Analysis of SolarWinds from the perspective of Cyber Threat Intelligence

Dinusha Dissanayaka

(a.d.dissanayaka@edu.salford.ac.uk)

@00608177

Abstract

Cybercrime has wreaked havoc on individuals, businesses, and even governments in recent years. Methods for detecting and classifying cybercrime have yielded various degrees of effectiveness in preventing and safeguarding data from such attacks. Several laws and measures have been put in place to combat cybercrime, with culprits facing stiff penalties.

One of the most complex and large-scale cyber operations ever identified is the SolarWinds computer hack. The operation, according to the US administration, is an intelligence collecting effort carried out by an actor who is most likely Russian in origin. Across the country, the operation has impacted federal institutions, courts, several private sector companies, and state and local governments. It's an example of a digital supply chain attack, in which hackers inject harmful code into trusted third-party software, possibly infecting the whole client base of the hacked organisation. (SENATOR ROY BLUNT, CHAIRMAN, 2021)

The purpose of this paper is to examine SolarWinds from the standpoint of Cyber Threat Intelligence (CTI). It describes the attackers' techniques, tactics, and procedures (TTPs) for spreading malware and infecting their target. This paper also includes a list of cyber security recommendations for protecting networks from these kinds of attacks.

1. Introduction

The computer attack of SolarWinds is a major security concern for the United States. Across the country, the operation has impacted federal agencies, federal courts, countless private-sector enterprises, and state and local governments. It is one of the most advanced cyberattacks ever carried out. Only a few countries could put up the work and money required to carry out an operation of this magnitude, technical skill, and apparent goal.

The operation is a digital supply chain attack, in which cybercriminals inject harmful code into trusted third-party software, possibly infecting the whole client base of the compromised software business. The attackers were thorough in concealing their tracks and went to great lengths to avoid being discovered. (Microsoft, 2021) The campaign's actors obtained access to a variety of public and private organisations around the world. Through trojanized updates to SolarWind's Orion IT monitoring and management software, they got access to victims. SolarWinds' customers downloaded the Orion upgrade in March and April, therefore the campaign might have started as early as February 2020. By May of 2020, the attackers had

gained access to the targeted networks and were reading emails and other documents. Lateral movement and data theft have been reported as part of the post-compromise activity of this supply chain breach. The operation was carried out with substantial operational security and was the result of a highly skilled actor. (FIREEYE, 2020) For the next eight months, they remained undiscovered. This infamous SolarWinds supply chain breach has been also known as "Solorigate" by Microsoft. (Ingalls, 2021)

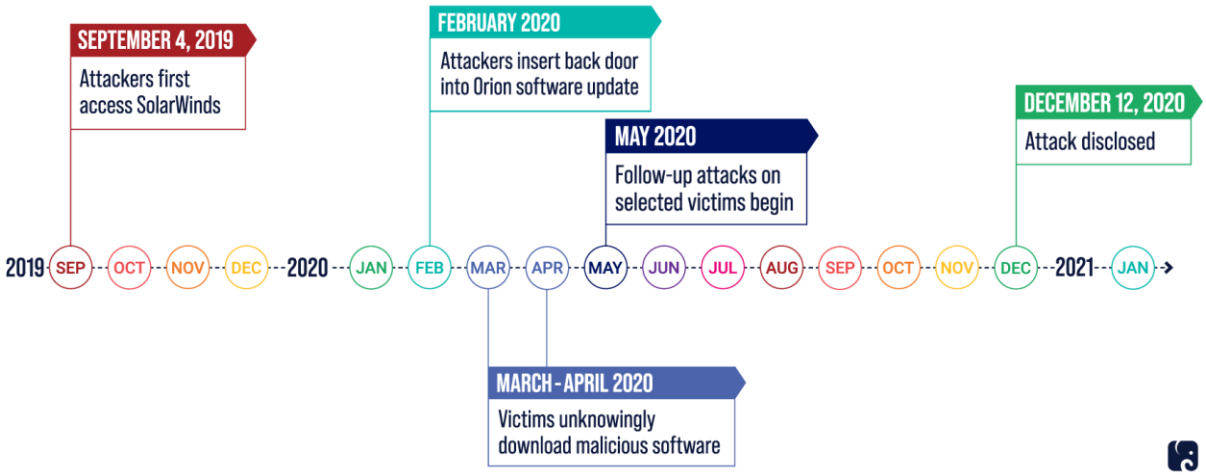


Figure 1: Timeline of SolarWinds attack (SENATOR ROY BLUNT, CHAIRMAN, 2021)

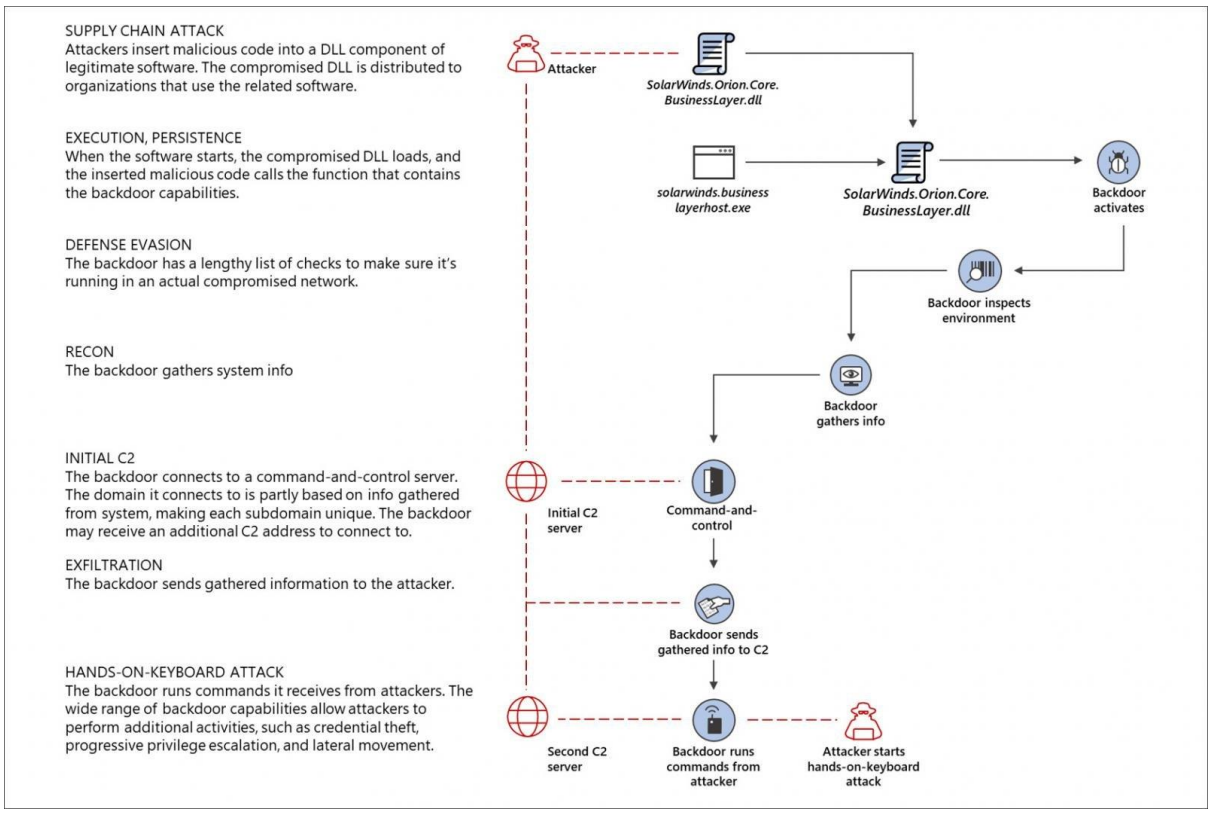


Figure 2: SolarWinds supply chain attack (Abrams, 2020)

Threat actors obtained access to the SolarWinds Orion build system and installed a backdoor in the legitimate SolarWinds.Orion.Core.BusinessLayer.dll DLL file as part of the attack. In a supply chain attack, this DLL was then delivered to SolarWinds customers using an automatic update mechanism that was utilised to push out new software updates (refer Figure 2). The DLL was signed and certified by the producer “SolarWinds”, as shown in Figure 3.

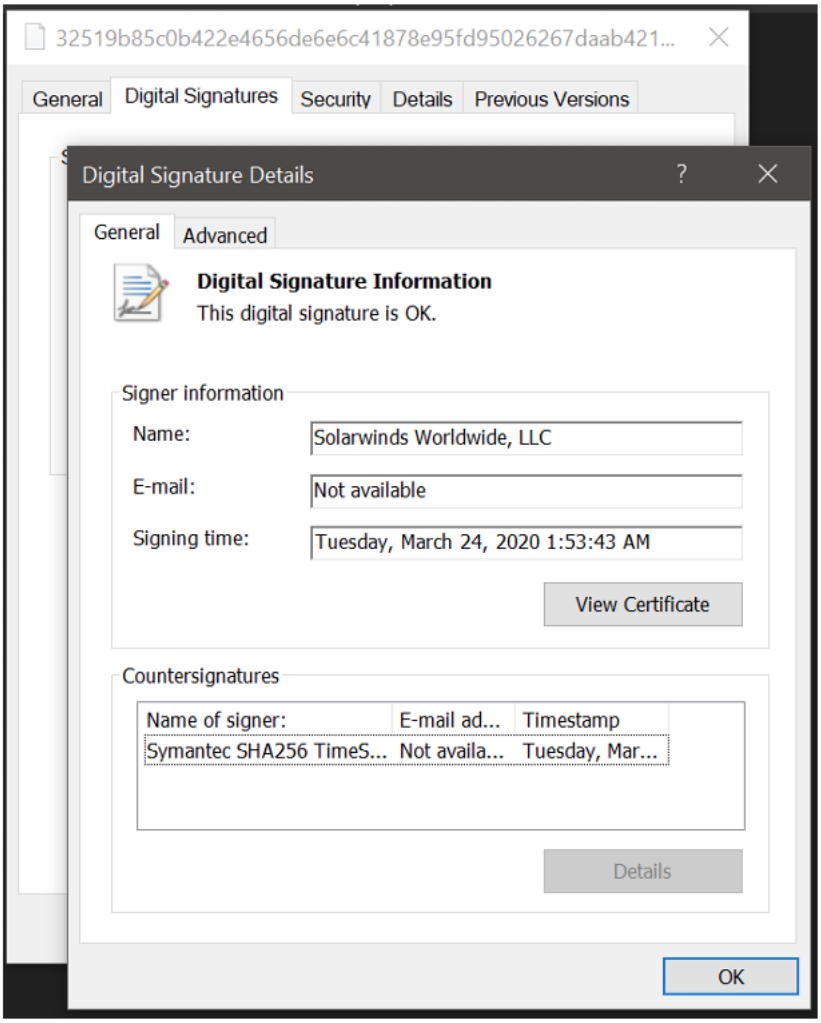


Figure 3 : SolarWinds.Orion.Core.BusinessLayer.dll malware file with the digital signature (FIREEYE, 2020)

The SolarWinds.BusinessLayerHost.exe software loads this DLL backdoor, which is known as Sunburst (FireEye) or Solorigate (Microsoft). Once loaded, it will connect to avsvmcloud[.]com's remote command and control server to receive "jobs," or tasks, to perform on the infected computer (as sjown in Figure 4).

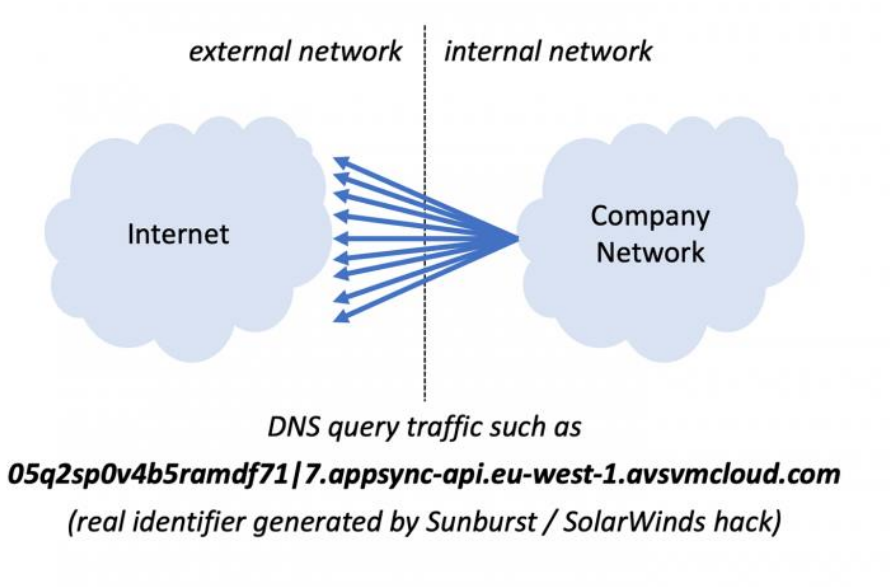


Figure 4: DNS query traffic (Stuker, 2021)

A domain creation algorithm (DGA) is used to establish an encoded subdomain of avsvmcloud[.]com for the backdoor's command control server. The subdomain is made by hashing "a victim userId with a reversible encoding of the victims local machine domain name," according to FireEye. '1btcr12b62me0buden60ceudo1uv2f0i.appsync-api.us-east-2[.]avsvmcloud.com,' is a subdomain utilised in this attack. (Abrams, 2020)

2. BACKGROUND – LITERATURE REVIEW, SCOPE & LIMITATIONS

SolarWinds is a firm established in Austin, Texas that supplies businesses and government organisations with large-scale information technology infrastructure management software and services. It serves over 320,000 customers in 190 countries, including 499 Fortune 500 companies. (SENATOR ROY BLUNT, CHAIRMAN, 2021)

FireEye , a cybersecurity consulting firm, reported a highly sophisticated cyber breach that used a commercial software programme from SolarWinds on December 13, 2020. Advanced persistent threat (APT) attackers entered SolarWinds' supply chain and inserted a backdoor into the product, according to the findings. Customers who updated their Orion software on a regular basis unwittingly got the imbedded malware. Once inside, the attackers had complete control over which regions they could access and could navigate around systems and carry out their operations without being noticed. (Center for Internet Security, 2021)

Researchers have identified SUNSPOT, SUNBURST, SUPERNOVA, TEARDROP, and RAINDROP as specific members of the malware family that worked together to act as a backdoor into a SolarWinds update framework. (Henneberry, 2021)

Palo Alto Networks and Microsoft discovered SUPERNOVA malware delivered using the App_Web_logoimagehandler.ashx.b6031896.dll file during their investigation into the SolarWinds attack.

This malware contains a backdoor that allows threat actors to transmit C# code to the malware, which is then built and executed as illustrated in Figure 5. (Abrams, 2020)

```
97    // Token: 0x06000005 RID: 5 RVA: 0x00002330 File Offset: 0x00000530
98    public string DynamicRun(string codes, string clazz, string method, string[] args)
99    {
100       ICodeCompiler codeCompiler = new CSharpCodeProvider().CreateCompiler();
101       CompilerParameters compilerParameters = new CompilerParameters();
102       compilerParameters.ReferencedAssemblies.Add("System.dll");
103       compilerParameters.ReferencedAssemblies.Add("System.ServiceModel.dll");
104       compilerParameters.ReferencedAssemblies.Add("System.Data.dll");
105       compilerParameters.ReferencedAssemblies.Add("System.Runtime.dll");
106       compilerParameters.GenerateExecutable = false;
107       compilerParameters.GenerateInMemory = true;
108       CompilerResults compilerResults = codeCompiler.CompileAssemblyFromSource(compilerParameters, codes);
109       if (compilerResults.Errors.HasErrors)
110       {
111           string.Join(Environment.NewLine, Enumerable.Select<CompilerError, string>(Enumerable.Cast<CompilerError>(compilerResults.Errors), (CompilerError
              err) => err.ErrorText));
112           Console.WriteLine("error");
113           return compilerResults.Errors.ToString();
114       }
115       object obj = compilerResults.CompiledAssembly.CreateInstance(clazz);
116       return (string)obj.GetType().GetMethod(method).Invoke(obj, args);
117   }
```

Figure 5: SUPERNOVA compile code

This cyber-attack is extremely sophisticated and is still evolving. Traditional identification techniques such as scanning for known indications of compromise (IOC) are of limited benefit because the attackers randomised parts of their activity. Affected firms had to expect a lengthy and tough recovery process as a result of the attack. (Center for Internet Security, 2021)

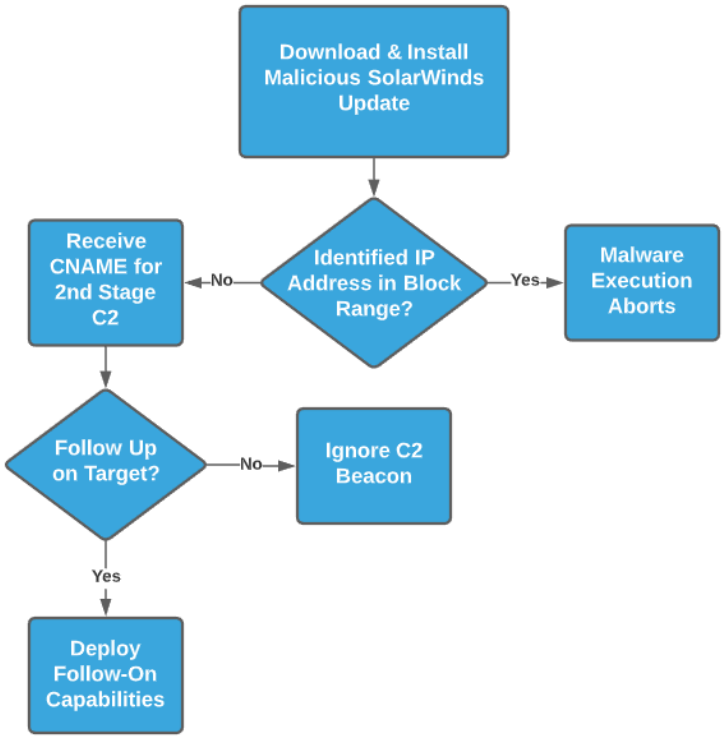


Figure 6: SolarWinds attack Overview

According to a research released by Kim Zetter, threat actors may have practised the distribution approach as early as October 2019. The DLL was delivered without the harmful Sunburst backdoor during this dry run (Figure6).

Researchers suspect that since the threat actors began disseminating the backdoor in March 2020, the attackers have been quietly sitting in some of the infected networks for months, gathering information or engaging in other malicious activity.

According to Zetter's research, FireEye discovered they had been compromised when the threat actors used stolen credentials to register a device with the company's multi-factor authentication (MFA) system. FireEye determined they had been hacked when the system informed the employee and the security team about the unfamiliar device.

The purpose of this study is to examine the SolarWinds malware campaign from several perspectives, particularly the technical one from a CTI standpoint. Because this malware was especially built to attack SolarWinds' supply chain system, it was impossible to completely understand and characterise the behaviour of SolarWind malware without executing and observing it in a real-world environment containing the relevant industrial infrastructure. This is the main limitation of the report.

3. METHODOLOGY

As stated in ENISA Threat Landscape's "Emerging Trends" report (ETL 2020)

"During the next decade, cybersecurity risks will become harder to assess and interpret due to the growing complexity of the threat landscape, adversarial ecosystem and expansion of the attack surface." ENISA Threat Landscape (ENISA, 2020)

Strategic, operational, and tactical stakeholders across the organisation can benefit from a well-designed CTI capability that provides contextualised and actionable threat awareness. To produce intelligence on SolarWinds, the steps of the intelligence cycle indicated in Figure 7 were followed.

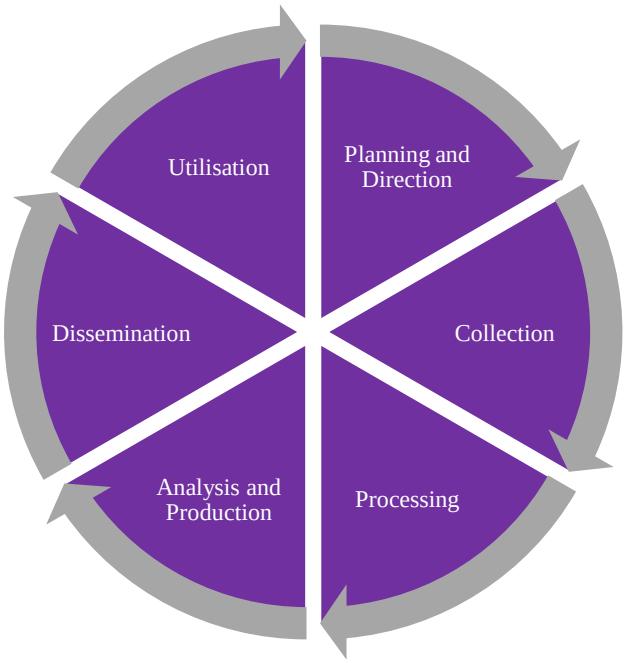


Figure 7: The intelligence Cycle

3.1. PLANNING AND DIRECTION

In practise, a CTI capability should strive to meet the following Information Requirements while taking into account the needs of the stakeholders as well as the context and environment of the organisation.

- Types of the cyber attack
- Indicators of compromise (IOC)
- Exploited vulnerabilities

- Incident initiated date and time.
- The attack vectors
- Techniques, tactics, and procedures (TTPs) used by attackers
- What is the typical behaviour and operation of adversaries?
- Sectors and organisations that are being targeted
- Regions and nations that have been adversely affected
- The attack's effect on the targets
- Threat Actors (TA)
- Intention and capabilities of TAs.
- What needs to be done to mitigate risks posed by these threats?

Different external open-source cyber threat intelligence sources were utilised in this SolarWinds scenario, including AlienVault - Open Threat Exchange, Microsoft Security Intelligence, and other related research publications. Scanning data, tool reports, malware analysis, and logging events were used as internal sources.

3.2. COLLECTION

Different IOCs were obtained from the above-mentioned sources, including IP addresses of Command and Control (CnC) servers, domain names, URLs, Hash values of SolarWind's variants, File system artefacts, and other important data. I moved on to the processing stage after fulfilling the collection requirements in order to organise the acquired data in a useful way. To prevent redundancy, this acquired data is shown in a processed form in the following section of the report relevant to the intelligence cycle's processing step.

3.3. PROCESSING

Researchers have got a better understanding of different malware used in this attack, after investigating SolarWinds supply chain victims. According to CrowdStrike, the SunSpot malware was first installed in the SolarWinds network to monitor for and automatically inject the Sunburst backdoor in development builds. Victims would then receive the Sunburst backdoor via automatic upgrades for the SolarWinds Orion platform. It would connect to a remote command and control server for orders to be executed on the infected device once it was executed. The Sunburst backdoor would release Teardrop malware, which is a previously undisclosed memory-only dropper and a post-exploitation tool used to deploy modified Cobalt

Strike beacons, according to FireEye. Finally, Symantec identified the RainDrop malware, which was also used to install Cobalt Strike beacons on other machines in a network that had previously been hacked. (Abrams, 2020)

MALWARE VARIANTS

Variant	Capabilities
Sunburst	It was the backdoor injected into a SolarWinds update that sat idle for up to two weeks before connecting to its command and control (C2) servers through HTTP to avsvmcloud[.]com subdomain.
Sunspot	Used by the threat actor to implant the SUNBURST backdoor code into the software update pipeline.
Teardrop	A memory-only dropper, also known as downloader malware, whose primary purpose is to download and install further malware components invisibly.
Supernova	A web shell that appears to be designed to keep persistent access to the system
Raindrop	Lowered the number of hosts needed to beacon out, allowing the threat actor to remain undetected

Table 1: Malware variants

MD5 HASH VALUES OF MALWARE

Md5	Filename	Version
02af7cec58b9a5da1c542b5a32151ba1	CORE-2019.4.5220.20574-SolarWinds-Core-v2019.4.5220-Hotfix5.msp	Not available
08e35543d6110ed11fdf558bb093d401	Solarwinds Worldwide, LLC	Not available
b91ce2fa41029f6955bff20079468448	SolarWinds.Orion.Core.BusinessLayer.dll	2019.4.5200.9083
d5aad0d248c237360cf39c054b654d69	SolarWinds.Orion.Core.BusinessLayer.dll	2020.2.100.12299
2c4a910a1299cdae2a4e55988a2f102e	SolarWinds.Orion.Core.BusinessLayer.dll	2020.2.5200.12394
846e27a652a5e1bfbd0ddd38a16dc865	SolarWinds.Orion.Core.BusinessLayer.dll	2020.2.5300.12432
baa3d3488db90289eb2889c1a2acbcde	Solarwinds Worldwide, LLC	Not available
e18a6a21eb44e77ca8d739a72209c370	SolarWinds.Orion.Core.BusinessLayer.dll	2019.4.5200.8890
3e329a4c9030b26ba152fb602a1d5893	SolarWinds.Orion.Core.BusinessLayer.dll	2019.4.5200.8890
4f2eb62fa529c0283b28d05ddd311fae	OrionImprovementBusinessLayer.2.cs	Not available
56ceb6d0011d87b6e4d7023d7ef85676	app_web_logoimagehandler.ashx.b6031896.dll	Not available

Table 2: MD5 hashes, filename and versions of malicious SolarWinds.Orion.Core.BusinessLayer.dll files spotted in the wild (Mandiant, 2020)

Domains	avsvmcloud[.]com - Killswitch domain/currently unblocked	SUNBURST
	zupertech[.]com	SUNBURST
	panhardware[.]com	SUNBURST
	databasegalore[.]com	SUNBURST
	incomeupdate[.]com	SUNBURST
	highdatabase[.]com	SUNBURST
	websitetheme[.]com	SUNBURST
	freescanonline[.]com	SUNBURST
	virtualdataserver[.]com	SUNBURST
	deftsecurity[.]com	SUNBURST
	thedoccloud[.]com	SUNBURST
	digitalcollege[.]org	SUNBURST
	globalnetworkissues[.]com	SUNBURST
	seobundlekit[.]com	SUNBURST
	virtualwebdata[.]com	SUNBURST
	kubecloud[.]com	BEACON
	lcomputers[.]com	BEACON
	solartrackingsystem[.]net	BEACON
	webcodez[.]com	BEACON
	ervsystem[.]com	TEARDROP
	infinitysoftwares[.]com	TEARDROP
IP Addresses	13.59.205[.]66	SUNBURST
	54.193.127[.]66	SUNBURST
	3.87.182[.]149	BEACON
	3.16.81[.]254	SUNBURST
	54.215.192[.]52	SUNBURST
	18.253.52[.]187	SUNBURST
	34.203.203[.]23	SUNBURST
	54.215.192[.]52	SUNBURST
	18.220.219[.]143	SUNBURST
	139.99.115[.]204	SUNBURST
	13.57.184[.]217	SUNBURST
	34.219.234[.]134	BEACON
	5.252.177[.]25	SUNBURST
	5.252.177[.]21	SUNBURST
	204.188.205[.]176	SUNBURST
	51.89.125[.]18	SUNBURST
	162.223.31[.]184	BEACON
	173.237.190[.]2	BEACON
	45.141.152[.]18	BEACON
Hashes (SHA256)	019085a76ba7126fff22770d71bd901c325fc68ac55aa743327984e89f4b0134	SUNBURST
	32519b85c0b422e4656de6e6c41878e95fd95026267daab4215ee59c107d6c77	SUNBURST

	ac1b2b89e60707a20e9eb1ca480bc3410ead40643b386d624c5d21b47c02917c	SUNBURST
	c09040d35630d75dfef0f804f320f8b3d16a481071076918e9b236a321c1ea77	SUNBURST
	c15abaf51e78ca56c0376522d699c978217bf041a3bd3c71d09193efa5717c71	SUPERNOVA
	ce77d116a074dab7a22a0fd4f2c1ab475f16eec42e1ded3c0b0aa8211fe858d6	SUNBURST
	d0d626deb3f9484e649294a8dfa814c5568f846d5aa02d4cdad5d041a29d5600	SUNBURST
	dab758bf98d9b36fa057a66cd0284737abf89857b73ca89280267ee7caf62f3b	SUNBURST
	1817a5bf9c01035bcf8a975c9f1d94b0ce7f6a200339485d8f93859f8f6d730c	TEARDROP
	b820e8a2057112d0ed73bd7995201dbed79a79e13c79d4bdad81a22f12387e07	TEARDROP
	0f5d7e6dfdd62c83eb096ba193b5ae394001bac036745495674156ead6557589	SUNBURST
	db9e63337dacf0c0f1baa06145fd5f1007002c63124f99180f520ac11d551420	SUNBURST
	118189f90da3788362fe85eafa555298423e21ec37f147f3bf88c61d4cd46c51	TEARDROP
	eb6fab5a2964c5817fb239a7a5079cabca0a00464fb3e07155f28b0a57a2c0ed	SUNBURST
	abe22cf0d78836c3ea072daeaf4c5eeaf9c29b6feb597741651979fc8fbd2417	SUNBURST
	20e35055113dac104d2bb02d4e7e33413fae0e5a426e0eea0dfd2c1dce692fd9	SUNBURST
	2ade1ac8911ad6a23498230a5e119516db47f6e76687f804e2512cc9bcfda2b0	SUNBURST
	6e4050c6a2d2e5e49606d96dd2922da480f2e0c70082cc7e54449a7dc0d20f8d	TEARDROP

Table 3: List of indicators of compromise (BIASINI, 2020)

FILE SYSTEM ARTIFACTS (IOCS)

- **HX file_operation_closed**
  actor-process: SolarWinds.BusinessLayerHost.exe
  file-path: C:\Windows\SysWOW64\NetSetupSvc.dll

- **Windows Defender Exploit Guard log entries**
  Process '...\svchost.exe' (PID ...) would have been blocked from loading the non-Microsoft-signed binary '\Windows\SysWOW64\NetSetupSvc.dll'.

PAYLOAD

A BEACON backdoor is unpacked in memory by layers of loaders.

1. **App_Web_logoimagehandler.ashx.b6031896.dll**

THREAT ACTORS

UNC2452 is the threat actor behind this effort, according to FireEye, but Volexity, a Washington-based cybersecurity firm, has linked this activity to a hacking gang known as Dark Halo.

According to unconfirmed media allegations, the attacks were linked to APT29 (aka Cozy Bear), a state-sponsored hacking team linked to Russia's Foreign Intelligence Service (SVR). (FIREEYE, 2020)

INTENTION OF TAS

Industrial Sabotage

CAPABILITIES OF TAS

The most sophisticated and stealthy attackers in the world.

TARGETED SECTORS AND ORGANISATIONS

According to FireEye, victims include government organisations and consultancy firms, as well as technology, telecom, and oil and gas companies. (BIASINI, 2020)

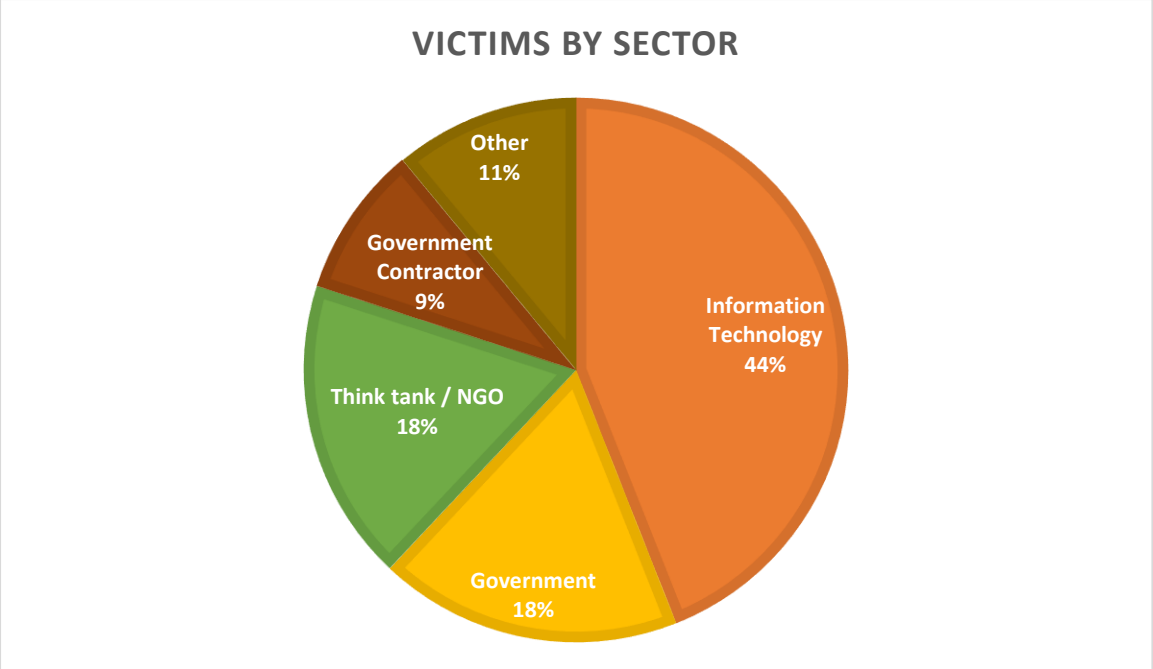


Figure 8: Victims by sector

The following companies have been identified as being affected by the SolarWinds supply chain attack: (Abrams, 2020)

- FireEye
- U.S. Department of the Treasury
- U.S. National Telecommunications and Information Administration (NTIA)
- U.S. Department of State
- The National Institutes of Health (NIH) (Part of the U.S. Department of Health)
- U.S. Department of Homeland Security (DHS)
- U.S. Department of Energy (DOE)
- U.S. National Nuclear Security Administration (NNSA)
- Some US states (Specific states are undisclosed)
- Microsoft
- Cisco

AFFECTED REGIONS:

North America, Europe, Asia, and the Middle East.

AFFECTED COUNTRIES:

United States of America, German, Mexico, Israel, Canada, Spain, Belgium, the United Arab Emirates, and the United Kingdom

IMPACT OF ATTACK:

SolarWinds reported that, about 18,000 of its 300,000 customers downloaded the tainted update. Nonetheless, with the company's products being employed by a number of high-value companies, the campaign's impact might be enormous. (BIASINI, 2020)

ATTACK VECTOR:

The main vector of attack was a vulnerability implanted inside the SolarWinds Orion platform. The following versions are highly vulnerable:

SolarWinds Orion Platform Version 2019.4 HF 5

SolarWinds Orion Platform Version 2020.2

SolarWinds Orion Platform Version 2020.2 HF 1

For CVE-2020-10148, SolarWinds Orion Platform versions 2019.2 HF 3, 2018.4 HF 3, and 2018.2 HF 6 are also affected.

TTPs:

The following are some of the evasion techniques used by attackers:

1. There was no reason to dispute the Sunburst certificate because it was correctly signed and the domain had been registered a year previously.
2. When the cyber crooks injected the DLL, they disabled logging and then enabled it again. There was no clear sign of the DLL being injected unless someone was specifically hunting for an intrusion of this level.
3. The DLL checked to see if it had been altered.
4. It was also assured that it was not performed by security tools at SolarWinds in a Sandbox. This is crucial because any security analysts who examine this DLL will do so in a Sandbox.

As a result, the DLL was able to evade execution in a sandbox. That was the level of sophistication of the attack. At every stage, it was able to elude discovery.

5. The DLL could also run at random times for up to two weeks after being restarted.
6. It possessed a complete process list, allowing it to look for and terminate endpoint security programmes and installed drivers, eluding all EDR capabilities. (Cyber Management Alliance, 2021)

There are three major aspects to these tactics, techniques, and procedures (TTPs):

1. Compromise or circumvent federated identity solutions; Compromise or circumvent federated identity solutions; Compromise or circumvent federated identity solutions;
2. Use forged authentication tokens to move laterally to Microsoft cloud environments; and
3. Use privileged access to a victim's cloud environment to set up difficult-to-detect persistence mechanisms for API-based access. (Cybersecurity and Infrastructure Security Agency, 2021)

3.4. ANALYSIS AND PRODUCTION

The malicious DLL uses the domains avsvmcloud.com to communicate with a remote network infrastructure in order to build possible second-stage payloads, move laterally within the organisation, and compromise or exfiltrate data.

Date first seen	Malware Variant Detected
Sep 2019	APT accessed SolarWinds; injects Sunspot malware
Feb 2020	Sunburst compiled and deployed for March update
Jun 2020	APT removes build VMs malware to avoid detection
Dec 2020	FireEye detects Sunburst; detection and patch solutions deployed
Jan 2021	Detection of Teardrop, Sunspot, and Raindrop; SolarWinds not alone
Feb 2021	Detection of 2nd APT and additional Orion vulnerabilities published

Table 4: SolarWinds Variants

Malware Family	Version	File System Artifact	MD5	SHA256
SUNBURST	2019.4.5200.9083	SolarWinds.Orion.Core.BusinessLayer.dll	b91ce2fa41029f6955bff20079468448	32519b85c0b422e4656de6e6c41878e95fd95026267daab4215ee59c107d6c77
SUNBURST	2020.2.100.12299	SolarWinds.Orion.Core.BusinessLayer.dll	d5aad0d248c237360cf39c054b654d69	abe22cf0d78836c3ea072daeaf4c5eeaf9c29b6feb597741651979fc8fbd2417
SUNBURST	2020.2.5200.12394	SolarWinds.Orion.Core.BusinessLayer.dll	2c4a910a1299cdae2a4e55988a2f102e	019085a76ba7126fff22770d71bd901c325fc68ac55aa743327984e89f4b0134

SUNBURST	2020.2.5300.12432	SolarWinds.Orion.Core.BusinessLayer.dll	846e27a652a5e1bfbd0ddd38a16dc865	ce77d116a074dab7a22a0fd4f2c1ab475f16eec42e1ded3c0b0aa8211fe858d6
SUPERNOVA	Not Available	app_web_logoimagehandler.ashx.b6031896.dll	56ceb6d0011d87b6e4d7023d7ef85676	c15abaf51e78ca56c0376522d699c978217bf041a3bd3c71d09193efa5717c71

Table 5: SolarWinds' indicator release hashes

SolarWinds.Orion.Core.BusinessLayer.dll (b91ce2fa41029f6955bff20079468448) is a SolarWinds-signed Orion software framework plugin component that contains an obfuscated backdoor that communicates with third-party servers via HTTP. It receives and executes commands known as "Jobs" after a dormant time of up to two weeks, including the ability to transfer and execute files, profile the system, and stop system services. (The Hacker News, 2021) By imitating the Orion Improvement Program (OIP) protocol and storing reconnaissance results within plugin configuration files, the backdoor's behaviour and network protocol blend in with legal SolarWinds activities. Multiple blocklists are used by the backdoor to find forensic and anti-virus tools via processes, services, and drivers. (FIREEYE, 2020)

Name	Type
APT_Backdoor_MSIL_SUNBURST_1	yara
APT_Backdoor_MSIL_SUNBURST_2	yara
APT_Backdoor_MSIL_SUNBURST_3	yara
APT_Backdoor_MSIL_SUNBURST_4	yara
APT_Webshell_MSIL_SUPERNOVA_2	yara
APT_Webshell_MSIL_SUPERNOVA_1	yara
APT_Dropper_Raw64_TEARDROP_1	yara
APT_Dropper_Win64_TEARDROP_2	yara

Table 6: Signature table of content (Mandiant, 2020)

STATIC ANALYSIS

Out of the static analysis techniques, multiple anti-virus scanning technique was used to identify concealed malware files.

The IOCs relating to the stealthy post-intrusion activities detected have been meticulously documented by FireEye and CISA. We can't presume that all victims' post-intrusion forensics will be identical. Indeed, threat actors are more likely to deploy highly personalised, human-operated campaigns to steal precise data from each victim.

Attacks like these create a strong case for using a Zero-trust model and behavior-based detections in supply chains. The attackers were successful in making their malicious

SolarWinds Orion DLL appear to be a legitimate version of the software. As everything appeared to be official, it was nearly impossible to detect. However, as the actors move across a network, accessing new accounts and handling data, and they don't know how to precisely duplicate the typical behaviour of all the users and devices they're running, which creates a significant window of opportunity for discovery.

The IOC data from FireEye's GitHub repository was used for this investigation. (Mandiant, 2020) Using YARA principles as shown in Table 6 is a technique that was used to discover unusual items that are lying about.

Several of these are likely to contain the string "Select * From Win32 SystemDriver." As a result, the attackers used a mix of compression and Base64 encoding to disguise all of the noisy strings. Because there are several hunting criteria that check for Base64 variations of the aforementioned string, a two-step method was required.

DYNAMIC ANALYSIS

Many of security analysts have done fantastic research into the SUNBURST trojan, and the goal here isn't to repeat what they've found, but to add insight we haven't seen before. The goal is to provide potential victims a better understanding of the campaign's capabilities so they can assess the likelihood of further persistence methods. (Maccaglia, 2020)

For the purposes of this investigation, they focused on the file "SolarWinds.Orion.Core.BusinessLayer.dll," which is related with the SolarWinds ORION software package and has been modified to include a class carrying the backdoor "SunBurst."

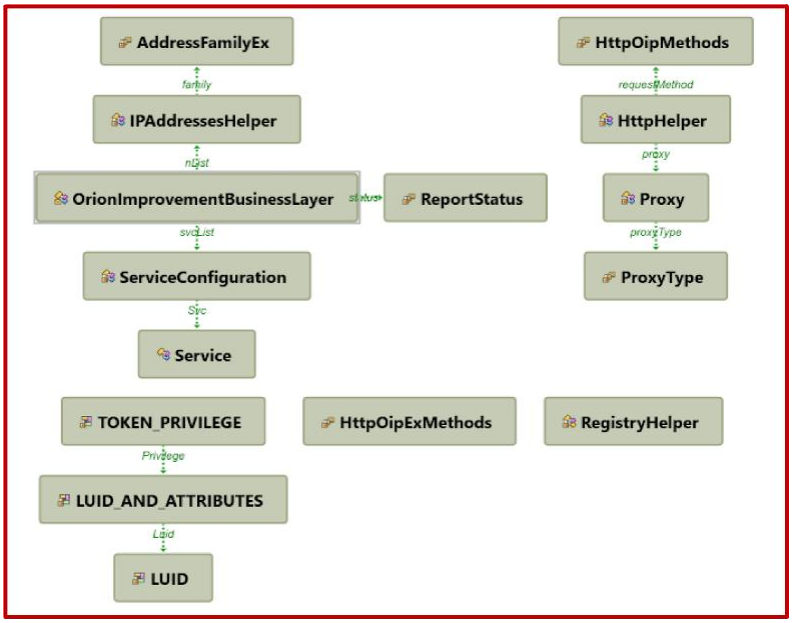


Figure 9: Added module and dependencies

The class begins by checking to see if the module is operating, and if it isn't, it will start the service and then enter a dormancy period.

```
private static void DelayMin(int minMinutes, int maxMinutes)
{
    if (maxMinutes == 0)
    {
        minMinutes = 30;
        maxMinutes = 120;
    }
    OrionImprovementBusinessLayer.DelayMs((double)minMinutes * 60 * 1000, (double)maxMinutes * 60 * 1000);
}

private static void DelayMs(double minMs, double maxMs)
{
    double i;
    if ((int)maxMs == 0)
    {
        minMs = 1000;
        maxMs = 2000;
    }
    for (i = minMs + (new Random()).NextDouble() * (maxMs - minMs); i >= 2147483647; i -= 2147483647)
    {
        Thread.Sleep(2147483647);
    }
    Thread.Sleep((int)i);
}
```

Figure 10: Sleep sequence of backdoor

According to FireEye, this phase of sleep might last anywhere from minutes to two weeks. The length of dormancy is determined by the checks that must be passed from the code, such as the hash of the Orion process, file write-times, process running, and so on. A slumber period of this duration is exceptional, and it indicates a patient foe.

The most critical strings inside the backdoors are encoded using the.NET Compression library's DeflateStream Class and the base64 encoder. They discover results that require additional

investigation by scanning the block-list. The local-IP address ranges and netmasks are the first entries:

- 10.0.0.0 255.0.0.0
- 172.16.0.0 255.240.0.0
- 192.168.0.0 255.255.0.0

The IPv6 local address equivalents follow:

fc00::,fe00::, fec0::,ffc0::,ff00::,ff00::

They ran a whois on those IP addresses to determine who they might be associated with. Although the netmasks used in certain entries are 'very' particular, there is no indication as to why the following IPs were included into the blocklist.

MEMORY ANALYSIS

For SolarWinds memory image analysis, I utilised Volatility Framework 2.6.1 deployed in a Kali Linux VM. I found the SolarWinds memory image online and downloaded it.

The state of a machine's memory is constantly changing when it is online. This means that IoCs in the computer's memory may be erased by malware or replaced spontaneously. A memory dump is a snapshot of the computer's memory that can be used to look for suspicious artefacts.

Malware, and any executable, is made up of a combination of software code and data. In certain circumstances, the data in these applications is in the form of human-readable strings. These strings can be exclusive to a malware type, giving them an effective and easy-to-find IoC.

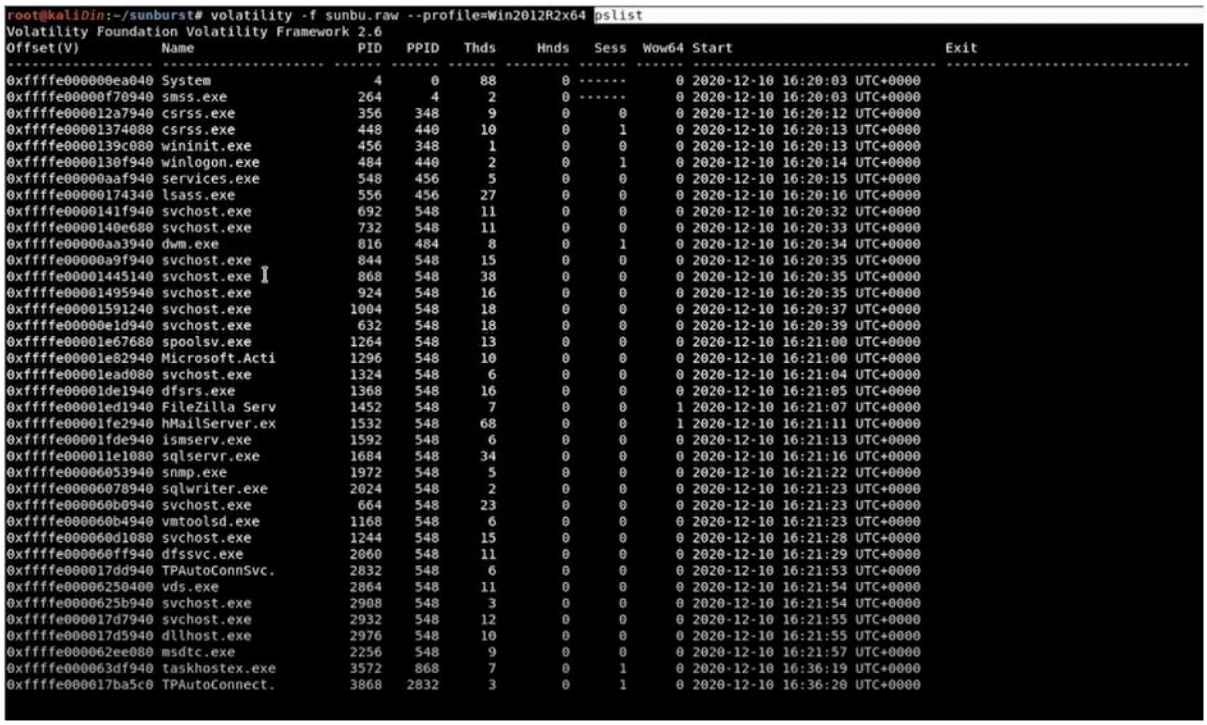
A built-in programme in Linux called strings extracts all printable strings from a file. Because it looks for anything printable in the computer's memory, running this against the memory dump file from the previous step will almost certainly produce a big list of results.

To make these results more manageable, use grep to search the list for certain strings. Sunburst malware was used in the SolarWinds intrusion, and FireEye has published a list of Snort rules that can be used to detect it.

These rules can also be applied to string results to filter them. For example, using the command strings | grep deft to search for the word deft will return results for the domain deftsecurity.com from FireEyes' list. If the list of detection rules provided by FireEyes returns any results, the system in question may have been infected with the Sunburst malware.

To go beyond looking at printable strings in the memory dump, you'll need forensic memory analysis software. Volatility, an open-source tool, is one of the best available tools for this.

It's feasible to run numerous distinct terminal commands against a memory sample with Volatility. Examining the processes running on the infected machine is an excellent place to start looking for malware IoCs. The command volatility -f –profile= pslist can be used to accomplish this.



```
root@kaliDin:~/sunburst# volatility -f sunbu.raw --profile=Win2012R2x64 pslist
Volatility Foundation Volatility Framework 2.6
Offset(V)          Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
------------------ -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0xffffe000000ea040 System                    4      0     88        0 ------      0 2020-12-10 16:20:03 UTC+0000
0xffffe00000f70940 smss.exe                264      4      2        0 ------      0 2020-12-10 16:20:03 UTC+0000
0xffffe000012a7940 csrss.exe               356    348      9        0      0      0 2020-12-10 16:20:12 UTC+0000
0xffffe00001374080 csrss.exe               448    440     10        0      1      0 2020-12-10 16:20:13 UTC+0000
0xffffe0000139c080 wininit.exe             456    348      1        0      0      0 2020-12-10 16:20:13 UTC+0000
0xffffe0000130f940 winlogon.exe            484    440      2        0      1      0 2020-12-10 16:20:14 UTC+0000
0xffffe00000aaf940 services.exe            548    456      5        0      0      0 2020-12-10 16:20:15 UTC+0000
0xffffe00000174340 lsass.exe               556    456     27        0      0      0 2020-12-10 16:20:16 UTC+0000
0xffffe0000141f940 svchost.exe             692    548     11        0      0      0 2020-12-10 16:20:32 UTC+0000
0xffffe0000140e680 svchost.exe             732    548     11        0      0      0 2020-12-10 16:20:33 UTC+0000
0xffffe00000aa3940 dwm.exe                 816    484      8        0      1      0 2020-12-10 16:20:34 UTC+0000
0xffffe00000a9f940 svchost.exe             844    548     15        0      0      0 2020-12-10 16:20:35 UTC+0000
0xffffe00001445140 svchost.exe             868    548     38        0      0      0 2020-12-10 16:20:35 UTC+0000
0xffffe00001495940 svchost.exe             924    548     16        0      0      0 2020-12-10 16:20:35 UTC+0000
0xffffe00001591240 svchost.exe            1004    548     18        0      0      0 2020-12-10 16:20:37 UTC+0000
0xffffe00000e1d940 svchost.exe             632    548     18        0      0      0 2020-12-10 16:20:39 UTC+0000
0xffffe00001e67680 spoolsv.exe            1264    548     13        0      0      0 2020-12-10 16:21:00 UTC+0000
0xffffe00001e82940 Microsoft.Acti         1296    548     10        0      0      0 2020-12-10 16:21:00 UTC+0000
0xffffe00001ead080 svchost.exe            1324    548      6        0      0      0 2020-12-10 16:21:04 UTC+0000
0xffffe00001de1940 dfsrs.exe              1368    548     16        0      0      0 2020-12-10 16:21:05 UTC+0000
0xffffe00001ed1940 FileZilla Serv         1452    548      7        0      0      1 2020-12-10 16:21:07 UTC+0000
0xffffe00001fe2940 hMailServer.ex         1532    548     68        0      0      1 2020-12-10 16:21:11 UTC+0000
0xffffe00001fde940 ismserv.exe            1592    548      6        0      0      0 2020-12-10 16:21:13 UTC+0000
0xffffe000011e1080 sqlservr.exe           1684    548     34        0      0      0 2020-12-10 16:21:16 UTC+0000
0xffffe00006053940 snmp.exe               1972    548      5        0      0      0 2020-12-10 16:21:22 UTC+0000
0xffffe00006078940 sqlwriter.exe          2024    548      2        0      0      0 2020-12-10 16:21:23 UTC+0000
0xffffe000060b0940 svchost.exe             664    548     23        0      0      0 2020-12-10 16:21:23 UTC+0000
0xffffe000060b4940 vmtoolsd.exe           1168    548      6        0      0      0 2020-12-10 16:21:23 UTC+0000
0xffffe000060d1080 svchost.exe            1244    548     15        0      0      0 2020-12-10 16:21:28 UTC+0000
0xffffe000060ff940 dfssvc.exe             2060    548     11        0      0      0 2020-12-10 16:21:29 UTC+0000
0xffffe000017dd940 TPAutoConnSvc.         2832    548      6        0      0      0 2020-12-10 16:21:53 UTC+0000
0xffffe00006250400 vds.exe                2864    548     11        0      0      0 2020-12-10 16:21:54 UTC+0000
0xffffe0000625b940 svchost.exe            2908    548      3        0      0      0 2020-12-10 16:21:54 UTC+0000
0xffffe000017d7940 svchost.exe            2932    548     12        0      0      0 2020-12-10 16:21:55 UTC+0000
0xffffe000017d5940 dllhost.exe            2976    548     10        0      0      0 2020-12-10 16:21:55 UTC+0000
0xffffe000062ee080 msdtc.exe              2256    548      9        0      0      0 2020-12-10 16:21:57 UTC+0000
0xffffe000063df940 taskhostex.exe         3572    868      7        0      1      0 2020-12-10 16:36:19 UTC+0000
0xffffe000017ba5c0 TPAutoConnect.         3868   2832      3        0      1      0 2020-12-10 16:36:20 UTC+0000
```

Figure 11: pslist command

This produces the same results as executing pslist on a live Windows computer. It may be possible to spot unusual processes that indicate a malware infestation by looking through the list.

It's time to delve deeper after spotting an unusual process. The following are a few alternatives for the next steps:

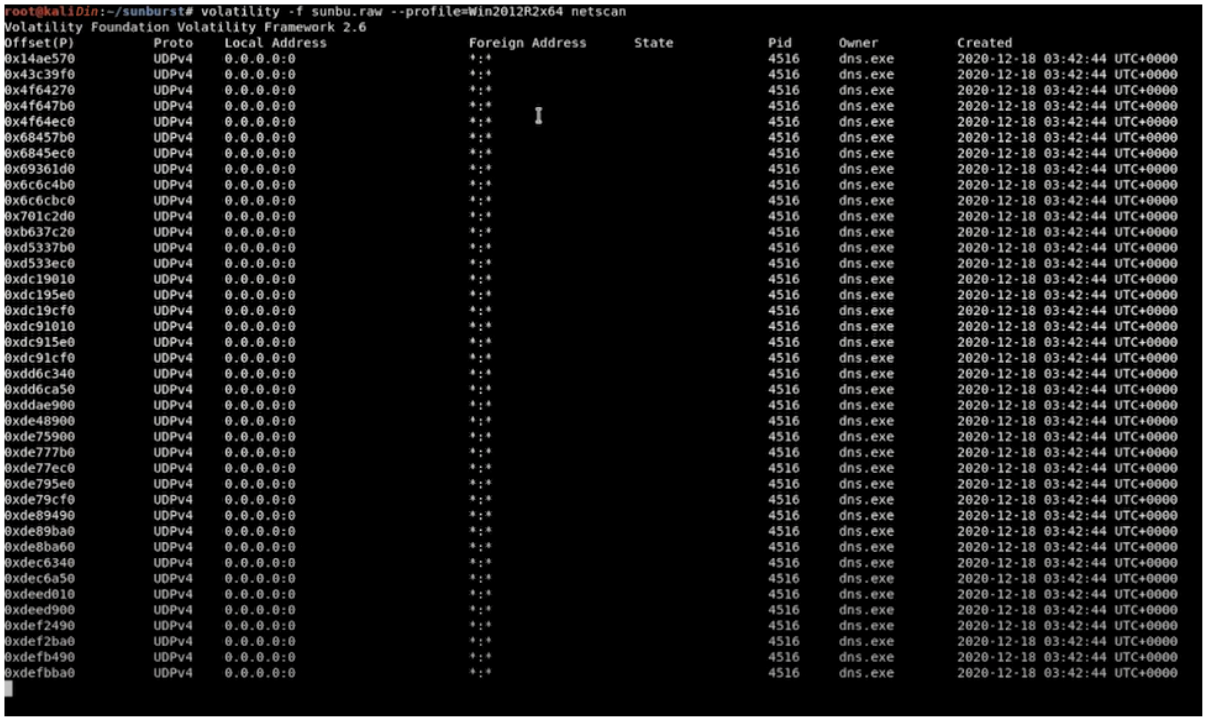
1. Looking for child processes: In Volatility, the pstree command can be used to determine which processes are the parent and children of a given process. This can assist in identifying the infection vector as well as the infection's effects.
2. Dumping processes: the procdump command can dump a process from Volatility using a process id (pid) from pslist or pstree. This results in a fully functional binary that can be run in a sandbox or disassembled for reverse engineering.

```
root@kaliDin:~/sunburst# volatility -f sunbu.raw --profile=Win2012R2x64 pstree
Volatility Foundation Volatility Framework 2.6
Name                                                 Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0xffffe0000139c080:wininit.exe                       456    348      1      0 2020-12-10 16:20:13 UTC+0000
. 0xffffe00000aaf940:services.exe                     548    456      5      0 2020-12-10 16:20:15 UTC+0000
.. 0xffffe00001ead080:svchost.exe                    1324    548      6      0 2020-12-10 16:21:04 UTC+0000
.. 0xffffe000060ff940:dfssvc.exe                     2060    548     11      0 2020-12-10 16:21:29 UTC+0000
.. 0xffffe00001e82940:Microsoft.Acti                 1296    548     10      0 2020-12-10 16:21:00 UTC+0000
.. 0xffffe00001le1080:sqlservr.exe                   1684    548     34      0 2020-12-10 16:21:16 UTC+0000
... 0xffffe00006581700:cmd.exe                       3244   1684      0 ------ 2020-12-11 16:36:42 UTC+0000
.... 0xffffe00008a91180:kai.exe                      3812   3244      0 ------ 2020-12-11 16:36:42 UTC+0000
..... 0xffffe00008a957c0:cmd.exe                     3680   3812      1      0 2020-12-11 16:38:45 UTC+0000
...... 0xffffe00008a05940:conhost.exe                3768   3680      2      0 2020-12-11 16:38:45 UTC+0000
.. 0xffffe00006700080:sppsvc.exe                     5388    548      0 ------ 2020-12-18 06:11:33 UTC+0000
.. 0xffffe000060b0940:svchost.exe                     664    548     23      0 2020-12-10 16:21:23 UTC+0000
.. 0xffffe00001328200:svchost.exe                    2692    548      1      0 2020-12-10 16:36:26 UTC+0000
.. 0xffffe00001495940:svchost.exe                     924    548     16      0 2020-12-10 16:20:35 UTC+0000
.. 0xffffe000017d5940:dllhost.exe                    2976    548     10      0 2020-12-10 16:21:55 UTC+0000
.. 0xffffe00006250400:vds.exe                        2864    548     11      0 2020-12-10 16:21:54 UTC+0000
.. 0xffffe0000625b940:svchost.exe                    2908    548      3      0 2020-12-10 16:21:54 UTC+0000
.. 0xffffe000060d1080:svchost.exe                    1244    548     15      0 2020-12-10 16:21:28 UTC+0000
... 0xffffe000064c1440:w3wp.exe                      3696   1244      0 ------ 2020-12-11 16:20:29 UTC+0000
.. 0xffffe0000141f940:svchost.exe                     692    548     11      0 2020-12-10 16:20:32 UTC+0000
... 0xffffe00008cf6940:WmiPrvSE.exe                  5360    692      8      0 2020-12-18 06:11:33 UTC+0000
.. 0xffffe00001fde940:ismserv.exe                    1592    548      6      0 2020-12-10 16:21:13 UTC+0000
.. 0xffffe00006053940:snmp.exe                       1972    548      5      0 2020-12-10 16:21:22 UTC+0000
.. 0xffffe000017dd940:TPAutoConnSvc.                 2832    548      6      0 2020-12-10 16:21:53 UTC+0000
... 0xffffe000017ba5c0:TPAutoConnect.                3868   2832      3      0 2020-12-10 16:36:20 UTC+0000
.... 0xffffe00002dd94c0:conhost.exe                  3880   3868      1      0 2020-12-10 16:36:20 UTC+0000
.. 0xffffe00001ddf940:dns.exe                        4516    548     14      0 2020-12-18 03:42:44 UTC+0000
.. 0xffffe00000a9f940:svchost.exe                     844    548     15      0 2020-12-10 16:20:35 UTC+0000
.. 0xffffe000062ee080:msdtc.exe                      2256    548      9      0 2020-12-10 16:21:57 UTC+0000
.. 0xffffe00001de1940:dfsrs.exe                      1368    548     16      0 2020-12-10 16:21:05 UTC+0000
.. 0xffffe00001445140:svchost.exe                     868    548     38      0 2020-12-10 16:20:35 UTC+0000
... 0xffffe000063df940:taskhostex.exe                3572    868      7      0 2020-12-10 16:36:19 UTC+0000
... 0xffffe00002021940:wuauclt.exe                   2272    868      1      0 2020-12-10 16:39:21 UTC+0000
.. 0xffffe00001ed1940:FileZilla Serv                 1452    548      7      0 2020-12-10 16:21:07 UTC+0000
.. 0xffffe0000140e680:svchost.exe                     732    548     11      0 2020-12-10 16:20:33 UTC+0000
.. 0xffffe000060b4940:vmtoolsd.exe                   1168    548      6      0 2020-12-10 16:21:23 UTC+0000
.. 0xffffe00006078940:sqlwriter.exe                  2024    548      2      0 2020-12-10 16:21:23 UTC+0000
.. 0xffffe00001591240:svchost.exe                    1004    548     18      0 2020-12-10 16:20:37 UTC+0000
.. 0xffffe00001e67680:spoolsv.exe                    1264    548     13      0 2020-12-10 16:21:00 UTC+0000
.. 0xffffe000017d7940:svchost.exe                    2932    548     12      0 2020-12-10 16:21:55 UTC+0000
.. 0xffffe00000e1d940:svchost.exe                     632    548     18      0 2020-12-10 16:20:39 UTC+0000
```

Figure 12: pstree command

In addition to looking at processes, looking at the connections that an infected computer has open can be beneficial. A memory dump snapshot also includes the current connection state of a system. (Black Hat, 2020)

Similar to executing netstat on a live system, the netscan command in Volatility generates a list of network connections. Any unusual connections may result in the detection of malware infections on the computer.



```
root@kaliDin:~/sunburst# volatility -f sunbu.raw --profile=Win2012R2x64 netscan
Volatility Foundation Volatility Framework 2.6
Offset(P)          Proto    Local Address                  Foreign Address      State          Pid      Owner          Created
0x14ae570          UDPv4    0.0.0.0:0                      *:*                                 4516     dns.exe        2020-12-18 03:42:44 UTC+0000
0x43c39f0          UDPv4    0.0.0.0:0                      *:*                                 4516     dns.exe        2020-12-18 03:42:44 UTC+0000
0x4f64270          UDPv4    0.0.0.0:0                      *:*                                 4516     dns.exe        2020-12-18 03:42:44 UTC+0000
0x4f647b0          UDPv4    0.0.0.0:0                      *:*                                 4516     dns.exe        2020-12-18 03:42:44 UTC+0000
0x4f64ec0          UDPv4    0.0.0.0:0                      *:*                                 4516     dns.exe        2020-12-18 03:42:44 UTC+0000
0x68457b0          UDPv4    0.0.0.0:0                      *:*                                 4516     dns.exe        2020-12-18 03:42:44 UTC+0000
0x6845ec0          UDPv4    0.0.0.0:0                      *:*                                 4516     dns.exe        2020-12-18 03:42:44 UTC+0000
0x69361d0          UDPv4    0.0.0.0:0                      *:*                                 4516     dns.exe        2020-12-18 03:42:44 UTC+0000
0x6c6c4b0          UDPv4    0.0.0.0:0                      *:*                                 4516     dns.exe        2020-12-18 03:42:44 UTC+0000
0x6c6cbc0          UDPv4    0.0.0.0:0                      *:*                                 4516     dns.exe        2020-12-18 03:42:44 UTC+0000
0x701c2d0          UDPv4    0.0.0.0:0                      *:*                                 4516     dns.exe        2020-12-18 03:42:44 UTC+0000
0xb637c20          UDPv4    0.0.0.0:0                      *:*                                 4516     dns.exe        2020-12-18 03:42:44 UTC+0000
0xd5337b0          UDPv4    0.0.0.0:0                      *:*                                 4516     dns.exe        2020-12-18 03:42:44 UTC+0000
0xd533ec0          UDPv4    0.0.0.0:0                      *:*                                 4516     dns.exe        2020-12-18 03:42:44 UTC+0000
0xdc19010          UDPv4    0.0.0.0:0                      *:*                                 4516     dns.exe        2020-12-18 03:42:44 UTC+0000
0xdc195e0          UDPv4    0.0.0.0:0                      *:*                                 4516     dns.exe        2020-12-18 03:42:44 UTC+0000
0xdc19cf0          UDPv4    0.0.0.0:0                      *:*                                 4516     dns.exe        2020-12-18 03:42:44 UTC+0000
0xdc91010          UDPv4    0.0.0.0:0                      *:*                                 4516     dns.exe        2020-12-18 03:42:44 UTC+0000
0xdc915e0          UDPv4    0.0.0.0:0                      *:*                                 4516     dns.exe        2020-12-18 03:42:44 UTC+0000
0xdc91cf0          UDPv4    0.0.0.0:0                      *:*                                 4516     dns.exe        2020-12-18 03:42:44 UTC+0000
0xdd6c340          UDPv4    0.0.0.0:0                      *:*                                 4516     dns.exe        2020-12-18 03:42:44 UTC+0000
0xdd6ca50          UDPv4    0.0.0.0:0                      *:*                                 4516     dns.exe        2020-12-18 03:42:44 UTC+0000
0xddae900          UDPv4    0.0.0.0:0                      *:*                                 4516     dns.exe        2020-12-18 03:42:44 UTC+0000
0xde48900          UDPv4    0.0.0.0:0                      *:*                                 4516     dns.exe        2020-12-18 03:42:44 UTC+0000
0xde75900          UDPv4    0.0.0.0:0                      *:*                                 4516     dns.exe        2020-12-18 03:42:44 UTC+0000
0xde777b0          UDPv4    0.0.0.0:0                      *:*                                 4516     dns.exe        2020-12-18 03:42:44 UTC+0000
0xde77ec0          UDPv4    0.0.0.0:0                      *:*                                 4516     dns.exe        2020-12-18 03:42:44 UTC+0000
0xde795e0          UDPv4    0.0.0.0:0                      *:*                                 4516     dns.exe        2020-12-18 03:42:44 UTC+0000
0xde79cf0          UDPv4    0.0.0.0:0                      *:*                                 4516     dns.exe        2020-12-18 03:42:44 UTC+0000
0xde89490          UDPv4    0.0.0.0:0                      *:*                                 4516     dns.exe        2020-12-18 03:42:44 UTC+0000
0xde89ba0          UDPv4    0.0.0.0:0                      *:*                                 4516     dns.exe        2020-12-18 03:42:44 UTC+0000
0xde8ba60          UDPv4    0.0.0.0:0                      *:*                                 4516     dns.exe        2020-12-18 03:42:44 UTC+0000
0xdec6340          UDPv4    0.0.0.0:0                      *:*                                 4516     dns.exe        2020-12-18 03:42:44 UTC+0000
0xdec6a50          UDPv4    0.0.0.0:0                      *:*                                 4516     dns.exe        2020-12-18 03:42:44 UTC+0000
0xdeed010          UDPv4    0.0.0.0:0                      *:*                                 4516     dns.exe        2020-12-18 03:42:44 UTC+0000
0xdeed900          UDPv4    0.0.0.0:0                      *:*                                 4516     dns.exe        2020-12-18 03:42:44 UTC+0000
0xdef2490          UDPv4    0.0.0.0:0                      *:*                                 4516     dns.exe        2020-12-18 03:42:44 UTC+0000
0xdef2ba0          UDPv4    0.0.0.0:0                      *:*                                 4516     dns.exe        2020-12-18 03:42:44 UTC+0000
0xdefb490          UDPv4    0.0.0.0:0                      *:*                                 4516     dns.exe        2020-12-18 03:42:44 UTC+0000
0xdefbba0          UDPv4    0.0.0.0:0                      *:*                                 4516     dns.exe        2020-12-18 03:42:44 UTC+0000
```

Figure 13: netscan command

Many victims were infected with multiple forms of malware in a number of ways in the SolarWinds attack, so being thorough during a forensic investigation is critical to guarantee you've found the full spectrum of a potential infection. (Hack eXPlorer, 2020)

3.5. DISSEMINATION

Two types of channels should be used to transmit the processed and refined information obtained from the analysis and production stages in the form of intelligence products. They are standard and alarm.

This intelligence is communicated with Lead System Admin, Security Operations Centre (SOC) Analysts, and the Daily Security Operations (SecOps) meetings via normal channels but, the Cyber Intelligence Reports are communicated with other entities via the Alarm route.

Alarm: Cyber Intel Report		
Date	04/09/2019	Preliminary Summary
Attack Type	APT	SolarWinds is a Texas-based IT management software company that is widely utilised in the public and private sectors, especially in the United States. The threat was discovered on a
Sources	Cisco Talos Incident Response (CTIR)	
Organisations Impacted	Yes	
Affected Region	North America, Europe, Asia, and the Middle East	

Affected Countries	United States of America, German, Mexico, Israel, Canada, Spain, Belgium, the United Arab Emirates, and the United Kingdom	SolarWinds Orion network management tool deployment. After that, the attacker, who is thought to be a Russian threat actor, gained access to the SolarWinds production environment as well as the victim's Microsoft 365 and Azure cloud environments.
Objective	Industrial Sabotage	
Attack Vector	SolarWinds Orion Platform Version 2019.4 HF 5	
	SolarWinds Orion Platform Version 2020.2	
	SolarWinds Orion Platform Version 2020.2 HF 1	

Table 7: Alarm channel CTI Report

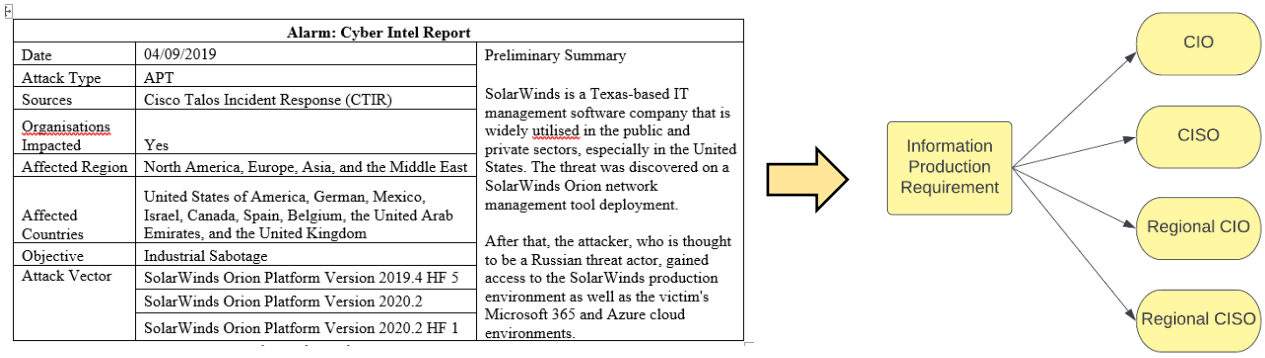


Figure 14: Alarm communication Channel

The alarm channel communication is exchanged with various appropriate authorities, such as organisational and regional CIOs and CISOs, via an intelligence product.

3.6. UTILISATION

As the final stage of the intelligence cycle, utilisation should be used to carry out actions in response to the information gathered. The regional CIO and CISO are in charge of notifying the relevant business leaders, as shown in the diagram. It is then up to corporate leaders to assign different teams to carry out appropriate tasks, such as informing the threat, which should be handled by the information security team and the IT Helpdesk. Forensic analysts will be responsible for reviewing traffic for IOCs. The findings will be communicated via the IT helpdesk and forensic analysts. Cisco Talos Incident Response and Threat Intelligence teams

should be in charge of monitoring and implementing endpoint protection products.

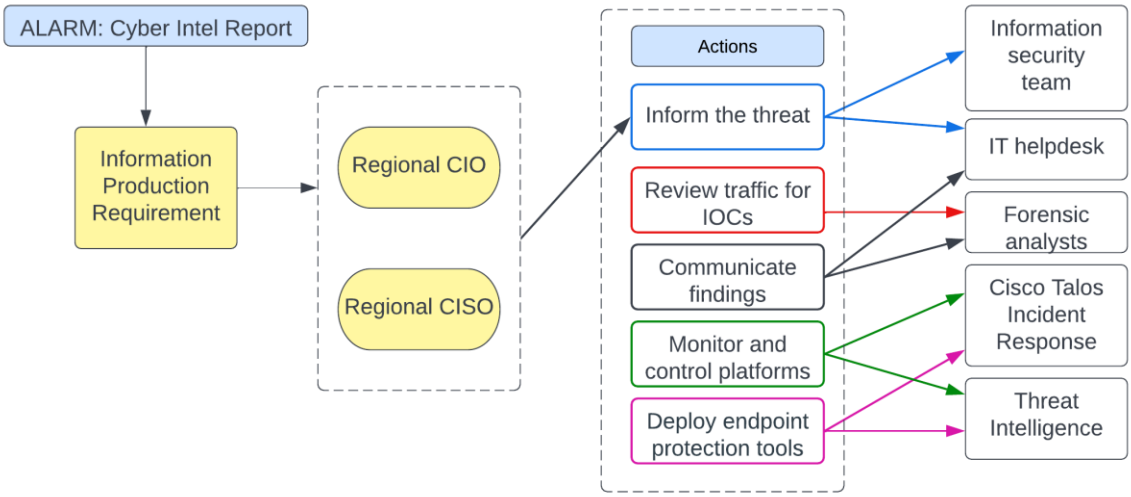


Figure 15: Taking actions on Intelligence

4. MITIGATION

The intelligence obtained throughout the intelligence cycle procedure is extremely important in preventing such attacks. Figure 14 depicts how we can automate the entire process and use the intelligence product to protect ourselves from SolarWinds malware.

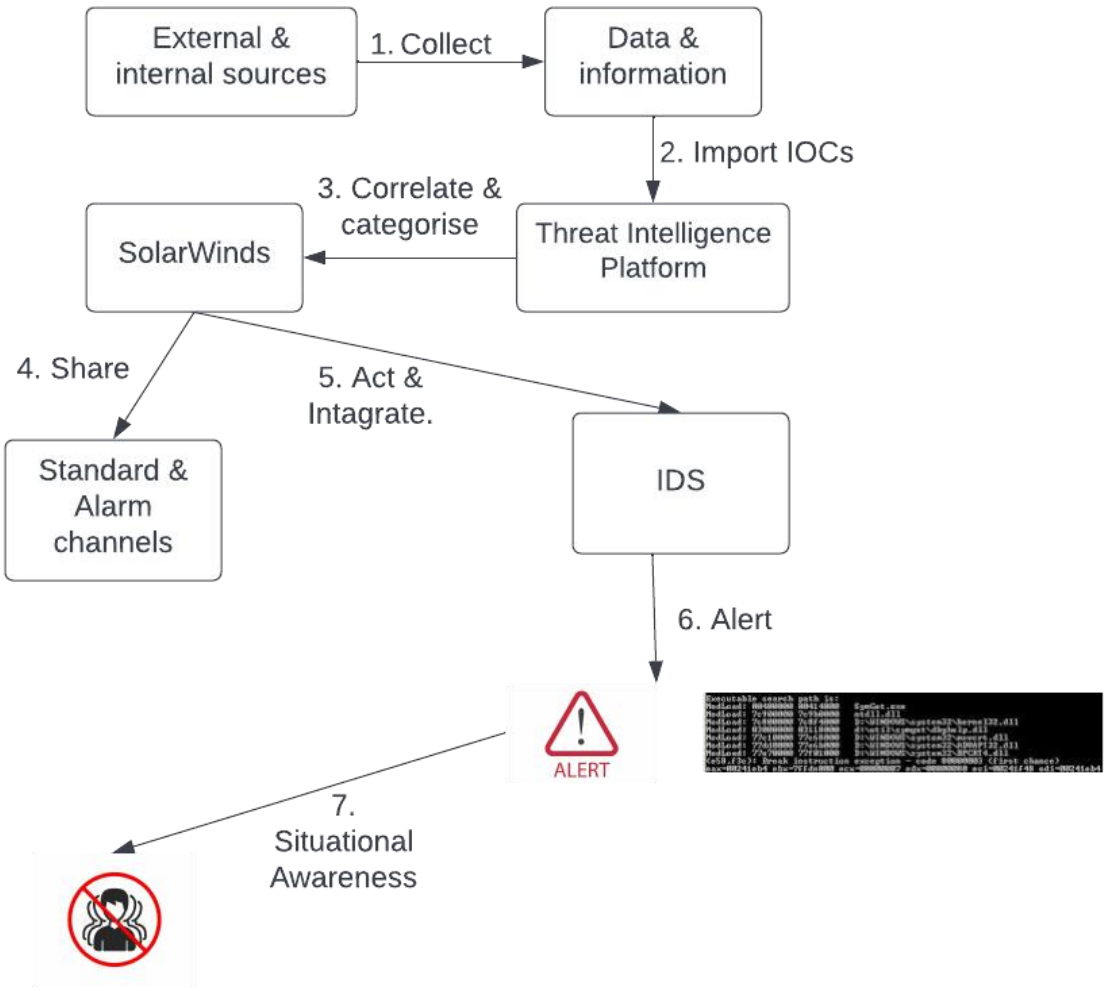


Figure 16: TIP and CTI for SolarWinds attack

5. RECOMMENDATION AND UNSOLVED PROBLEMS

SolarWinds responded by releasing a new version of its software, although there is fear that even this may pose a risk due to the attacker's ability to identify weaknesses. In addition to the advice of the cybersecurity agency warnings, stakeholders should completely evaluate the available diagnostics and mitigation methods.

1. Regularly review your log retention policy.

2. Make it a habit to test upgrades from a security standpoint.

3. To help you locate the TTPs, understand your network and use Behavioral Network Analytics.

4. Collaboration is the key when it comes to collective defence. (Cyber Management Alliance, 2021)

5. Updating antivirus or EDR software to detect compromised SolarWinds libraries and potentially unusual process behaviour caused by these binaries is a good idea. Consider completely disabling SolarWinds in your environment until you're certain you have a reliable build free of injected code. Consult SolarWinds' Security Advisory for further information.

6. Using your network infrastructure, block the known C2 endpoints listed below in IOCs.

7. When it comes to securing your SAML token signing keys, follow the best practises recommended by your identity federation technology vendor. If your identity federation technology supplier enables it, consider using hardware security for your SAML token signing certificates. For more information, contact your identity federation technology supplier. Review Microsoft's recommendations for Active Directory Federation Services here: Securing ADFS: Best Practices

8. Ensure that administrative user accounts adhere to best practices, such as using privileged access workstations, JIT/JEA, and strong authentication. Reduce the number of users who have access to Directory Roles with high privileges, such as Global Administrator, Application Administrator, and Cloud Application Administrator.

9. Ensure that administrative service accounts and service principals employ high-entropy secrets, such as certificates, that are held securely. As part of your security monitoring programme, keep an eye on changes to the secrets used for service accounts and service principals. Keep an eye out for unusual service account usage. Keep an eye on your sign-ins. Session anomalies are detected by Microsoft Azure AD, as well as Microsoft Cloud App Security if it is enabled.

10. Remove/disable unwanted or superfluous apps and service principles to save space. Reduce active application and service principal permissions, particularly application (AppOnly) permissions. (Microsoft Security Response Center, 2020)

In the field of CTI, there are a few unsolved difficulties that are mentioned here. Some industries are unable to utilise CTI fully and efficiently due to its lack of development. Although there are multiple standards for describing CTI data in structured format have been created for exchanging intelligence, keeping up with them while using this technology is difficult, complex, and costly as these are developing standards.

6. CONCLUSION

The SolarWinds SUNBURST cyberattack is the most well-known in recent years. The attackers exploited a hacked supply chain to attack a variety of clients, including federal government agencies and tech firms. In the hands of cyber criminals, it might be a lethal weapon. As a result, enterprises may mitigate such attacks by employing cutting-edge tactics such as CTI, exchanging threat intelligence, and building cybersecurity alliances.

REFERENCES

Abrams, L. (2020, December 19). *The SolarWinds cyberattack: The hack, the victims, and what we know*. Retrieved from BleepingComputer: https://www.bleepingcomputer.com/news/security/the-solarwinds-cyberattack-the-hack-the-victims-and-what-we-know/

BIASINI, N. (2020, December 14). *Threat Advisory: SolarWinds supply chain attack*. Retrieved from TalosIntelligence: https://blog.talosintelligence.com/2020/12/solarwinds-supplychain-coverage.html

Black Hat. (2020, January 15). Investigating Malware Using Memory Forensics - A Practical Approach. Retrieved from https://www.youtube.com/watch?v=BMFCdAGxVN4

Center for Internet Security. (2021, March 15). *The SolarWinds Cyber-Attack: What You Need to Know*. Retrieved from Center for Internet Security: https://www.cisecurity.org/solarwinds

Cyber Management Alliance. (2021, November 16). *What really happened in the SolarWinds cyber-attack?* Retrieved from Cyber Management Alliance: https://www.cm-alliance.com/cybersecurity-blog/what-really-happened-in-the-solarwinds-cyber-attack

Cybersecurity and Infrastructure Security Agency. (2021, April 15). *Detecting Post-Compromise Threat Activity in Microsoft Cloud Environments*. Retrieved January 8, 2021, from Cybersecurity and Infrastructure Security Agency: https://www.cisa.gov/uscert/ncas/alerts/aa21-008a

ENISA. (2020, April). *Emerging.* European Union Agency for Cybersecurity. Retrieved January 2019, from https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/etl-review-folder/etl-2020-emerging-trends

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

Hack eXPlorer. (2020, January 24). Using Memory forensics in security investigations - Volatility. Retrieved from Youtube: https://www.youtube.com/watch?v=eluS7_eSm8M

Henneberry, B. (2021, February 22). *Anatomy of the SolarWinds Attack: Five Types of Malware*. Retrieved from Blumira: https://www.blumira.com/solarwinds-attack-anatomy-five-types-of-malware/#:~:text=SUNSPOT%2C%20SUNBURST%2C%20SUPERNOVA%2C%20TEARDROP%2C%20and%20RAINDROP%20have%20been,SUNBURST%20backdoor%20code%20into%20the%20software%20update%20pipeline.?msclkid=8e0cc44aa

Ingalls, S. (2021, February 3). *Protecting Against Solorigate TTPs: SolarWinds Hack Defenses*. Retrieved from eSecurityPlanet: https://www.esecurityplanet.com/threats/protecting-against-solorigate-ttps-solarwinds-hack/

Maccaglia, S. (2020). *Sunburst Analysis.* RSA. Retrieved from https://community.securid.com/yfcdo34327/attachments/yfcdo34327/netwitness-blog/1886/1/Sunburst%20Analysis%20-%20SMaccaglia%20-%20RSA%20IR%20Team.pdf

Mandiant. (2020, December 17). *sunburst_countermeasures.* Retrieved from Github: https://github.com/mandiant/sunburst_countermeasures

Microsoft. (2021, January 20). *Deep dive into the Solorigate second-stage activation: From SUNBURST to TEARDROP and Raindrop*. Retrieved from Microsoft: https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/

Microsoft Security Response Center. (2020, December 13). *Customer Guidance on Recent Nation-State Cyber Attacks*. Retrieved from Microsoft: https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/

SENATOR ROY BLUNT, CHAIRMAN. (2021, January 29). *THE SOLARWINDS CYBERATTACK*. Retrieved from https://www.rpc.senate.gov/policy-papers/the-solarwinds-cyberattack

Stuker, V. J. (2021, January 7). *DOMAIN GENERATION ALGORITHMS OR HOW TO EASILY DETECT THE SUNBURST / SOLARWINDS HACK*. Retrieved from Stucker: https://stuker.com/2021/domain-generation-algorithms-or-how-to-easily-detect-the-sunburst-solarwinds-hack/

The Hacker News. (2021, April 13). *Detecting the "Next" SolarWinds-Style Cyber Attack*. Retrieved from The Hacker News: https://thehackernews.com/2021/04/detecting-next-solarwinds-attack.html