SolarWinds Teknisk Reference

Reference: https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

Dato: 15. december 2020

Sagsnr.: NIL
Dok. nr.: NIL

Forsvarets Efterretningstjeneste
Kastellet 30
2100 København Ø

Tlf.: 33 32 55 80
E-mail: cfcs@cfcs.dk
www.cfcs.dk

Aktøren UNC2452 (FireEye) har foretaget et Supply Chain Attack mod SolarWinds Orion business software updates, hvilket har gjort at en malware kaldet SUNBURST kan distribueres til brugere af SolarWinds Orion softwaren. FireEye mener, at kampagnen allerede kan være startet i foråret 2020.

SolarWinds.Orion.Core.BusinessLayer.dll er en digitalt signeret dll komponent af SolarWinds Orion software framework, som indeholder en bagdør der kommunikerer via HTTP til tredjepartsservere. Denne trojaniserede version af SolarWinds Orion pluginnet bliver – af FireEye – kaldt SUNBURST.

Malwaren starter med at slumre i 2 uger. Herefter modtager & eksekverer den såkaldte 'Jobs', som bl.a. inkluderer filoverførsel, fileksekvering, systemprofilering, system genstart og deaktivering af systemservices.

Malwaren skjuler sig i netværkstrafikken som Orion Improvement Program (OIP) protokollen og gemmer rekognoscerings resultater i legitime plugin konfigurationsfiler, hvilket tillader den at blænde sig ind i legitim SolarWinds-aktivitet. Bagdøren bruger flere obfuskerede blokeringslister til at identificere forensics- og anti-virusværktøjer, som kan køre som processer, services og/eller drivere.

Flere trojaniserede opdateringerne er digitalt signeret fra marts – maj 2020 og uploadet til SolarWinds opdaterings hjemmeside.

Filen er en standard Windows Installer Patch-fil der inkluderer komprimerede ressourcer associeret med opdateringen, herunder den ondsindede SolarWinds.Orion.Core.BusinessLayer.dll komponent.

Når opdateringen er installeret vil den ondsindede DLL blive loaded af den legitime SolarWinds.BusinessLayerHost.exe eller SolarWinds.BusinessLayer-Hostx64.exe alt efter systemopsætningen.

Herefter kommer slumre-perioden på op til 2 uger, hvorefter malwaren vil forsøge at resolve et subdomæne på avsvmcloud[.]com. DNS-svaret

vil returnere en CNAME-record (Canonical Name Record – der mapper et domænenavn (alias) til et andet (canonical name)) der peger på et C2 domæne.

C2-trafikken til det ondsindede domæne er signed til at efterligne normal SolarWinds API kommunikation.

Listen af kendt ondsindet infrastruktur er tilgængelig på FireEyes GitHub:
https://github.com/fireeye/sunburst_countermeasures

Efter succesfuld kompromittering af en virksomheds SolarWinds Orion software, forsøger aktøren sig med flere forskellige teknikker for at skjule deres aktivitet, mens de påbegynder lateral movement.

Flere SUNBURST-samples indeholder metoder til at levere forskellige payloads. Herunder bl.a. en ukendt memory-only dropper, som FireEye har kaldt TEARDROP.

Derudover er der også set deployering af Cobalt Strike-beacon.

TEARDROP er en memory-only dropper der kører som en 'service', som spawner en tråd og læser fra en fil kaldet "gracious_truth.jpg" – som muligvis indeholder en falsk JPG header.

Derefter tjekker den at registry nøglen "HKU\SOFTWARE\Microsoft\CTF" eksisterer, hvorefter den decoder et embedded payload ved brug af en custom rolling XOR-algoritme, der manuelt indlæser et embedded payload, som benytter en custom PE-lignende filformat, ind i memory.

TEARDROP deler ikke kode med tidligere observeret malware, og menes at blive brugt til at eksekvere en custom Cobalt Strike-beacon.

SolarWinds.Orion.Core.BusinessLayer.dll (b91ce2fa41029f6955bff20079468448) har en Subdomain DGA (DomainName Generation Algorithm) der genererer forskellige DNS requests; CNAME-svar peger til et C2 domæne, som malwaren kommunikerer med.

IP-blokken af A-record svar kontrollerer malwarens opførsel. C2-trafikken efterligner den legitime OIP (Orion Improvement Program) protokol. Koden skjuler sig ved at bruge falske variabelnavne samtidig med at skrive til legitime komponenter.

Opdateringspakken CORE-2019.4.5220.20574-SolarWinds-Core-v2019.4.5220-Hotfix5.msp[1] indeholder SUNBURST.

Efter installationen vil Orion softwareframeworket eksekvere .NET programmet SolarWinds.BusinessLayerHost.exe, som loader plugins, herunder SolarWinds.Orion.Core.BusinessLayer.dll (SUNBURST).

[1] 02af7cec58b9a5da1c542b5a32151ba1

Denne fil indeholder mange legitime namespaces, klasser og rutiner, der står for funktionaliter i Orion-frameworket. Dog indeholder filen også en HTTP-baseret bagdør i klassen SolarWinds.Orion.Core.BusinessLayer.OrionImprovementBusinessLayer.

Koden i den logisk urelaterede rutine SolarWinds.Orion.Core.BusinessLayer.BackgroundInventory.InventoryManager.RefreshInternal starter koden til bagdøren når 'Inventory Manager' pluginnet er loadet.

SolarWinds.Orion.Core.BusinessLayer.dll er signeret af SolarWinds, og bruger et certifikat med serienummeret: 0f:e9:73:75:20:22:a6:06:ad:f2:a3:6e:34:5d:c0:ed.

Filen er signeret d. 24. marts 2020.

Ved eksekvering af den ondsindede SolarWinds.Orion.Core.BusinessLayer.OrionImprovementBusinessLayer.Initialize metode, verificeres at dens process navn (i lowercase) har følgende hashværdi: 17291806236368054941.

Denne hashværdi er beregnet som den standard FNV-1A 64 bit hash med en ekstra XOR af 6605813339339102567 efter FNV-1A. Denne hashværdi matcher en proces kaldet businesslayerhost.exe.

Malwaren eksekverer kun, hvis filsystemets skrivetid er mindst 12 til 14 dage før eksekveringstiden. Det præcise tidspunkt er valgt tilfældigt baseret på et interval mellem 12 og 14 dage.

Hvis dette er opfyldt, vil der blive lavet en named pipe 583da945-62af-10e8-4902-a8f205c72b2e, der agerer som en sikkerhed for at kun et eksemplar af malwaren kører, før SolarWinds.Orion.Core.BusinessLayer.dll.config er læst fra disken, og XML-feltet 'appSettings' hentes.

'appSettings'-feltet er en legitim værdi, som den ondsindede kode genbruger som en persistent konfiguration.

Hvis 'ReportWatchRetry' er en hvilken som helst anden værdi end 3, fortsætter eksekveringen. Herefter tjekker malwaren om computeren er domænestyret, og henter domænenavnet før den fortsætter. Et userID bliver generet ved at tage en MD5 værdi af alle netværksinterfaces MAC-adresser der er oppe, ikke-loopback enheder, domænenavnet samt registry-værdien "HKEY_LOCAL_MACHINE\SOFTWARE\Microoft\Cryptography\MachineGuid".

UserID er encoded via et custom XOR-skema efter MD5-værdien er beregnet. ReportWatcherPostpone værdien af appSettings bliver herefter læst fra SolarWinds.Orion.Core.BusinessLayer.dll.config til at hente den legitime værdi.

Bagdøren finder sin C2 server ved brug af DGA til at beregne og resolve et subdomæne af 'avsvmcloud[.]com'.

Opdateringsmetoden er ansvarlig for at initialisere de kryptografiske hjælpeprocessorer for at generere random C2-subdomains.

Disse subdomæner er sammensat af en af følgende for at generere hostnamet der skal resolves:
.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

Procesnavn, servicenavn og driversti anskaffes og hver værdi bliver hashet via FNV-1A + XOR-algoritmen og tjekket op imod hardcoded blokeringslister. Herefter stopper den de services malwaren ikke vil køre.

Hvis alle blokerings- og connectivitychecks er OK, begynder malwaren at generere domæner i et while-loop via dens DGA.

Malwaren har et random delay til genereringen af domæner, i intervallet 1 – 3 minutter, 30 – 120 minutter eller hvis der sker en fejl 420 – 540 minutter (9 timer).

DNS A-recorden af genererede domæner er tjekket op imod en liste af hardcoded IP-adresser (blokke), der kontrollerer malwarens opførsel. IP-adresse blokke i nedenstående ranges vil terminere malwaren og opdatere konfigurationsnøglen ReportWatcherRetry til en værdi der stopper yderligere eksekvering:

- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16
- 224.0.0.0/3
- fc00:: - fe00::
- fec0:: - ffc0::
- ff00:: - ff00::
- 20.140.0.0/15
- 96.31.172.0/24
- 131.228.12.0/22
- 144.86.226.0/24

Når et domæne succesfuldt er blevet fundet i et CNAME DNS-svar, vil malwaren lave en ny tråd, hvor den eksekverer HttpHelper.Initialize som står for alt C2-kommunikation og forsendelser af data.

HTTP tråden vil maksimalt lave 1 request per minut.

Malwaren bruger HTTP GET eller HEAD requests, når der forespørges data, og HTTP PUT og HTTP POST requests, når data skal sendes.

HTTP PUT metoden bruges når payloadet er mindre end 10.000 bytes; ellers bliver POST metoden brugt. 'If-None-Match' HTTP header indeholder en XOR-encoded præsentation af userID, med en vilkårlig liste af bytes tilføjet af samme længde.

Et JSON-payload er tilstede for alle HTTP POST og PUT requests der indeholder "userId", "sessionId", og "steps" (liste af objekter med følgende keys: "Timestamp", "Index", "EventType", "EventName", "DurationMs", "Succeeded", og "Message".

JSON-keyen "EventType" er en hardcoded værdi.

"Orion" og "EventName" er hardcoded til "EventManager".

Malwarens svar til C2-serveren er DEFLATE-komprimeret og single-byte-XOR encoded og derefter splittet mellem "Message" felter i "steps" array.

Hver "Message"-værdi er Base64-encoded separat.

Kommandoer er extracted fra HTTP response bodies ved at søge efter HEX strenge ved brug af følgende RegEx: "\{[0-9a-f-]{36}\}"|"[0-9a-f]{32}"|"[0-9a-f]{16}".

Kommandodata er spredt mellem flere strenge der ligner GUID og HEX-strenge.

Alle matchende substrenge i svaret er filtreret for non-HEX-karakterer, joined, og HEX-decoded.

Kommandoer er derefter tilføjet til JobExecutionEngine baseret på kommandoværdien:

Command	**Value**	**Operation**
Idle	0	No operation
Exit	1	Terminate the current thread.
SetTime	2	Sets the delay time between main event loop executions Delay is in seconds, and varies random between [.9 * <delay>, 1.1 * <delay>]. If the delay is < 300 it is doubled on the next execution through the loop, this means it should settle onto an interval of around [5, 10] minutes. There is a second, unrelated delay routine that delays for a random interval between [16hrs, 83hrs]
CollectSystemDescription	3	Profile the local system including hostname, username, OS version, MAC addresses, IP address, DHCP configuration, and domain information.
UploadSystemDescription	4	Perform a HTTP request to the specified URL, parse the results and compare components against unknown hashed values. Format a report and send to the C2 server.
RunTask	5	Starts a new process with the given file path and arguments

GetProcessByDescription	6	Returns a process listing. If no arguments are provided returns just the PID and process name. If an argument is provided it also returns the parent PID and username and domain for the process owner.
KillTask	7	Terminate the given process, by PID.
GetFileSystemEntries	8	Given a path and an optional match pattern recursively list files and directories
WriteFile	9	Given a file path and a Base64 encoded string write the contents of the Base64 decoded string to the given file path. Write using append mode. Delay for [1s, 2s] after writing is done.
FileExists	10	Tests whether the given file path exists.
DeleteFile	11	Deletes the specified file path.
GetFileHash	12	Compute the MD5 of a file at a given path and return result as a HEX string. If an argument is provided, it is the expected MD5 hash of the file and returns an error if the calculated MD5 differs.
ReadRegistryValue	13	Arbitrary registry read from one of the supported hives
SetRegistryValue	14	Arbitrary registry write from one of the supported hives.
DeleteRegistryValue	15	Arbitrary registry delete from one of the supported hives
GetRegistrySubKeyAndValueNames	16	Returns listing of subkeys and value names beneath the given registry path
Reboot	17	Attempts to immediately trigger a system reboot.

Kontakt
Hvis du har spørgsmål, er du velkommen til at kontakte Center for Cybersikkerhed på telefon 33 32 55 80 eller på mail cert@cert.cfcs.dk.

Om Center for Cybersikkerhed
Center for Cybersikkerhed under Forsvarets Efterretningstjeneste har som hovedopgave at under-støtte et højt informationssikkerhedsniveau i den informations- og kommunikationsteknologiske infrastruktur, som samfundsvigtige funktioner er afhængige af.

Denne opgave løses blandt andet ved, at Center for Cybersikkerheds Netsikkerhedstjeneste opdager, analyserer og bidrager til at imødegå avancerede cyberangreb mod myndigheder og virksomheder, der er beskæftiget med samfundsvigtige funktioner.

Om TLP-markeringen
Dette dokument er markeret med Traffic Light Protocol (TLP), som er defineret af den internationale it-sikkerhedsorganisation FIRST. Denne markering fortæller dig som modtager, hvordan eller hvorvidt indholdet af dokumentet kan deles ud fra, hvor følsomme informationerne er.

Det er alene Center for Cybersikkerhed som afsender, der kan afgøre dette efter en konkret vurdering af, hvor stor skade en offentliggørelse af informationerne ville medføre. Derfor er det vigtigt, at du som modtager forstår og respekterer den TLP-markering, som vi har angivet.

Definitioner af TLP
TLP-skalaen er opdelt i fire niveauer, som både i navn og farvekode indikerer, hvor følsomme informationerne er, og hvordan de må anvendes af dig som modtager. Det er vigtigt at understrege, at restriktionerne for deling både gælder det markerede dokument samt anden mundtlig og skriftlig omtale af indholdet. Niveauerne er defineret herunder:

TLP:RED = må ikke deles med andre, udelukkende forbeholdt modtager(e).
TLP:RED vælges, når afsender vurderer, at informationen ikke har relevans for andre end de udvalgte modtagere, og at et muligt misbrug af informationerne kan påvirke en parts privatlivspolitik, omdømme eller operationer. Modtagere må ikke dele oplysninger markeret med TLP:RED med andre uden for kredsen af specifikke modtagere eller med andre uden for mødet eller samtalen, hvori oplysningerne oprindeligt blev delt. I forbindelse med eksempelvis afholdte møder må oplysninger markeret med TLP kun deles med mødedeltagerne. I de fleste tilfælde bør TLP:RED deles mundligt eller personligt.

TLP:AMBER = begrænset deling, kan deles internt i egne organisationer.
TLP:AMBER vælges, når afsender vurderer, at modtager er nødt til at involvere andre for at kunne reagere hensigtsmæssigt på indholdet, selv om det muligvis vil kunne påvirke privatlivspolitikker, omdømme og operationer, hvis det deles bredt med andre end de involverede organisationer. Modtagere må kun dele oplysninger markeret med TLP:AMBER med organisationsmedlemmer eller med kunder eller klienter, der er nødt til at kende indholdet for at kunne beskytte sig selv eller forhindre yderligere skade. **Afsender kan frit fastsætte yderligere begrænsninger på de oplysninger, der må deles. Disse begrænsninger skal overholdes.**

TLP:GREEN = begrænset deling, kan deles med andre inden for egen sektor og branche.
TLP-GREEN vælges, når afsender vurderer, at informationen har relevans i forhold til kendskabet om et område, der vedrører egne organisationer såvel som samarbejdspartnere inden for branchen eller sektoren. Modtager må dele oplysninger markeret med TLP:GREEN med egne organisationer og samarbejdspartnere inden for egen sektor eller branche, men ikke gennem offentligt tilgængelige kommunikationskanaler. Information i denne kategori kan deles bredt inden for en

bestemt branche. TLP:GREEN må ikke deles uden for branchen/egen sektor.

TLP:WHITE = ingen begrænsninger på deling.
TLP:WHITE kan vælges, når afsender vurderer, at der er minimal eller ingen risiko for misbrug af informationerne i henhold til gældende regler og procedurer for offentliggørelse. Informationer markeret med TLP:WHITE kan frit distribueres, hvis de er i overensstemmelse med reglerne for ophavsret.

Kilde: https://www.first.org/tlp