CENTER FOR CYBERSIKKERHED

Undersøgelsesrapport

SolarWinds: Statsstøttet globalt software supply chain-angreb

Historien bag et af de største supply chain-angreb nogensinde.

1. udgave oktober 2021

Indhold

CENTER FOR CYBERSIKKERHED

Kastellet 30
2100 København Ø
Telefon: + 45 3332 5580
E-mail: cfcs@cfcs.dk

1. udgave oktober 2021.

Formål

Denne undersøgelsesrapport beskriver, hvordan en statsstøttet hackergruppe udførte et globalt software supply chain-angreb via it-virksomheden SolarWinds. Sagen illustrerer, hvordan hackere kan bruge en leverandør til at kompromittere mange ellers velbeskyttede ofre på én gang. Målgruppen for denne rapport er både it-sikkerhedsorganisationen, it-ledelse, it-teknikere og organisationens ledelse generelt.

Resumé

- I marts 2020 gemte hackere en specialudviklet bagdør i det udbredte it-managementsystem Orion fra virksomheden SolarWinds. Bagdøren blev ifølge SolarWinds distribueret via inficerede softwareopdateringer til op mod 18.000 organisationer verden over. Angrebet er et af de mest omfangsrige supply chain-angreb nogensinde.
- CFCS vurderer, at hackerne kun udnyttede bagdøren mod de mest interessante mål blandt ofrene. Disse angreb gruppen til gengæld med specialkonstrueret malware og avancerede angrebsmetoder.
- CFCS vurderer, at hackerne primært udnyttede bagdørene hos centrale amerikanske myndigheder og virksomheder.
- Mere end 50 danske organisationer modtog bagdøren. CFCS har løbende bistået berørte organisationer med rådgivning og teknisk analyse.
- CFCS vurderer, at angrebet blev udført af statsstøttede hackere med henblik på at udføre cyberspionage.
- Amerikanske myndigheder har offentligt anklaget Rusland for at stå bag angrebet.
- SolarWinds-angrebet har vist, at der fortsat er et stort behov for at hæve det generelle cybersikkerhedsniveau i Danmark.
- Særligt tre områder kunne have styrket Danmarks digitale forsvar. CFCS anbefaler, at organisationer fremadrettet særligt (1) implementerer god logning, (2) har og øver en beredskabsplan og (3) styrker kontrollen med leverandørforhold for at sikre overblikket over sin it-infrastruktur.

Indledning

Mens Corona-pandemien lukkede verden ned i foråret 2020, blev et cyberangreb i global skala ubemærket iværksat. Konsekvenserne begyndte først at blive synlige i december 2020, da verden opdagede, at virksomheden SolarWinds var blevet hacket. Undersøgelsesrapporten går i dybden med angrebet, der er et af de hidtil alvorligste supply chain-angreb nogensinde. SolarWinds blev udnyttet til at kompromittere tusinder af SolarWinds' kunder verden over. Angrebet påvirkede særligt amerikanske myndigheder og virksomheder, men også danske organisationer blev ramt. Det er et angreb, som alle der arbejder med it-sikkerhed, bør kende til, da det belyser de udfordringer, leverandørforhold skaber for it-sikkerheden hos de fleste organisationer.

Rapporten består af tre dele. Første del handler om, hvordan hackerne udførte software supply chain-angrebet via SolarWinds, og hvad hackerne udnyttede deres adgange til. Andel del beskriver, hvordan angrebet påvirkede Danmark. I den sidste del præsenterer CFCS tre tiltag, som danske organisationer med fordel kan arbejde på fremadrettet for at styrke deres cyberforsvar mod lignende angreb.

Software supply chain-angrebet mod SolarWinds

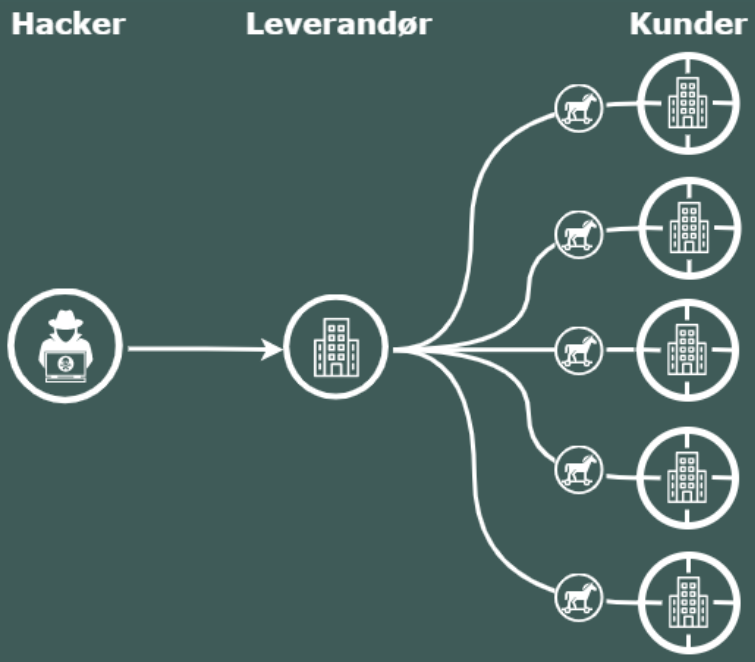
I begyndelsen af december 2020 meddelte it-sikkerhedsvirksomheden FireEye, at de havde været udsat for et sofistikeret hackerangreb. Hackerne havde bl.a. stjålet FireEyes pen-test værktøjer, som virksomheden bruger til at teste it-sikkerheden hos deres kunder.

Få dage senere stod det klart, at FireEye ikke var de eneste, der var ramt. FireEye var sammen med tusinder af andre organisationer blevet kompromitteret via en skjult bagdør gemt i inficerede opdateringer til Orion-softwaren udviklet af SolarWinds.

Ifølge SolarWinds havde op mod 18.000 af deres kunder verden over downloadet bagdøren via Orion-opdateringer udgivet mellem marts og juni 2020. Det stod hurtigt klart, at en hackergruppe havde angrebet SolarWinds for at bruge dem som trædesten ind i flere centrale - primært amerikanske - myndigheder og virksomheder.

Supply chain-angreb
Et supply chain-angreb er kendetegnet ved kompromittering via en leverandør eller betroede samarbejdspartnere.

Et software supply chain-angreb er en særlig type supply chain-angreb, hvor aktører gemmer malware i software-opdateringer, som en leverandør distribuerer til sine kunder. Hackere har tidligere brugt denne teknik, f.eks. ved NotPetya-angrebet i 2017, der bl.a. ramte Mærsk.



Figur 1: Illustration af et software supply chain-angreb

SolarWinds' software var den perfekte vej ind til attraktive mål
Statsstøttede hackergrupper forsøger aktivt og vedholdende at kompromittere vestlige myndigheder og virksomheder. SolarWinds blev sandsynligvis et middel til det mål af to hovedårsager.

For det første havde hackerne set, at SolarWinds' it-værktøjer blev benyttet af mange højtprofilerede organisationer. SolarWinds' Orion software bliver typisk brugt til at drive og supportere store komplekse netværk. Det er ofte store organisationer, der har brug for den type af værktøjer. SolarWinds havde desuden en oversigt over deres kunder på deres hjemmeside. Her stod bl.a., at SolarWinds havde mere end 300.000 kunder globalt, heriblandt det amerikanske forsvar, centrale amerikanske myndigheder og 425 af US Fortune 500 virksomhederne. Den type organisationer bliver ofte angrebet af statsstøttede hackergrupper.

SolarWinds' Customers

SolarWinds' comprehensive products and services are used by more than 300,000 customers worldwide, including military, Fortune 500 companies, government agencies, and education institutions. Our customer list includes:

- More than 425 of the US Fortune 500
- All ten of the top ten US telecommunications companies
- All five branches of the US Military
- The US Pentagon, State Department, NASA, NSA, Postal Service, NOAA, Department of Justice, and the Office of the President of the United States
- All five of the top five US accounting firms
- Hundreds of universities and colleges worldwide

Partial customer listing:

Acxiom	General Dynamics	Sabre
Ameritrade	Gillette Deutschland GmbH	Saks
AT&T	GTE	San Francisco Intl. Airport
Bellsouth Telecommunications	H&R Block	Siemens
Best Western Intl.	Harvard University	Smart City Networks
Blue Cross Blue Shield	Hertz Corporation	Smith Barney
Booz Allen Hamilton	ING Direct	Smithsonian Institute
Boston Consulting	IntelSat	Sparkasse Hagen
Cable & Wireless	J.D. Byrider	Sprint
Cablecom Media AG	Johns Hopkins University	St. John's University
Cablevision	Kennedy Space Center	Staples
CBS	Kodak	Subaru
Charter Communications	Korea Telecom	Supervalu
Cisco	Leggett and Platt	Swisscom AG
CitiFinancial	Level 3 Communications	Symantec
City of Nashville	Liz Claiborne	Telecom Italia
City of Tampa	Lockheed Martin	Telenor
Clemson University	Lucent	Texaco
Comcast Cable	MasterCard	The CDC
Credit Suisse	McDonald's Restaurants	The Economist
Dow Chemical	Microsoft	Time Warner Cable
EMC Corporation	National Park Service	U.S. Air Force
Ericsson	NCR	University of Alaska
Ernst and Young	NEC	University of Kansas
Faurecia	Nestle	University of Oklahoma
Federal Express	New York Power Authority	US Dept. Of Defense
Federal Reserve Bank	New York Times	US Postal Service

Figur 2: Udsnit af SolarWinds' kundeliste fra deres hjemmeside før angrebet.

For det andet bliver Orion-softwaren ofte konfigureret med omfattende administrative rettigheder, fordi den skal kunne styre it-infrastruktur på tværs af netværk. Høje

privilegier gør det lettere for hackere at udnytte deres indledende adgang til eksempelvis at bevæge sig videre i systemerne.

Kombinationen af en liste med mange interessante kunder, og en software ofte konfigureret med omfattende rettigheder på netværket, gjorde SolarWinds til et attraktivt mål for de statsstøttede hackere.

Hackerne var i SolarWinds' systemer i måneder, før de angreb kunderne

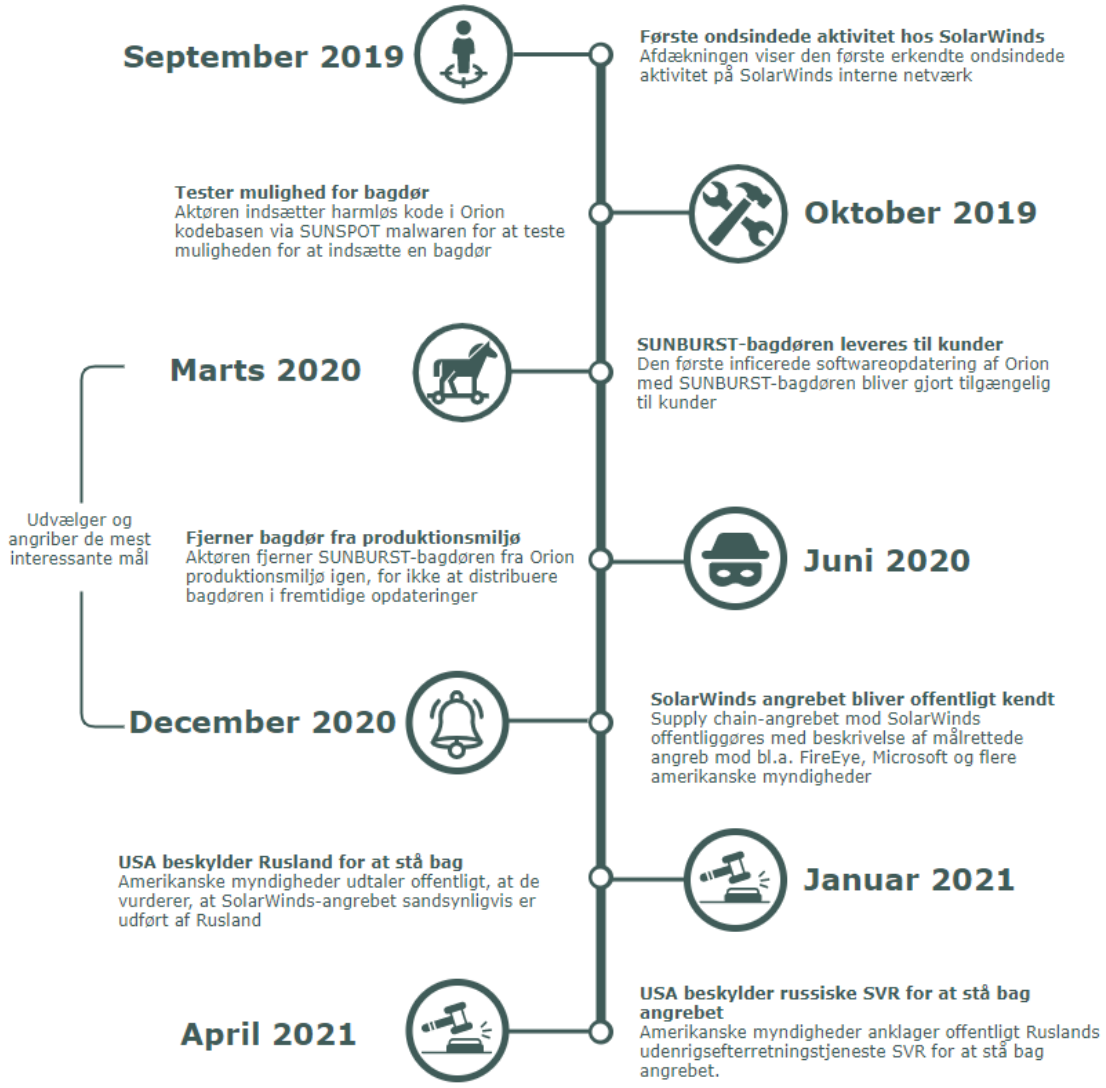
Det er fortsat uklart præcist, hvordan SolarWinds blev kompromitteret. Ifølge SolarWinds' egne undersøgelser havde hackerne haft adgang til deres interne netværk mindst siden september 2019. Under angrebet tog hackerne bl.a. kontrol over SolarWinds' softwareproduktionsmiljø for at placere en bagdør i deres software. Til det brugte de en hidtil ukendt malware ved navn SUNSPOT.

SUNSPOT gav hackerne mulighed for at følge softwareudviklingen af Orion. Når SolarWinds' softwareudviklere omdannede kildekoden til det færdige softwareprodukt, erstattede SUNSPOT én bestemt fil med hackernes egen kopi, hvori de kunne tilføje ekstra kode. På den måde tog hackerne kontrol over SolarWinds' softwareudvikling af Orion, og fik mulighed for at indlejre en bagdør. SUNSPOT havde desuden indbygget adskillige funktioner for ikke at vække opsigt.

SUNSPOT fulgte mere specifikt softwareudviklingen hos SolarWinds ved at holde øje med brugen af Microsoft Visual Studio, som mange virksomheder bruger til at udvikle software. Selvom SUNSPOT var konfigureret til specifikt at identificere udviklingen af Orion, ville det være muligt for hackerne også at rette den mod udviklingen af anden software.

Ifølge SolarWinds testede hackerne SUNSPOT i løbet af oktober 2019, før de for alvor satte gang i den verdensomspændende kampagne. Her tilføjede de først ubetydelig kode til Orion-kodebasen for at se, om tilføjelsen ville gå ubemærket hen, og nå helt ud til kunderne. Testen var succesfuld. Hackerne kunne konstatere, at en opdatering med hackernes tilføjelse af harmløs kode blev gjort tilgængelig for Solarwinds' kunder, uden at det blev opdaget.

I de følgende måneder arbejdede hackerne på udviklingen af selve bagdøren. Her studerede de bl.a. Orions interne protokol, så de kunne designe bagdøren til at efterligne legitim Orion-trafik. Det kræver betydelige ressourcer og tekniske færdigheder at udvikle og tilpasse en sådan type bagdør. Hackerne endte med den sofistikerede og skræddersyede bagdør, nu kendt som SUNBURST.



Figur 3: De vigtigste overordnede begivenheder i SolarWinds supply chain-angrebet.

SUNBURST: En særdeles godt skjult bagdør

SUNBURST var designet til at etablere skjult adgang til nogle af de mest sikkerhedsbevidste organisationer i verden. Den havde derfor indbygget adskillige tiltag for ikke at blive opdaget og anvendte en unik domænegenereringsalgoritme til at kommunikere tilbage til hackerne. SUNBURST er særligt kendetegnet ved at:

- Den lå i dvale mellem 12 og 14 dage, før den etablerede sin indledende kommando og kontrol (C2) kommunikation.
- Den ledte efter tilstedeværelsen af en række antivirus- og forensicsværktøjer.
- Den var designet til at undgå specifikke organisationer.
- Den efterlignede legitim Orion trafik.
- Den anvendte en unik domænegenereringsalgoritme i sin indledende C2 kommunikation, som hackerne bl.a. brugte til at identificere og målrette deres angreb med.

SUNBURST blev distribueret til SolarWinds' kunder via flere softwareopdateringer af Orion mellem marts og juni 2020. Den første inficerede opdatering blev digitalt underskrevet 24. marts 2020, og gjort tilgængelig for SolarWinds' kunder 26. marts. Herefter begyndte tusindvis af virksomheder og myndigheder verden over at hente inficerede opdateringer uvidende om, at de havde fået en skjult bagdør med i overførslen. I starten af april 2020 begyndte de første SUNBURST-bagdøre at kommunikere tilbage til hackerne efter at have ligget i dvale i små to uger.

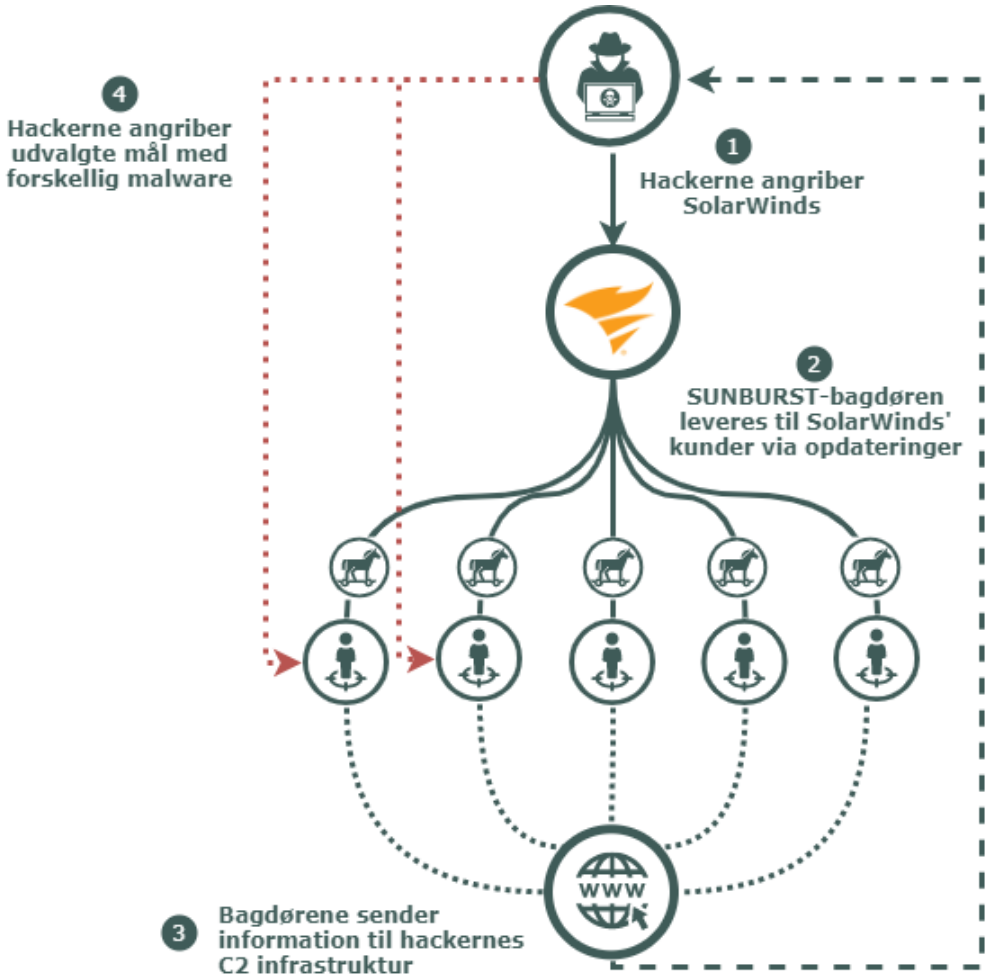
Denne indledende kommunikation skete via den unikke domænegenereringsalgoritme. Algoritmen var udformet til at ligne legitim trafik, men kommunikationen var i virkeligheden skjulte beskeder til hackerne. Beskederne informerede bl.a. hackerne om, hvilke organisationer der havde downloadet bagdøren.

Ud fra den information kunne hackerne sortere i ofrene og sætte SUNBURST i en ny og aktiv tilstand hos udvalgte mål via et nyt lag C2 infrastruktur. Hackerne enten deaktiverede eller efterlod bagdøren i dvale hos resten. Mellem marts og december 2020 angreb aktøren udvalgte mål med skræddersyede operationer via SUNBURST-bagdøren.

CFCS vurderer, at hackerne kun nåede at udnytte bagdøren mod få af SUNBURST-ofrene. Kun en brøkdel af de op mod 18.000 kompromitterede organisationer blev udvalgt til dybere, målrettede angreb. Dem planlagde gruppen imidlertid at angribe med et betydeligt arsenal af specialkonstrueret malware og skræddersyede operationer. Blandt andre Microsoft og flere amerikanske centrale myndigheder har offentligt meldt ud, at de blev udsat for yderligere angreb.

Digital signatur
Softwareudviklere beskytter deres software gennem digitale signaturer. En signatur bekræfter udviklerens identitet og garanterer, at koden ikke er blevet ændret eller ødelagt, efter den blev underskrevet.

Hos SolarWinds indlejrede hackerne imidlertid bagdøren lige inden softwaren blev digitalt underskrevet. På den måde formåede hackerne at indlejre bagdøren i opdateringer med legitime digitale underskrifter.



Figur 4: Angrebsforløbet i SolarWinds software supply chain-angrebet.

Virksomheder aktiverede kill-switch mod SUNBURST
I et koordineret samarbejde mellem flere private it-virksomheder overtog Microsoft 15. december 2020 det primære ondsindede domæne, som SUNBURST forsøgte at kommunikere til.

Indsatsen forhindrer potentielle fremtidige aktiveringer af SUNBURST, men hjælper dog ikke i de tilfælde, hvor hackerne nåede at igangsætte målrettede angreb.

Udvalgte organisationer blev udsat for skræddersyede angreb via SUNBURST
Flere amerikanske virksomheder har offentligt berettet om, hvordan hackergruppen udførte målrettede angreb mod dem via SUNBURST-bagdøren.

FireEye har eksempelvis beskrevet, hvordan hackerne anvendte SUNBURST til at levere en specialkonstrueret loader. Loaderen ved navn TEARDROP hentede en specialkonfigureret version af det bredt tilgængelige pentest-værktøj COBALT STRIKE. Herefter ledte hackerne særligt efter information om firmaets kunder og stjal FireEye's

egenudviklede pentest-værktøjer. En loader er malware designet til at hente og installere yderligere malware.

Pentest-værktøjer
Cybersikkerhedsfirmaer bruger pentest-værktøjer til at efterligne avancerede hackerangreb mod deres kunder under kontrollerede forhold. På den måde kan organisationer prøve kræfter med avancerede hackerangreb for at teste deres cybersikkerhed og indrette deres forsvar efter erfaringerne. En ondsindet hackergruppe kan omvendt bruge samme værktøjer til angribe ofre direkte med pentest-værktøjerne i rigtige angreb. Ofte er det ikke andet end hensigten, der adskiller pentestere fra ondsindede hackere.

Hos Microsoft udnyttede hackerne SUNBURST-bagdøren til at tilgå kodebasen til flere af Microsofts produkter via en intern konto. Ifølge Microsoft afhænger sikkerheden af deres produkter dog ikke af fortroligheden af deres kodebase, hvorfor effekten af hackernes indsigt skulle være begrænset. Indsigt i kildekoder kan ellers traditionelt hjælpe hackergrupper med at identificere sårbarheder i produkterne, som de senere kan udnytte. Microsoft har konkluderet, at angrebet mod dem ikke har påvirket deres kunder.

CFCS vurderer, at aktøren bag angrebet har kapacitet til at planlægge og udføre sofistikerede, målrettede og langsigtede operationer. Det er sandsynligt, at aktøren havde kapacitet til at udføre andre angreb sideløbende med det meget omfattende supply chain-angreb gennem SolarWinds.

Malware fundet på SolarWinds' servere tilknyttet anden aktør
I FireEyes første offentliggørelse af supply chain-angrebet var der informationer relateret til en webshell ved navn SUPERNOVA. CFCS vurderer imidlertid, at SUPERNOVA er en del af en uafhængig sideløbende kampagne mod SolarWinds' servere udført af en anden trusselsaktør uden relation til SolarWinds supply chain-angrebet. Det understreger blot, at SolarWinds har udgjort et interessant mål.

SolarWinds-angrebet i Danmark

SolarWinds-angrebet har også berørt Danmark. CFCS har siden december 2020 undersøgt angrebet fra et dansk perspektiv. I samarbejde med nationale, internationale og private partnere har CFCS arbejdet på at identificere og udbedre konsekvenserne af angrebet hos danske ofre. CFCS har bl.a. på baggrund af CFCS' sensornetværk, åbne kilder og oplysninger fra samarbejdspartnere løbende varslet og samarbejdet med de danske berørte organisationer.

På baggrund af de indledende analyser identificerede CFCS mere end 150 potentielle ofre, som CFCS kontaktede og varslede. Derudover delte CFCS information med organisationer, der var tilsluttet sensornetværket og de Decentrale Cyber- og Informationssikkerhedsenheder (DCIS). CFCS publicerede også rådgivning og vejledninger via cfcs.dk og sociale medier.

Efter at sagen blev offentligt kendt, blev der løbende offentliggjort flere tekniske indikatorer, de såkaldte indicators of compromise (IOC'er), som kunne bruges i undersøgelserne af angrebet. Mange private it-sikkerhedsfirmaer bidrog også til den globale indsats for at komme til bunds i angrebets omfang.

Når SUNBURST-bagdøren var blevet installeret hos ofrene, kommunikerede den tilbage til hackernes infrastruktur. Den kommunikation til det ondsindede domæne kunne CFCS se i sensornettet. På den måde kunne CFCS hurtigt danne sig et overblik over hvilke af de danske myndigheder og virksomheder, som var tilsluttet sensornetværket, der med stor sandsynlighed havde fået SUNBURST-bagdøren installeret.

CFCS lavede dybdegående tekniske analyser i færre end ti sager. Mange af de organisationer, som CFCS havde kontakt med omkring SolarWinds-hacket og SUNBURST-bagdøren havde meget få logs eller anden data, som kunne undersøges for ondsindet trafik eller malware. Så det var kun hos de organisationer, der enten var tilkoblet CFCS' sensornetværk eller selv havde et basalt niveau af logs fra deres systemer, hvor det var muligt for CFCS at analysere de tekniske hændelser.

I de udvalgte sager arbejdede CFCS' analytikere med at afdække potentiel videre kompromittering. Disse analyser viste, at en lille del af organisationerne sandsynligvis var blevet profileret til at være et særligt interessant mål. CFCS vurderer dog, at det er mindre sandsynligt, at hackerne havde udnyttet bagdøren til at installere yderligere malware på organisationens systemer.

CFCS havde kontakt med mange myndigheder og virksomheder i forbindelse med SolarWinds-hacket. CFCS sendte desuden et spørgeskema ud til de mere end 150 mulige ofre for at afdække angrebets omfang i Danmark. Af disse svarede lidt mindre end halvdelen af organisationerne på spørgeskemaet. Udover at det bidrog til et overblik over SolarWinds-sagen i Danmark, gav det samtidig en indikation på det generelle cybersikkerhedsniveau blandt strategisk vigtige organisationer i Danmark. SolarWinds Orion-software er et produkt, der er særlig relevant for organisationer med store komplekse netværk. Det er oftest den type af virksomheder eller myndigheder, der har en særlig vigtig rolle i det danske samfund. Derfor er det også organisationer, hvor det har store konsekvenser, hvis de blev ramt af et omfattende cyberangreb.

I den efterfølgende analyse, som CFCS lavede på baggrund af svarene fra spørgeskemaerne, blev det særligt tydeligt, at logning er et område, hvor der er et stort behov for at hæve det generelle sikkerhedsniveau i Danmark. En stor del af de organisationer, der svarede på spørgeskemaet, tilkendegav, at de ikke har selv den mest basale logning i deres systemer på plads. Bliver disse virksomheder udsat for et større cyberangreb, vil det være meget vanskeligt at undersøge angrebet og rydde op efter det, som også var tilfældet med SolarWinds-hacket.

Flere organisationer svarede ikke på CFCS' henvendelser. Derfor er det muligt, at der er kompromitterede danske organisationer, som CFCS ikke har kendskab til.

CFCS vurderer, at angrebet blev udført af en statsstøttet hackergruppe, og at angrebet primært var rettet mod amerikanske myndigheder og virksomheder med det formål at udføre spionage. CFCS vurderer, at selvom angrebet var meget alvorligt, var der begrænset skadevirkning i Danmark.

Tre indsatsområder til et bedre cyberforsvar

Software supply chain-angreb er svære at opdage, fordi de udnytter et allerede etableret samarbejde med en leverandør, der er tillid til. Dog kan en indsats på særligt tre områder medvirke til at styrke organisationens digitale forsvar. CFCS anbefaler, at organisationer fremadrettet særligt implementerer god logning, sørger for at have en opdateret og testet plan for hændelseshåndtering og styrker kontrollen med organisationens leverandører.

Hvorfor logning?
Tilbundsgående undersøgelse og analyse af en hændelse kræver gode logs. CFCS' afdækning af SolarWinds-sagen har vist, at der har været begrænset logning hos mange af de danske ofre. Det betyder, at det er svært at vurdere hændelsen, kortlægge hvordan hackeren har bevæget sig rundt i netværket og identificere, om hackeren har været i berøring med systemer og data. Manglende logs og analysemulighed gør det vanskeligt at få et overblik over det samlede omfang af hændelsen, og dermed vanskeligt at sikre at hullerne er lukket og hackernes fortsatte adgang er forhindret.

CFCS giver i vejledningen "Logning – en del af et godt cyberforsvar" gode råd til, hvor i netværket man skal logge, og hvad man skal logge for at kunne undersøge en it-sikkerheds hændelse. Når logning er implementeret, anbefaler CFCS at man løbende tester, om den er korrekt sat op og er tilstrækkelig til at undersøge en eventuel kompromittering.

Hvorfor en hændelseshåndteringsplan?
CFCS' afdækning af SolarWinds har vist, at der er stor forskel på paratheden til at håndtere hændelser hos de berørte organisationer. Nogle organisationer fulgte nedskrevne processer og procedurer, mens andre måtte improvisere. Det har i nogle tilfælde betydet spild af ressourcer, og deraf følgende forsinkelse af arbejdet med at undersøge og få stoppet hændelsen.

Alle organisationer bør have en velafprøvet hændelseshåndteringsplan, der sikrer, at hændelser håndteres på en ensartet og systematisk måde.

Jf. NIST SP800-61 bør en hændelseshåndteringsplan omfatte:

- **Forberedelse:** Sørg for at have opdateret dokumentation over it-aktiver, servere, systemer, netværk.
- **Identifikation og analyse:** Opdagelse af hændelse og muligvis indkaldelse af evt. ekstern assistance.
- **Begræns, udbedring, genopretning:** Afhængig af hændelsens omfang kan denne del være meget ressourcekrævende.
- **Erfaringsopsamling:** Sørg for at opsamle læring fra hændelsen.

CFCS anbefaler, at der foreligger aftaler med eksterne ressourcer om assistance, hvis organisationen ikke selv har kompetencerne. Opret faste kanaler for rapportering, og sørg for på forhånd at have klart definerede roller for hvem, der gør hvad. Det anbefales at teste sin hændelseshåndteringsplan jævnligt, således at uhensigtsmæssigheder identificeres og udbedres.

Hvorfor styrket leverandørkontrol?
I CFCS-vejledningen "Cybersikkerhed i leverandørforhold" gives vejledning til, hvordan styring af forholdet mellem forretningen og leverandøren kan varetages. Specielt den løbende dialog mellem forretningen og leverandøren er vigtig, når en aftale er indgået, og samarbejdet går i gang.

Der bør altid foreligge en risikovurdering. Leverandøren skal bidrage til kundens risikovurdering ved at levere risikovurderinger for de ydelser, kunden anvender. Leverandøren skal på sin side gennemføre risikovurdering for egen forretning med input fra underleverandører.

Her er det vigtigt løbende at vurdere forhold, der kan påvirke informationssikkerheden i leverancen, eksempelvis:

- Leverandørens brug af underleverandører, herunder krav til overblik.
- Leverandørens informationssikkerhed generelt, dvs. sikkerhedsforhold, der ikke direkte berører kunden, men som indikerer ændringer i leverandørens tilgang til sikkerhed.
- Leverandørens evne til at agere i tilfælde af sikkerhedshændelser.

Det er vigtigt med hurtig opfølgning på ændringer i ovennævnte forhold og afvigelser fra de aftalte krav til informationssikkerhed i overensstemmelse med aftalen.