One of The Biggest Cybersecurity Companies In The World Just Got Hacked

In a blog post, FireEye CEO Kevin Mandia said the company was targeted by "a nation with top-tier offensive capabilities."

By Joseph Cox

December 8, 2020, 3:53pm

FireEye, a top-end cybersecurity firm that works to protect government and corporate systems alike, itself announced on Tuesday it was the target of what it described as hackers from "a nation with top-tier offensive capabilities," with the hackers stealing FireEye's own offensive tools which could be used for future hacking operations.

The news highlights how those in the cybersecurity industry can also be the target of hackers, and in particular, those who may hold valuable hacking techniques.

"This attack is different from the tens of thousands of incidents we have responded to throughout the years," FireEye CEO Kevin Mandia wrote in a blog post. "The attackers tailored their world-class capabilities specifically to target and attack FireEye. They are highly trained in operational security and executed with discipline and focus. They operated clandestinely, using methods that counter security tools and forensic examination. They used a novel combination of techniques not witnessed by us or our partners in the past."

Specifically, the announcement said FireEye found the hackers stole "Red Team assessment tools," tools that are used to offensively test systems' security for the benefit of customers who want to make sure that their defenses could withstand a real attack. In response, FireEye released methods for detecting the use of such tools, presumably in case the hackers decide to use them in the future.

"We are not sure if the attacker intends to use our Red Team tools or to publicly disclose them. Nevertheless, out of an abundance of caution, we have developed more than 300 countermeasures for our customers, and the community at large, to use in order to minimize the potential impact of the theft of these tools," Mandia's post added.

The FireEye announcement added that the attacker primarily sought out information related to "certain government customers."

"While the attacker was able to access some of our internal systems, at this point in our investigation, we have seen no evidence that the attacker exfiltrated data from our primary systems that store customer information from our incident response or consulting engagements or the metadata collected by our products in our dynamic threat intelligence systems," it added.

The case bears some similarities to that of a theft of offensive hacking tools used by the NSA. In 2016, a group of self-described hackers calling themselves the Shadow Brokers started to publicly release powerful exploits stolen from the agency. Microsoft issued patches for a number of the underlying vulnerabilities, but other hackers were still able to adapt and use the exploits for their own purposes. Famously, the WannaCry ransomware attack, which devastated networks across the world, including in hospitals, made use of code the Shadow Brokers released. Multiple private and government entities have attributed the WannaCry attacks to hackers working on behalf of North Korea.

The Shadow Brokers dump included zero day exploits, which take advantage of vulnerabilities which, at the time of release, impacted manufacturers were not aware of, and so couldn't create a patch. FireEye's announcement said its own stolen toolkit did not include zero day exploits.

FireEye has been involved in responding to some of the most high profile hacks stretching back years, including Sony, Equifax, and Anthem.

"We have come to expect and demand that companies take real steps to secure their systems, but this case also shows the difficulty of stopping determined nation-state hackers. As we have with critical infrastructure, we have to rethink the kind of cyber assistance the government provides to American companies in key sectors on which we all rely," Senator Mark Warner said in a statement reacting to news of the hack.

Threat Research

Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor

December 13, 2020 | by FireEye

FIREEYE EVASION SUPPLY CHAIN

Executive Summary

- We have discovered a global intrusion campaign. We are tracking the actors behind this campaign as UNC2452.
- FireEye discovered a supply chain attack trojanizing SolarWinds Orion business software updates in order to distribute malware we call SUNBURST.

- The attacker's post compromise activity leverages multiple techniques to evade detection and obscure their activity, but these efforts also offer some opportunities for detection.
- The campaign is widespread, affecting public and private organizations around the world.
- FireEye is releasing signatures to detect this threat actor and supply chain attack in the wild. These are found on our public GitHub page. FireEye products and services can help customers detect and block this attack.

Summary

FireEye has uncovered a widespread campaign, that we are tracking as UNC2452. The actors behind this campaign gained access to numerous public and private organizations around the world. They gained access to victims via trojanized updates to SolarWind's Orion IT monitoring and management software. This campaign may have begun as early as Spring 2020 and is currently ongoing. Post compromise activity following this supply chain compromise has included lateral movement and data theft. The campaign is the work of a highly skilled actor and the operation was conducted with significant operational security.

SUNBURST Backdoor

SolarWinds.Orion.Core.BusinessLayer.dll is a SolarWinds digitally-signed component of the Orion software framework that contains a backdoor that communicates via HTTP to third party servers. We are tracking the trojanized version of this SolarWinds Orion plug-in as SUNBURST.

After an initial dormant period of up to two weeks, it retrieves and executes commands, called "Jobs", that include the ability to transfer files, execute files, profile the system, reboot the machine, and disable system services. The malware masquerades its network traffic as the Orion Improvement Program (OIP) protocol and stores reconnaissance results within legitimate plugin configuration files allowing it to blend in with legitimate SolarWinds activity. The backdoor uses multiple obfuscated blocklists to identify forensic and anti-virus tools running as processes, services, and drivers.

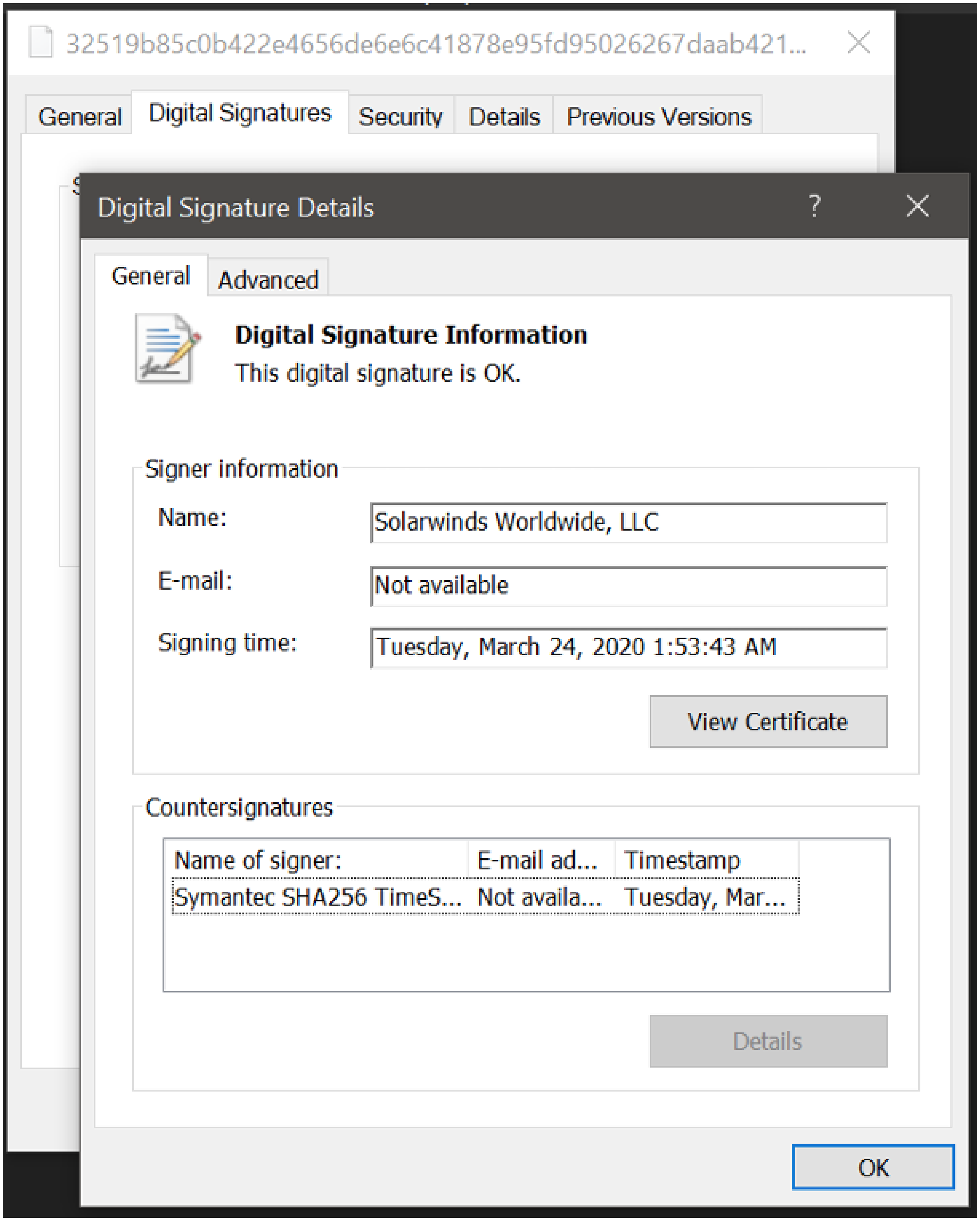

Figure 1: SolarWinds digital signature on software with backdoor

Multiple trojanzied updates were digitally signed from March - May 2020 and posted to the SolarWinds updates website, including:

- hxxps://downloads.solarwinds[.]com/solarwinds/CatalogResources/Core/2019.4/2019.4.5220.20574/SolarWinds-Core-v2019.4.5220-Hotfix5.msp

The trojanized update file is a standard Windows Installer Patch file that includes compressed resources associated with the update, including the trojanized SolarWinds.Orion.Core.BusinessLayer.dll component. Once the update is installed, the malicious DLL will be loaded by the legitimate SolarWinds.BusinessLayerHost.exe or SolarWinds.BusinessLayerHostx64.exe (depending on system configuration). After a dormant period of up to two weeks, the malware will attempt to resolve a subdomain of avsvmcloud[.]com. The DNS response will return a CNAME record that points to a Command and Control (C2) domain. The C2 traffic to the malicious domains is designed to mimic normal SolarWinds API communications. The list of known malicious infrastructure is available on FireEye's GitHub page.

Worldwide Victims Across Multiple Verticals

FireEye has detected this activity at multiple entities worldwide. The victims have included government, consulting, technology, telecom and extractive entities in North America, Europe, Asia and the Middle East. We anticipate there are additional victims in other countries and verticals. FireEye has notified all entities we are aware of being affected.

Post Compromise Activity and Detection Opportunities

We are currently tracking the software supply chain compromise and related post intrusion activity as UNC2452. After gaining initial access, this group uses a variety of techniques to disguise their operations while they move laterally (Figure 2). This actor prefers to maintain a light malware footprint, instead preferring legitimate credentials and remote access for access into a victim's environment.

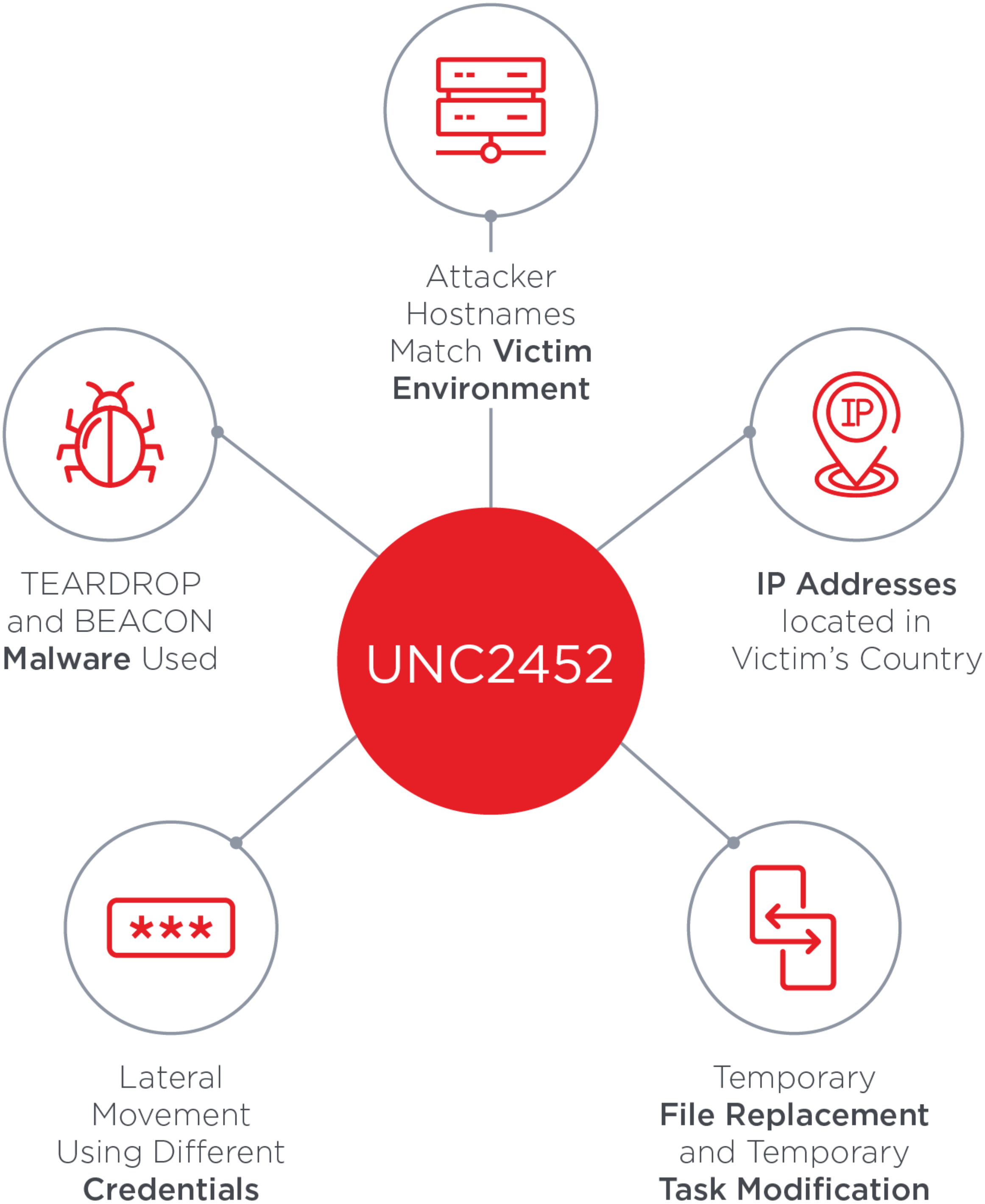

Figure 2: Post-compromise tactics

This section will detail the notable techniques and outline potential opportunities for detection.

TEARDROP and BEACON Malware Used

Multiple SUNBURST samples have been recovered, delivering different payloads. In at least one instance the attackers deployed a previously unseen memory-only dropper we've dubbed TEARDROP to deploy Cobalt Strike BEACON.

TEARDROP is a memory only dropper that runs as a service, spawns a thread and reads from the file "gracious_truth.jpg", which likely has a fake JPG header. Next it checks that HKU\SOFTWARE\Microsoft\CTF exists, decodes an embedded payload using a custom rolling XOR algorithm and manually loads into memory an embedded payload using a custom PE-like file format. TEARDROP does not have code overlap with any previously seen malware. We believe that this was used to execute a customized Cobalt Strike BEACON.

Mitigation: FireEye has provided two Yara rules to detect TEARDROP available on our GitHub. Defenders should look for the following alerts from FireEye HX: MalwareGuard and WindowsDefender:
Process Information

> file_operation_closed
> file-path*: “c:\\windows\\syswow64\\netsetupsvc.dll
> actor-process:
> pid: 17900

Window’s defender Exploit Guard log entries: (Microsoft-Windows-Security-Mitigations/KernelMode event ID 12)

> Process”\Device\HarddiskVolume2\Windows\System32\svchost.exe” (PID XXXXX) would have been blocked from loading the non-Microsoft-signed binary
> ‘\Windows\SysWOW64\NetSetupSvc.dll’

Attacker Hostnames Match Victim Environment
The actor sets the hostnames on their command and control infrastructure to match a legitimate hostname found within the victim’s environment. This allows the adversary to blend into the environment, avoid suspicion, and evade detection.

Detection Opportunity
The attacker infrastructure leaks its configured hostname in RDP SSL certificates, which is identifiable in internet-wide scan data. This presents a detection opportunity for defenders -- querying internet-wide scan data sources for an organization’s hostnames can uncover malicious IP addresses that may be masquerading as the organization. (Note: IP Scan history often shows IPs switching between default (WIN-*) hostnames and victim’s hostnames) Cross-referencing the list of IPs identified in internet scan data with remote access logs may identify evidence of this actor in an environment. There is likely to be a single account per IP address.

IP Addresses located in Victim’s Country
The attacker’s choice of IP addresses was also optimized to evade detection. The attacker primarily used only IP addresses originating from the same country as the victim, leveraging Virtual Private Servers.

Detection Opportunity
This also presents some detection opportunities, as geolocating IP addresses used for remote access may show an impossible rate of travel if a compromised account is being used by the legitimate user and the attacker from disparate IP addresses. The attacker used multiple IP addresses per VPS provider, so once a malicious login from an unusual ASN is identified, looking at all logins from that ASN can help detect additional malicious activity. This can be done alongside baselining and normalization of ASN’s used for legitimate remote access to help identify suspicious activity.

Lateral Movement Using Different Credentials
Once the attacker gained access to the network with compromised credentials, they moved laterally using multiple different credentials. The credentials used for lateral movement were always different from those used for remote access.

Detection Opportunity
Organizations can use HX’s LogonTracker module to graph all logon activity and analyze systems displaying a one-to-many relationship between source systems and accounts. This will uncover any single system authenticating to multiple systems with multiple accounts, a relatively uncommon occurrence during normal business operations.

Temporary File Replacement and Temporary Task Modification
The attacker used a temporary file replacement technique to remotely execute utilities: they replaced a legitimate utility with theirs, executed their payload, and then restored the legitimate original file. They similarly manipulated scheduled tasks by updating an existing legitimate task to execute their tools and then returning the scheduled task to its original configuration. They routinely removed their tools, including removing backdoors once legitimate remote access was achieved.

Detection Opportunity

Defenders can examine logs for SMB sessions that show access to legitimate directories and follow a delete-create-execute-delete-create pattern in a short amount of time. Additionally, defenders can monitor existing scheduled tasks for temporary updates, using frequency analysis to identify anomalous modification of tasks. Tasks can also be monitored to watch for legitimate Windows tasks executing new or unknown binaries.

This campaign's post compromise activity was conducted with a high regard for operational security, in many cases leveraging dedicated infrastructure per intrusion. This is some of the best operational security that FireEye has observed in a cyber attack, focusing on evasion and leveraging inherent trust. However, it *can* be detected through persistent defense.

In-Depth Malware Analysis

SolarWinds.Orion.Core.BusinessLayer.dll (b91ce2fa41029f6955bff20079468448) is a SolarWinds-signed plugin component of the Orion software framework that contains an obfuscated backdoor which communicates via HTTP to third party servers. After an initial dormant period of up to two weeks, it retrieves and executes commands, called "Jobs", that include the ability to transfer and execute files, profile the system, and disable system services. The backdoor's behavior and network protocol blend in with legitimate SolarWinds activity, such as by masquerading as the Orion Improvement Program (OIP) protocol and storing reconnaissance results within plugin configuration files. The backdoor uses multiple blocklists to identify forensic and anti-virus tools via processes, services, and drivers.

Unique Capabilities

- Subdomain DomainName Generation Algorithm (DGA) is performed to vary DNS requests
  - CNAME responses point to the C2 domain for the malware to connect to
  - The IP block of A record responses controls malware behavior
  - DGA encoded machine domain name, used to selectively target victims
- Command and control traffic masquerades as the legitimate Orion Improvement Program
- Code hides in plain site by using fake variable names and tying into legitimate components

Delivery and Installation

Authorized system administrators fetch and install updates to SolarWinds Orion via packages distributed by SolarWinds's website. The update package CORE-2019.4.5220.20574-SolarWinds-Core-v2019.4.5220-Hotfix5.msp (02af7cec58b9a5da1c542b5a32151ba1) contains the SolarWinds.Orion.Core.BusinessLayer.dll described in this report. After installation, the Orion software framework executes the .NET program SolarWinds.BusinessLayerHost.exe to load plugins, including SolarWinds.Orion.Core.BusinessLayer.dll. This plugin contains many legitimate namespaces, classes, and routines that implement functionality within the Orion framework. Hidden in plain sight, the class SolarWinds.Orion.Core.BusinessLayer.OrionImprovementBusinessLayer implements an HTTP-based backdoor. Code within the logically unrelated routine SolarWinds.Orion.Core.BusinessLayer.BackgroundInventory.InventoryManager.RefreshInternal invokes the backdoor code when the Inventory Manager plugin is loaded.

SolarWinds.Orion.Core.BusinessLayer.dll is signed by SolarWinds, using the certificate with serial number 0f:e9:73:75:20:22:a6:06:ad:f2:a3:6e:34:5d:c0:ed. The file was signed on March 24, 2020.

Initialization

On execution of the malicious SolarWinds.Orion.Core.BusinessLayer.OrionImprovementBusinessLayer.Initialize method the sample verifies that its lower case process name hashes to the value 17291806236368054941. This hash value is calculated as the standard FNV-1A 64-bit hash with an additional XOR by 6605813339339102567 after computing the FNV-1A. This hash matches a process named "solarwinds.businesslayerhost".

The sample only executes if the filesystem write time of the assembly is at least 12 to 14 days prior to the current time; the exact threshold is selected randomly from an interval. The sample continues to check this time threshold as it is run by a legitimate recurring background task. Once the threshold is met, the sample creates the named pipe 583da945-62af-10e8-4902-a8f205c72b2e to act as a guard that only one instance is running before reading SolarWinds.Orion.Core.BusinessLayer.dll.config from disk and retrieving the XML field appSettings. The appSettings fields' keys are legitimate values that the malicious logic re-purposes as a persistent configuration. The key ReportWatcherRetry must be any value other than 3 for the sample to continue execution.

The sample checks that the machine is domain joined and retrieves the domain name before execution continues. A userID is generated by computing the MD5 of a network interface MAC address that is up and not a loopback device, the domain name, and the registry value HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MachineGuid. The userID is encoded via a custom XOR scheme after the MD5 is calculated. The ReportWatcherPostpone key of appSettings is then read from SolarWinds.Orion.Core.BusinessLayer.dll.config to retrieve the initial, legitimate value. This operation is performed as the sample later bit packs flags into this field and the initial value must be known in order to read out the bit flags. The sample then invokes the method Update which is the core event loop of the sample.

DGA and Blocklists

The backdoor determines its C2 server using a Domain Generation Algorithm (DGA) to construct and resolve a subdomain of avsvmcloud[.]com. The Update method is responsible for initializing cryptographic helpers for the generation of these random C2 subdomains. Subdomains are generated by concatenating a victim userId with a reversible encoding of the victims local machine domain name. The attacker likely utilizes the DGA subdomain to vary the DNS response to victims as a means to control the targeting of the malware. These subdomains are concatenated with one of the following to create the hostname to resolve:

- .appsync-api.eu-west-1[.]avsvmcloud[.]com
- .appsync-api.us-west-2[.]avsvmcloud[.]com
- .appsync-api.us-east-1[.]avsvmcloud[.]com
- .appsync-api.us-east-2[.]avsvmcloud[.]com

Process name, service name, and driver path listings are obtained, and each value is hashed via the FNV-1a + XOR algorithm as described previously and checked against hardcoded blocklists. Some of these hashes have been brute force reversed as part of this analysis, showing that these routines are scanning for analysis tools and antivirus engine components. If a blocklisted process is found the Update routine exits and the sample will continue to try executing the routine until the blocklist passes. Blocklisted services are stopped by setting their HKLM\SYSTEM\CurrentControlSet\services\<service_name>\Start registry entries to value 4 for disabled. Some entries in the service list if found on the system may affect the DGA algorithms behavior in terms of the values generated. The list of stopped services is then bit-packed into the ReportWatcherPostpone key of the appSettings entry for the samples' config file. If any service was transitioned to disabled the Update method exits and retries later. The sample retrieves a driver listing via the WMI query Select * From Win32_SystemDriver. If any blocklisted driver is seen the Update method exits and retries. If all blocklist tests pass, the sample tries to resolve api.solarwinds.com to test the network for connectivity.