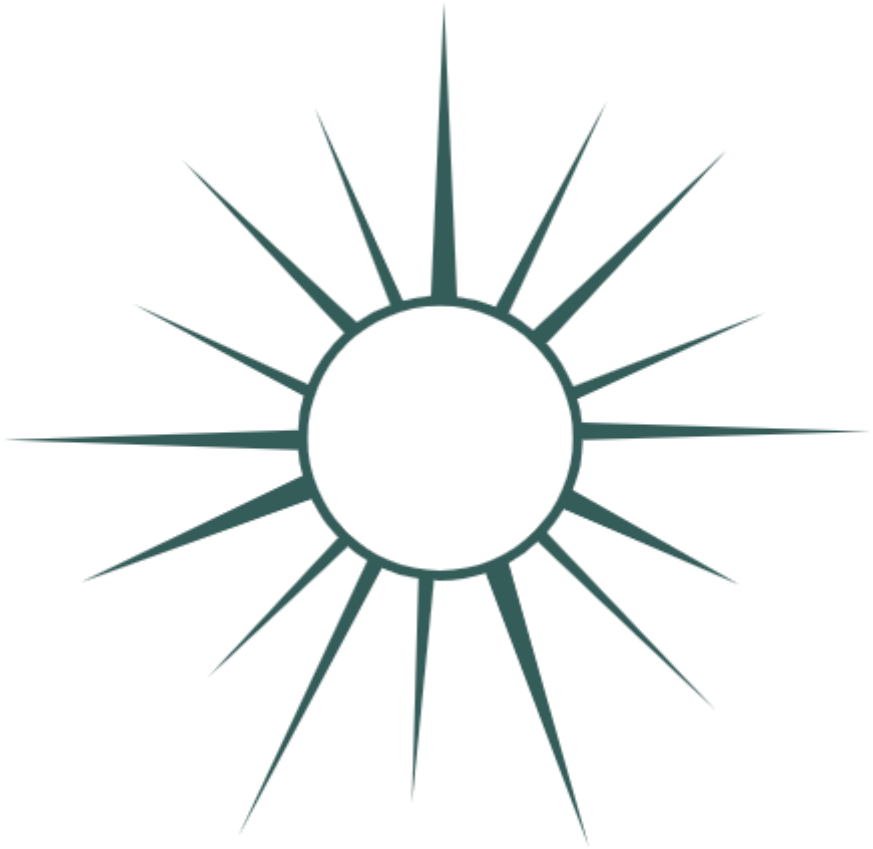
CENTRE FOR CYBER SECURITY



INVESTIGATION REPORT:

SolarWinds: State-sponsored global software supply chain attack

The story behind one of the largest supply chain attacks in history

1st edition November 2021

Table of Contents

Kastellet 30
2100 København Ø
Phone: + 45 3332 5580
Email: cfcs@cfcs.dk

1st edition November 2021

PURPOSE

This investigation report outlines how a state-sponsored hacker group conducted a global software supply chain attack via the SolarWinds software company. The incident illustrates how hackers were able to gain access to multiple victim systems through a single breach by targeting suppliers. This report is intended for IT security architects, IT executives, IT technicians and the senior management of an organization, in general.

Summary

- In March 2020, hackers infected SolarWinds's widely popular Orion IT network management system with a custom backdoor. According to SolarWinds, the backdoor was distributed via infected software updates delivered to as many as 18,000 organizations worldwide. The attack is one of the most comprehensive supply chain attacks known to date.
- The CFCS assesses that the hackers only exploited the backdoor to target high-profile victims. The hacker group then attacked these selected victims with bespoke malware and sophisticated attack techniques.
- The CFCS assesses that the hackers mainly used the backdoors against top US federal government agencies and major private companies.
- More than 50 Danish organisations were infected with the backdoor. The CFCS has continuously provided guidance and technical analysis to the compromised organizations.
- The CFCS assesses that the attack was conducted by state-sponsored hackers for the purpose of cyber espionage.
- US authorities have publicly accused Russia of being behind the attack.
- The SolarWinds attack has demonstrated that the overall cyber security level in Denmark needs to be raised.
- Three areas in particular need to be reinforced to bolster Denmark's digital defence posture. The CFCS recommends that in future, organizations specifically (1) implement proper logging solutions, (2) have contingency plans in place and regularly test these plans (3) strengthen control of supplier relationships in an effort to maintain overview of IT infrastructure.

Introduction

While the COVID-19 pandemic put most of the world into lockdown in the spring of 2020, a cyber attack of global proportions unfolded unnoticed. The effects of the attack first became apparent in December 2020, when news broke about the SolarWinds cyber breach. This investigation report aims to provide an in-depth analysis of one of the most comprehensive supply chain attacks known to date. SolarWinds was used as a springboard to compromise thousands of SolarWinds customers worldwide. The attack took down US federal government agencies and private companies, in particular, but Danish private companies were also compromised. Everyone working with IT security processes should familiarize themselves with this attack as it highlights the security risks that supply chains expose organizations to.

This report is divided into three parts: The first part describes how the SolarWinds software supply chain attack happened, and what the hackers were after. The second part outlines the impact of the attack on Danish society. In the last part of the report, the CFCS presents three protective measures to effectively strengthen Danish organizations' cyber security and defence posture.

The SolarWinds software supply chain attack

In early December 2020, the cyber security firm FireEye announced that it had fallen victim to a sophisticated hacker attack. The perpetrators had stolen, among other things, penetration testing tools that the company uses to test its customers' IT security.

A few days later it became evident that FireEye was not the only victim, and that thousands of other organizations had also been compromised via backdoor injected into SolarWinds Orion software updates.

According to SolarWinds, up to 18,000 of its customers worldwide had inadvertently downloaded the malicious Orion software update that was released between March and June 2020. It quickly became evident that a hacker group had attacked SolarWinds to gain initial foothold on the internal networks of several federal – mainly US – government agencies and private companies.

Supply chain attacks

A supply chain attack is characterized by a breach via a supplier or trusted partners.

A software supply chain attack is a particular type of supply chain attack that involves injection of malware into software updates that suppliers distribute to customers. This technique has previously been used in, for instance, the 2017 NotPetya attack against Maersk, among others.

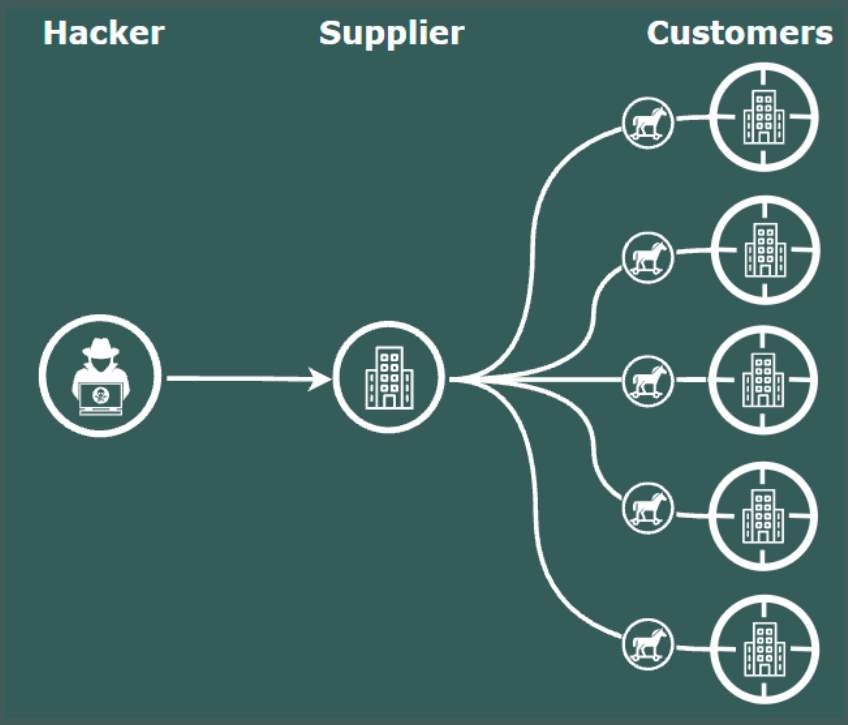


Figure 1: Illustration of a software supply chain attack

SolarWinds software was the perfect entry point into high-profile targets

State-sponsored hacker groups are actively and persistently making attempts to compromise Western authorities and companies. The SolarWinds attack was likely a means to this end for two main reasons.

Firstly, hackers had discovered that SolarWinds' IT tools were used by many high-profile organizations. SolarWinds' Orion platform is a network management software for large enterprise-class networks. Also, SolarWinds had a customer list published on its website stating that the company had more than 300,000 customers worldwide, including all branches of the US military, central US federal government agencies and 425 of the US Fortune 500 companies. Such high-profile organizations are popular targets of state-sponsored hacker groups.

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

Figure 2: A partial customer list posted on SolarWinds' website prior to the attack.

Secondly, the Orion software is often configured with extensive administrative rights as it operates IT infrastructure across networks. Extensive privileges make it easier for hackers to exploit initial entry points to move laterally into the organization networks.

The combination of a high-profile customer list and software often configured with broad network privileges made SolarWinds an attractive target to state-sponsored hackers.

Hackers were operating inside SolarWinds systems for months prior to attacking customers

It still remains unclear exactly how SolarWinds was compromised. SolarWinds' internal investigation revealed that the hackers might have had unauthorised access to the company's internal network at least since September 2019. The hackers seized control of SolarWinds' software production platform to plant a backdoor into its software update infrastructure, containing a previously unknown piece of malware named SUNSPOT.

SUNSPOT enabled the hackers to monitor the Orion software development platform. When SolarWinds' software developers converted the source code to create the finished software product, the SUNSPOT malware replaced a single file with the hackers' own copy to which they were able to add extra code. As a result, the hackers gained access to SolarWinds' Orion Platform software, allowing them to inject a backdoor. SUNSPOT had also several new built-in features to evade detection.

SUNSPOT monitored SolarWinds' Microsoft Visual Studio development tools, which are used by a range of companies to develop software. Even though SUNSPOT was configured to specifically identify the Orion Platform software, the hackers would also be able to exploit SUNSPOT to deploy attacks on other software development platforms.

According to SolarWinds, the hackers tested SUNSPOT in October 2019 ahead of their global hacking campaign. In their preliminary test, the hackers inserted an insignificant code into the Orion code base to see if the modified code could pass without being detected and subsequently be distributed to customers. The test was successful as the hackers discovered that the code modification passed undetected and the trojanized update was subsequently distributed to SolarWinds' customers.

In the following months, the hackers were working on the development of the actual backdoor, studying the internal protocol of Orion in order to design the backdoor to mimic legitimate Orion network traffic. Development and modification of this type of backdoor require significant resources and technical skills. The hackers ultimately developed the sophisticated custom backdoor now known as SUNBURST.

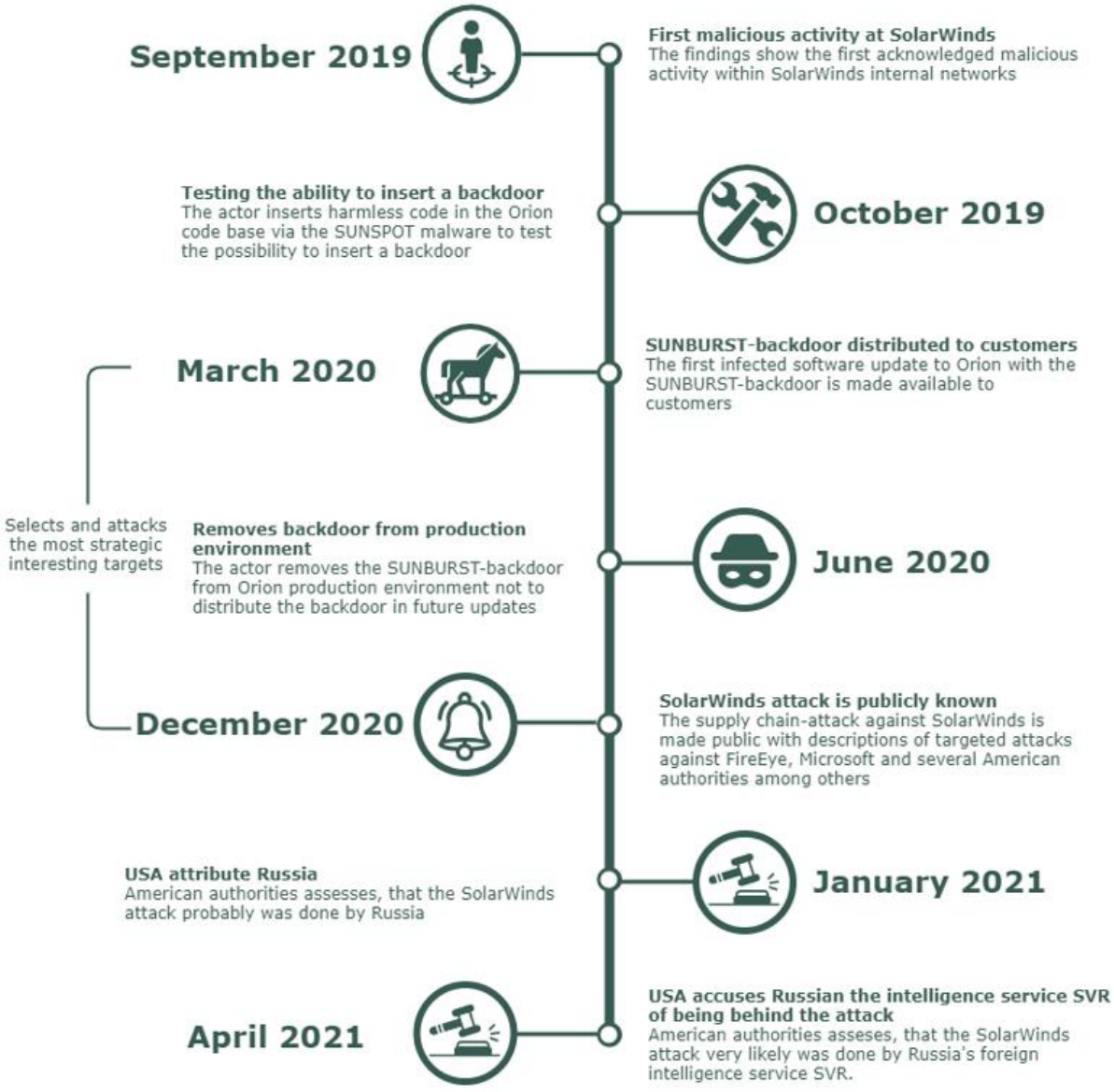


Figure 3: The main overall course of events in the SolarWinds supply chain attack.

SUNBURST: An extremely well-hidden backdoor

SUNBURST was designed to establish hidden backdoor access to some of the most security aware organizations in the world. To this end, the SUNBURST backdoor had several built-in features to avoid detection and used a unique domain generation algorithm to establish command-and-control (C2) connection to the hackers.
The unique features of SUNBURST:

- It has a dormant period of up to two weeks before operationalizing initial command and control (C2) domains
- It checks to ensure that forensic and anti-virus tools are present
- It was designed to avoid specific organizations
- It imitated legitimate Orion network traffic
- It used unique domain generation algorithm in initial C2 communication phase, which the hackers used to identify and target attacks

SUNBURST was delivered to SolarWinds customers through several trojanized Orion software updates between March and June 2020. The first infected update was digitally

signed on 24 March 2020 and distributed to SolarWinds customers on 26 March, whereupon thousands of private companies and government agencies worldwide began to download the infected software updates, unaware of the injected backdoor. In early April 2020, the first SUNBURST backdoors started to communicate with the hacker controlled servers after an initial dormant period of up to two weeks.

This initial communication was ensured via the unique domain generation algorithm. While the algorithm was designed to imitate legitimate network traffic, the actual communication contained hidden information to the hackers, such as the identity of organizations that had downloaded the backdoor.

Based on this information, the hackers were able to look through the pool of victims and reactivate SUNBURST in selected targets via a new layer of C2 infrastructure. The hackers either deactivated or left the backdoor dormant in the remaining victim systems. Between March and December 2020, the hackers used the custom SUNBURST backdoor to target specific victims.

Digital signature

Digital signatures are used by software developers to protect and secure their software entities. A digital signature validates the developer's identity and guarantees that the code has not been modified or breached after signing.

However, in the SolarWinds incident the hackers were able to inject the backdoor right before the software was digitally signed, thus enabling the hackers to deploy digitally signed backdoor malware embedded in software updates.

The CFCS assesses that the hackers only managed to use the backdoor against a few SUNBURST victims. Only a small fraction of the approx. 18,000 compromised organizations saw follow-on hacking activity. However, the selected victims were attacked with an extensive arsenal of custom malware and tailored operations. Microsoft and several US federal government agencies, among others, have revealed that they were victims of additional targeted attacks.

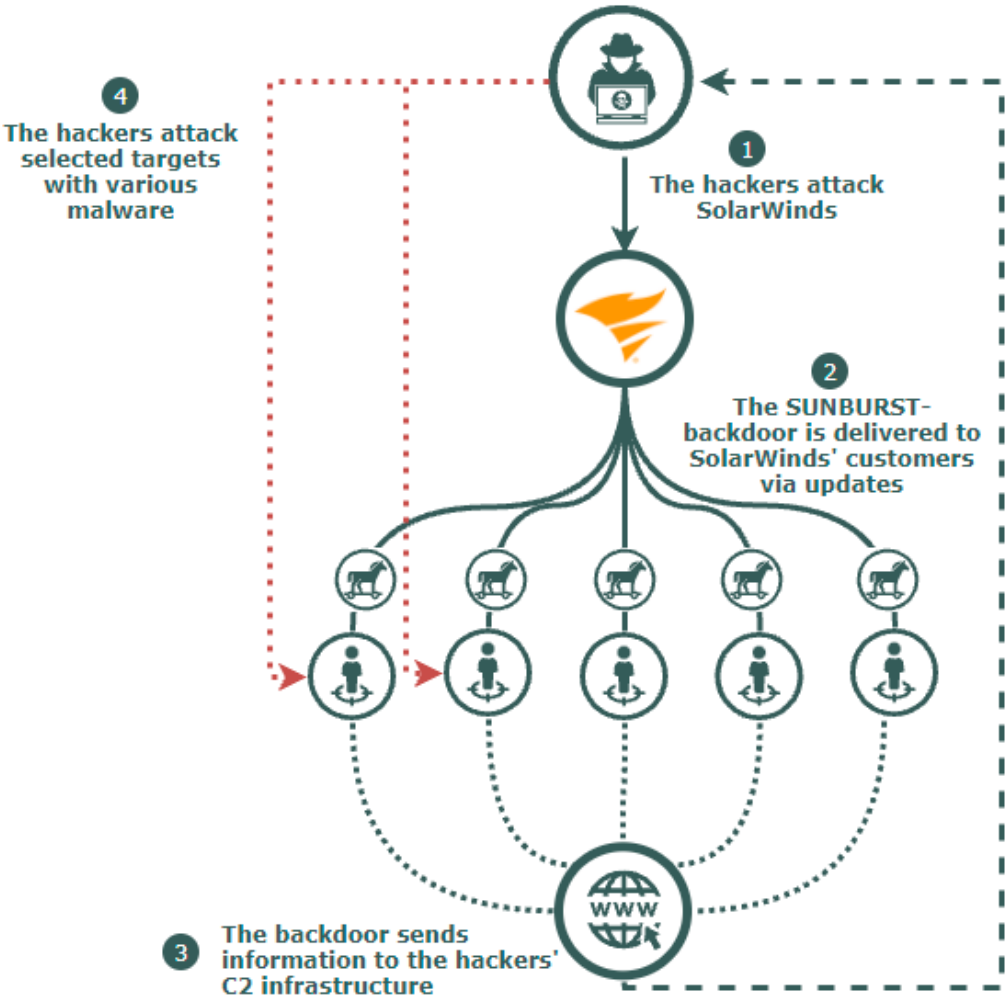


Figure 4: The progress of the SolarWinds software supply chain attack.

Private companies activated kill switch against SUNBURST
On 15 December 2020, Microsoft – together with a coalition of private IT companies – seized control of the domain which served as the command and control server for the SUNBURST malware.

The kill switch mechanism prevents potential future deployments of the SUNBURST malware but in networks where the attackers have already deployed additional persistence mechanisms, the kill switch will not remove the threat from victim networks.

Select organizations fell victim to bespoke SUNBURST attacks

Several US companies have publicly explained how the hacker group was able to open a backdoor into their network by injecting the SUNBURST malware.

For example, FireEye has described how hackers used SUNBURST to deploy a custom loader. The loader, dubbed TEARDROP, delivered a specially configured version of the widely popular penetration testing tool COBALT STRIKE, which enabled the hackers to access information on FireEye customers, in particular, and steal FireEye's proprietary penetration testing tools. A loader is a malware designed to extract and install additional malware.

Penetration testing tools
Cyber security companies employ penetration testing tools to safely stage sophisticated hacker attacks against their customers under controlled conditions. This allows organizations to perform simulated hacker attacks to test their cyber security defence and modify their defence mechanisms accordingly. However, malicious hacker groups may, in turn, use the same penetration testing tools to deploy malicious attacks instead. Often, it is only the intent that separates malicious actors from pentesters.

When the hackers gained access to Microsoft, they exploited the SUNBURST backdoor to access Microsoft source code repositories via an internal account. However, according to Microsoft, it does not rely on the secrecy of source code for the security of its product, thus limiting the effect of the hackers' insight. Knowledge of source codes would traditionally allow hacker groups to identify product vulnerabilities for subsequent potential exploitation. Microsoft concluded that its customers were unaffected by the attack.

The CFCS assesses that the hackers have the capabilities to plan and conduct sophisticated, targeted and long-term operations. The actors likely had the capability to launch simultaneous attacks while the very extensive SolarWinds supply chain attacks were in progress.

Malware detected on SolarWinds' servers linked to other actor
FireEye's first public notification of the supply chain attack included information on a web shell called SUPERNOVA. However, the CFCS assesses that SUPERNOVA is part of an independent, simultaneous campaign against SolarWinds' servers carried out by another threat actor and that this activity is unrelated to the SolarWinds supply chain attack. This second attack just highlights that SolarWinds was an attractive target.

The impact of the SolarWinds attack on Denmark

The SolarWinds attack has also affected Denmark. Since December 2020, the CFCS has investigated the impact of the attack from a Danish perspective. In cooperation with national, international and private partners, the CFCS has made efforts to identify and mitigate the impact of the attack on Danish victims. Based on the CFCS sensor network, open sources and information from cooperation partners, among others, the CFCS has continuously notified and cooperated with the affected Danish organizations.

Based on the preliminary analyses, the CFCS identified at least 150 potential victims that were contacted and notified. Also, the CFCS shared information with organizations connected to the sensor network and the Decentralised Cyber Information Security unit (DCIS). The CFCS also published guidance and guidelines on its website cfcs.dk and on social media.

When the world learned of the attack, additional technical indicators, the so-called indicators of compromise (IOC) that were useful in the investigation of the attack, were continuously made publicly available. Many private IT companies also contributed to the global efforts to understand the full scope of the attack.

Once the SUNBURST backdoor was deployed to the victim systems, it established communication with the hackers' C2 server. This traffic could be seen by the CFCS in the sensor network, thus allowing the CFCS to quickly form an overview of the Danish public authorities and private companies connected to the sensor network that had highly likely been infected with the SUNBURST backdoor.

The CFCS performed in-depth technical analyses in less than ten cases. Many of the organizations that were contacted by the CFCS in connection with the SolarWinds hack and the SUNBURST backdoor had insufficient logging or data that could be examined for malicious traffic or malware. Consequently, only the organizations that were either connected to the CFCS sensor network or had basic logging in place on their systems could be included in the CFCS technical analysis.

In the selected incidents, CFCS analysts investigated potential attempts of lateral movements. These analyses indicated that a few of the organizations had likely been identified as particularly attractive targets. However, the CFCS assesses it less likely that the hackers had exploited the backdoor to inject additional malware into the organization systems.

The CFCS was in contact with many public authorities and private companies in connection with the SolarWinds hack. In addition, in an effort to uncover the scope of the attack in Denmark, the CFCS sent a questionnaire to the 150 potential victims to which less than half of the 150 organizations replied. In addition to providing an overview of the SolarWinds incident in Denmark, it also provided an indication of the overall cyber security level of key strategic organizations in Denmark. SolarWinds Orion software is a product that is particularly relevant to organizations with complex networks, often including private companies or public authorities that are critical to the functioning of the Danish society. Consequently, when such organizations are hit by a large-scale attack, the consequences are that much more serious.

In the subsequent analysis conducted by the CFCS based on the questionnaire replies, it became particularly clear that logging is an area where the overall security level in Denmark needs to be heightened. A large share of the organizations that replied to the questionnaire revealed that they do not have even the most basic logging processes in place. Should these organizations fall victim to a large-scale cyber attack, it would prove

very difficult to investigate the incident and provide post-breach clean-up, which, in fact, was also the case with the SolarWinds hack.

Several organizations neglected to reply to CFCS' enquiries, suggesting that there may be additional compromised Danish organizations of which the CFCS is unaware.

The CFCS assesses that a state-sponsored hacker group was behind the attack and that the aim was to conduct cyber espionage mainly against US government agencies and private companies. The CFCS assesses that even though the attack was very serious, the impact on Danish society was limited.

Three approaches to cyber resilience

Software supply chain attacks are difficult to detect because they are designed to exploit trusted relationships between companies and suppliers. However, three approaches, in particular, may help contribute to enhancing the organization's cyber security posture. The CFCS recommends that organizations implement proper logging solutions in future, have a well laid-out and tested incident response plan in place and strengthen control of organization suppliers, in particular.

Why logging?
Adequate logging is a key element in in-depth incident investigation and analyses. The CFCS' investigation of the SolarWinds incident has revealed that many of the Danish victims had insufficient logging, which limits the possibilities of investigating the incident, mapping the movements of the hacker inside the network and identifying whether hackers have infected other systems and data deeper in the network. Insufficient logging and lack of analysis make it impossible to create an overview of the overall extent of the incident, which, in turn, makes it harder to patch the vulnerabilities and thus prevent hackers from continuing their malicious activities.

In the CFCS guide "Logging – part of a resilient cyber defence", the Centre provides recommendations on which networks to log, and in which systems data should be logged to ensure proper investigation of a potential IT security incident. Once logging procedures are implemented, the CFCS recommends that organizations run regular mock tests to ensure that logging solutions are properly set up and are adequate in case of a potential incident investigation.

Why the need for a cyber incident response plan?
The CFCS' investigation of SolarWinds has shown that the affected organizations have very different approaches to incident response. Some organizations followed a set of established processes and procedures while others had to improvise, which, in some instances, has caused waste of resources and thus delays in investigation and incident eradication.

Every organization should have a tried-and-tested incident response plan in place that ensures uniform and systematic incident response procedures.

An incident response plan must include, cf. NIST SP800-61:

- **Preparation:** Ensure updated documentation of IT assets, servers, systems and networks.
- **Identification and analysis:** Incident detection and potential engaging of external assistance.
- **Containment, eradication, recovery:** Depending on the scope of the incident, this part of the response plan may be very resource demanding.
- **Lessons learned:** Analyse and document everything learned from the breach.

The CFCS recommends that organizations establish mutual assistance agreements that engage outside resources in the event of a data breach, should they not retain in-house support providers. Establish permanent reporting channels and outline clearly defined roles and responsibilities. We recommend that the organization's incident response plan be regularly tested in order to identify and eradicate irregularities.

Why the need for strengthened supplier control?
The CFCS guide "Information security in supplier relationships" contains a number of pointers on how to handle relations between organizations and suppliers. A regular and consistent dialogue, in particular, between organization and supplier is essential once the parties have agreed on cooperation.

A risk assessment should always be available. The supplier should contribute to the client's risk assessment by performing risk evaluations of the services provided to the client. The supplier's task is to perform risk assessments on its own business with input from sub-suppliers.

This requires a consistent assessment of factors that may affect the delivery of information security, for example:

- The supplier's use of sub-suppliers, including oversight requirements.
- The supplier's information security procedures, in general, such as security that does not directly affect the client but indicate changes to the supplier's security procedures.
- The supplier's ability to counteract in the event of security incidents.

Quick follow-ups are essential in connection with changes to above-mentioned relations and modifications in relation to the agreed terms and conditions of information security in accordance with the agreement.

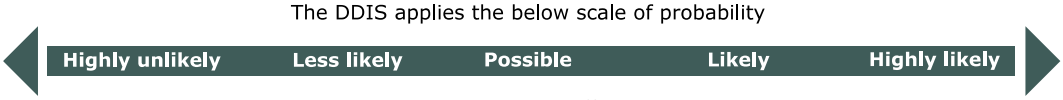
Threat levels

Definition of threat levels

The DDIS uses the following threat levels, ranging from **NONE** to **VERY HIGH**.

NONE	No indications of a threat. No acknowledged capacity or intent to carry out attacks. Attacks/harmful activities are unlikely.
LOW	A potential threat exists. Limited capacity and/or intent to carry out attacks. Attacks/harmful activities are not likely.
MEDIUM	A general threat exists. Capacity and/or intent to attack and possible planning. Attacks/harmful activities are possible.
HIGH	An acknowledged threat exists. Capacity and intent to carry out attacks and planning. Attacks/harmful activities are likely.
VERY HIGH	A specific threat exists. Capacity, intent to attack, planning and possible execution. Attacks/harmful activities are very likely.

The DDIS applies the below scale of probability



"We assess" corresponds to "likely" unless a different probability level is indicated.