITY

Case Number:	Reporting Office:	Type of Activity:
CYBER-21-0019-I	Investigations	Interview - Victim
Date of Activity:	**Date Report Drafted:**	**Location of Activity:**
February 2, 2021	January 2, 2021	875 15th Street, NW, Washington, DC
Subject of Activity:		**Activity Conducted By (Name(s) and Title(s)):**
(b) (6), (b) (7)(C) Office of Foreign Asset Control		(b) (6), (b) (7)(C), Senior Special Agent

On February 2, 2021, Department of the Treasury, Office of Inspector General (TIG) Senior Special Agent (b) (6), (b) (7)(C) and two officers from the Department of the Treasury, Office of Counterintelligence (OCI) conducted an interview with Office of Foreign Assets Control (OFAC) (b) (6), (b) (7)(C) (b) (6), (b) (7)(C) made the following comments and statements during the interview:

(b) (6), (b) (7)(C) has been working for OFAC since (b) (6), (b) (7)(C) in their Office of Enforcement. The mission of the Office of Enforcement is to enforce sanctions implemented by other offices within OFAC.

(b) (6), (b) (7)(C) stated that the Office of Enforcement receives leads regarding violations of sanctions from many different places including public information and informants, but added that many violations are self-reported by the companies. Once these leads are received she often sends subpoenas for additional information and issues cautionary letters to the violators. These may lead to Public Enforcement Actions including fines for more egregious violations.

All individuals working in the Office of Enforcement are generalist, but (b) (6), (b) (7)(C) is assigned significant work involving the Global Magnitsky Act and North Korea, while also working cases involving Iran and Cuba. (b) (6), (b) (7)(C) added that much of her work involves entities that are newly sanctioned as there are higher numbers of voluntary disclosures related to these entities.

(b) (6), (b) (7)(C) noted that she had worked recent cases involving the Magnitsky Act, XPCC, relating to the Chinese use of Uyghur labor, Hong Kong, and other high level human rights abuse. She also recently worked a technology case involving Apple in which a public action was taken. She did draft a written statement regarding the Apple

case for the OFAC website, but was given specific instructions from the OFAC web team to strip the PDF document she submitted of identifying details prior to submitting it.

(b) (6), (b) (7)(C) noted that her name is only tied to these cases internally, and is not publicly released with any actions she is involved with, and that email communications she has regarding her cases are typically not pre-decisional.

(b) (6), (b) (7)(C) does occasionally send Requests for Information (RFI's) and subpoenas to companies from her Treasury email address, and noted that she does not typically sanitize these documents of metadata.

The drafting and approval process for (b) (6), (b) (7)(C) work products go through the OFAC administrative records system OASIS, which (b) (6), (b) (7)(C) believes is a front-end application supported by SharePoint. Initial Disclosures received through a group mailbox are assigned to (b) (6), (b) (7)(C) and others through OASIS. (b) (6), (b) (7)(C) has access through OASIS to Enforcement and Compliance work products along with Records and Licensing work products. (b) (6), (b) (7)(C) does not have access to the Office of Global Targeting data set within OASIS. OASIS is secured by and accessed through credentials stored in (b) (6), (b) (7)(C) PIV card. (b) (6), (b) (7)(C) does not have the option to sign in to OASIS using a user name and password.

(b) (6), (b) (7)(C) has given group talks along with the Bureau of Industry and Security and the Commerce Department to industry participants, where she talks about OFAC sanctions programs. (b) (6), (b) (7)(C) does not have business cards and doesn't typically give her email and/or phone number out.

(b) (6), (b) (7)(C) does have a LinkedIn profile that indicates that she works for OFAC (b) (6), (b) (7)(C) , but that page does not have a photograph of her. She also has Facebook and Instagram accounts that may mention her previous employment at (b) (6), (b) (7)(C) These accounts are not linked to her Treasury email account, but rather are linked to her Gmail account (b) (6), (b) (7)(C)

(b) (6), (b) (7)(C) uses her OFAC-issued laptop to work remotely from home, accessing the OFAC network via DORA. She does not check her personal email from her work computer as it is blocked by DORA.

(b) (6), (b) (7)(C) is currently working cases that involve Facebook, SAP and NewTek that are going through the penalty process. She is also working cases in which she has issued or sent cautionary letters via email including NCH Capitol, CarMax, Spacial Networks, DHL Express. She is also working an investigation on an individual, (b) (6), (b) (7)(C) for dealing with a Specially Designated National (SDN) and Sophos, which involves Anti-Virus software sales in Iran, Cuba, Ukraine and Russia. She noted that the case number of the Sophos investigation disappeared in Sophos in April of 2020 unexpectedly and OFAC was unable to determine why or how. Finally, she is working an investigation into Apple, in which a warning notice has been issued. This case relates to the Magnitsky Act designation of (b) (6), (b) (7)(C)

MEMORANDUM OF ACTIVITY

Case Number:	Reporting Office:	Type of Activity:
CYBER-21-0019-I	Investigations	Interview - Witness
Date of Activity:	**Date Report Drafted:**	**Location of Activity:**
December 18, 2020	December 18, 2020	US Department of the Treasury, 1500 Pennsylvania Avenue, NW, Washington DC
Subject of Activity:		**Activity Conducted By (Name(s) and Title(s)):**
(b) (6), (b) (7)(C) [redacted]		(b) (6), (b) (7)(C), Senior Special Agent

On December 18, 2020, Department of Treasury, Office of Inspector General (TIG) Senior Special Agent (SSA) (b) (6), (b) (7)(C) spoke with (b) (6), (b) (7)(C) who provided an update on Treasury's response to the computer breach and the extent of the intrusion. (b) (6), (b) (7)(C) hosted the call by merging (b) (6), (b) (7)(C) and SSA (b) (6), (b) (7)(C) by phone. (b) (6), (b) (7)(C) provided the following update. It is the information known to him as of December 18, 2020.

There were 57 SolarWinds software implementations in the Department of the Treasury. Of those, 19 were found to be vulnerable. Four of the 19 vulnerable instances show some element of command and control (C2) activity. The four entities that have shown C2 activity are OCC, OFR, TTB, and DO.

DO is the only one of the four C2 victims to show signs of activity beyond command and control. The DO network showed possible malicious activity related to Microsoft's 365 program.

There are eight, known compromised accounts related to the implementation of Microsoft Office 365. Four of the compromised accounts do not have any data associated with them. These four accounts were not migrated to Office 365 thus no data was associated to the users' accounts. Four others, however, had data associated since they had migrated to Office 365. Two were OCIO accounts and two were not.

Counter Intelligence has been engaged and apprised of the breach.

(b) (6), (b) (7)(C) said he would provide a copy of the images being taken of the victimized

Case Number:	Subject of Activity (*Brief Description*):	Date of Activity:
CYBER-21-0019-I	(b) (6), (b) (7)(C)	December 18, 2020

SolarWinds instances, but the priority is Mandiant as they are providing incident response. The images will be centralized at the Government Security Operations Center (GSOC) but are not yet ready. The size of the data to image is larger than the capacity to hold it.

Lastly, (b) (6), (b) (7)(C) said he would like to be notified if TIG becomes aware of any other threats. He said there are news reports of various cyber threats, but he does not know which ones are accurate and which are not. (b) (6), (b) (7)(C) said he wants to address any threat that TIG may be aware of. He also asked that TIG inform him, at any time, if there are problems or concerns regarding compliance to law or regulation.

Report of Investigation

Case Information:

Complaint Number	CYBER-21-0019-I
Complaint Title	Lazy Fortnite
Date Closed	December 15, 2021
Subject Type	[Unknown]
Allegation Location	District of Columbia
Confidentiality	No
Congressional Interest	Yes
Cooperating Agencies	Federal Bureau of Investigation
Allegation(s)	Cyber,Misuse of Government Computer,Theft

Closing Summary:

On November 1, 2021, the OIG completed its report of investigation regarding the unauthorized access of several Treasury employees' email accounts, which was caused by a malicious program provided to Treasury by an authorized software vendor. Affected Treasury personnel were notified of the incident and the nature of their work was reviewed to determine the extent of harm to Treasury. The FBI is leading a government wide national security investigation.

Approval:

Andrea L. Peacock Digitally signed by Andrea L. Peacock
Date: 2021.12.15 01:57:55 -05'00'

Special Agent in Charge

Report of Investigation

Subject(s):

Unknown,