CENTRE FOR CYBER SECURITY

Threat Assessment:

The cyberthreat against the Danish financial sector

1. Edition December 2020. Last updated June 2022

Table of Content

CENTRE FOR CYBER SECURITY

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

2. edition June 2022.

Centre for Cyber Security (CFCS) raises the threat level for cyber activism to HIGH for the Danish financial sector.

CFCS is raising the threat level for cyber activism against the Danish financial sector from **MEDIUM** to **HIGH**. This implies that organizations within the sector are likely to become targets of cyber activism within the next two years.

CFCS raised the overall threat level for cyber activism against Denmark on January 31st 2023. CFCS assesses that this increased threat from cyber activism also applies to the Danish financial sector.

CFCS raised the threat level based on a combination of the pro-Russian cyber activists' significant level of activity against NATO member states, including Denmark, and their more formalized modus operandi and increased capacity.

The threat assessment's core text is not updated, and the section on cyber activism does not reflect the current threat level.

For additional information on why the threat level from cyber activism is raised as well as how the threat manifests itself, please refer to the threat assesment "The CFCS raises the threat level of cyber activism against Denmark from MEDIUM to HIGH" published on January 31st 2023.

The threat assessment is available on www.cfcs.dk/en

The cyber threat against the Danish financial sector

The purpose of this threat assessment is to provide an update on the cyber threat against the Danish financial sector in order to improve its cyber resilience. This threat assessment is intended for decision-makers and risk owners in Danish authorities and institutions in the financial sector. The threat assessment replaces the August 2018 threat assessment on the Danish financial sector.

This threat assessment was updated in June 2022 with adjustments to the chapter on the threat of cyber activism following the increase in the threat level described in the CFCS assessment "CFCS hæver trusselsniveauet for cyberaktivisme" (only available in Danish) published 18 May 2022. The threat level of cyber activism has been raised from **LOW** to **MEDIUM**. The rest of the text remains unchanged.

Key assessment

- The threat from cyber crime against the Danish financial sector is **VERY HIGH**. The threat from cyber criminals is persistent, and some of their attacks may be sophisticated and extensive. Cyber crime, for instance in the form of ransomware attacks, may potentially disrupt the availability of services afforded by the Danish financial sector.

- The threat from cyber espionage is **HIGH**. Foreign states likely have political as well as financial motives for conducting cyber espionage against private companies and public authorities in the Danish financial sector.

- The threat from cyber activism against Denmark has been raised from **LOW** to **MEDIUM**. CFCS has raised the cyber threat level in response to the cyber activist attacks against European NATO countries carried out in relation to the war in Ukraine. It is possible that pro-Russian hackers, in particular, will attack targets in Denmark, including targets in the financial sector.

- The threat from destructive cyber attacks is **LOW.** Foreign states are less likely to excecute destructive cyber attacks against critical infrastructure in Denmark, including the financial sector.

- The threat of cyber terrorism is **NONE**. At present, militant extremists not only lack the technical capabilities and organizational resources required to launch serious cyber attacks causing the same destruction as conventional terrorist attacks, they also have little intent to launch such attacks.

Introduction

This threat assessment describes the overall cyber threat against the Danish financial sector. This assessment is the second general threat assessment on the Danish financial sector published by the Centre for Cyber Security (CFCS).

Cyber attacks still remain a significant and persistent threat against Danish financial sector institutes, their clients and cooperation partners. Since the public release of the 2018 threat assessment, the threat levels of cyber activism and terrorism have been lowered to **LOW** and **NONE** respectively. In addition, the CFCS has assigned a threat level for destructive cyber attacks. The threat of destructive cyber attacks is **LOW**.

Phishing is still the most common form of cyber attack. Cooperation between cyber criminals continues throughout the criminal ecosystems, and certain actors are increasingly specializing in gaining access to victims and selling this access to other criminals. A new trend has emerged in which Danish private companies are increasingly falling victim to targeted ransomware attacks. This type of attack poses a threat to many sectors, including the financial sector. The threat of digital bank robberies persists even though recent years have seen only a few publicly known attacks. State actors and criminals continue to use many of the same tools, and they are also increasingly exploiting legitimate programmes in their cyber attacks.

The financial sector supports functions vital to Danish society. Persistent and sophisticated cyber attacks against critical segments of the Danish financial infrastructure may undermine public confidence in the financial sector and, at worst, threaten financial stability and, ultimately, the Danish national economy. Thus, it is vital that companies, infrastructure and services are available, reliable and stable, allowing citizens and companies to use the services afforded by the sector while fully relying on the integrity of the systems.

The financial sector includes multi-faceted and multi-functional companies. In this assessment, the financial sector includes private companies subject to financial regulation and relevant public authorities responsible for the financial sector.

Cyber crime

The CFCS assesses that the threat of cyber crime is **VERY HIGH**. This means that it is highly likely that organisations in the financial sector will be subject to attempts at cyber crime within the next two years.

Cyber criminals use different attack techniques. Common to all attack techniques is that hackers are trying to gain unauthorized access to sensitive information or systems for financial gain.

Most cyber attacks still start with an email
Phishing is still an effective technique for attacking authorities, private companies, and citizens. Many – both small-scale and large-scale – cyber attacks begin with an employee being tricked into opening a phishing email. This is despite that fact that the majority of the phishing attacks targeting the financial sector is opportunistic and, at times, poorly performed. Hackers are capable of sending large volumes of phishing emails with little effort, raising the likelihood that an employee accidentally or inadvertently clicks on a malware-infected link or attachment.

Phishing is used for all sorts of criminal activity, but typically for:

- Theft of usernames and passwords to Internet services such as email accounts, social media, web stores, etc.
- BEC fraud in which the victim is lured into transferring money to cyber criminals.
- Installation of malware on victim computers.
- Establishing a foothold in IT networks as a stepping stone for further compromise.
- Theft of additional sensitive or protection-worthy information.
- Theft of debit card information.
- Theft of NemID passwords and codes.

Among other things, hackers use phishing and spear phishing to gain initial access to victim systems, allowing them to move through the organization network. To this end, hackers send spear phishing emails to IT employees in an attempt to gain unauthorized access to IT employees' privileges or network tools, which can then be exploited to move deeper into the organization network.

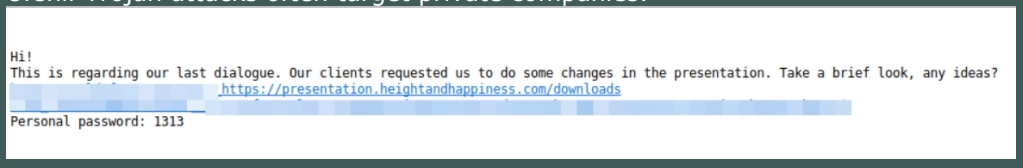
Phishing emails may also come from legitimate entities that are exploited by cyber criminals. Such phishing emails are often inserted into existing email threads between the recipient and the sender. This is also called email thread hijacking. This technique makes it difficult for the recipient to detect the phishing email as it purports to be from

a known and trusted individual or company. Hackers are capable of spreading their activities from one organization to another through this technique.

CFCS has knowledge of several incidents where Danish corporations have received emails from trusted entities whose email accounts had been hacked. For example, several Danish victims of targeted ransomware attacks were compromised via email thread hijacking.

Hackers have also used this technique against the Danish and Nordic financial sector. For example, hackers tried to spread the Ursnif malware through email hijacking. The hackers compromised an email account and sorted through the ongoing email correspondence. They then sent malware-infected email replies, making the infected emails appear to be part of an existing email thread.

Ursnif
Ursnif is a banking Trojan malware that can steal bank account information, passwords and other sensitive information from the victim. Ursnif is typically delivered to the victim in Word or Excel documents through spam campaigns. Ursnif Trojan attacks often target private companies.


Hi!
This is regarding our last dialogue. Our clients requested us to do some changes in the presentation. Take a brief look, any ideas?
https://presentation.heightandhappiness.com/downloads
Personal password: 1313

Excerpt from a phishing email with Ursnif sent to a Danish financial company. The email looks like it is part of an ongoing conversation.

Hackers also use phishing emails to commit BEC scams aimed at tricking companies or public authorities to wire funds to the hacker's accounts. The criminals often try to trick the recipients of the email into wiring the funds by impersonating in-house executives, and criminals have occasionally exploited compromised email accounts belonging to executive staff in the organization. The CFCS is not aware of any successful BEC scams targeting organizations in the Danish financial sector although attempts are regularly made.

Norfund loses approx. USD 10 million to a BEC scam
In March 2020, Norway's state investment fund, Norfund, fell victim to what was likely a BEC scam. The scammers succeeded to falsify payment information concerning a loan to a microfinance institution in Cambodia, instead directing USD 10 million to accounts in Mexico.

High frequency trader fell victim to BEC fraud
In May 2020, US company Virtu Financial lost USD 6.9 million in a BEC scam. An email account belonging to an executive employee was compromised and subsequently exploited to send fraudulent requests to the company's accounting department leading to two wire transfers to two different banks based in China.

Phishing of customers create indirect losses for financial institutions
Cyber criminals repeatedly try to phish information from financial institutions' customers, for example through fake websites. In the spring of 2020 amid the height of the COVID-19 pandemic in Denmark, cyber criminals created multiple fake websites in an effort to trick Danish victims into sharing sensitive information, including NemID (digital signature) or debit card information. Some of the fake websites are almost identical in appearance to the legitimate websites. The largest Danish banks are not the only banks imitated by cyber criminals in their phishing attempts. For example, in August 2020, Vestjysk Bank warned its customers about a fake used in an effort to trick them into submitting their NemID credentials.

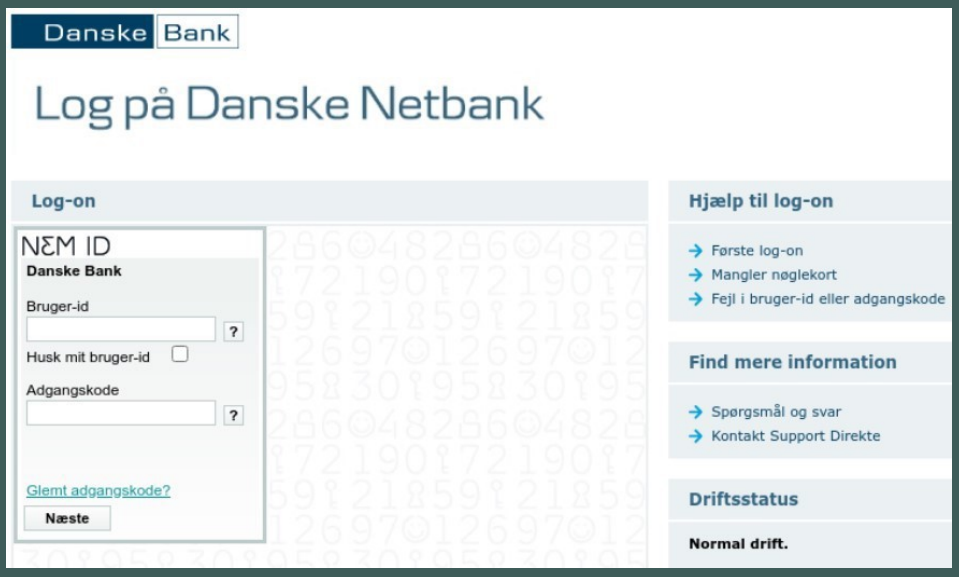
The CFCS pursues fake websites

Since 12 March 2020, the CFCS has dedicated its efforts to identify domains that are used to leverage phishing attacks targeting, amongst other things, Danish NemID and debit card information. The CFCS has developed a tool called PhishHook that monitors approx. 6.5 million domains on a daily basis. PhishHook conducts a preliminary analysis of the domains as to whether a number of select words are used in the domains such as "Bank" or "Nets". Subsequently, PhishHook conducts a more sophisticated analysis of source codes on selected websites. Analysts then carry out a manual analysis of the domains that PhishHook points out have a high risk of being used for phishing against Danish citizens.

If the analysis indicates that the aim of the domain is phishing, the CFCS will share the information with relevant parties, including the Danish National Cyber Crime Center (NC3) and the hosting provider responsible for the domain. Hosting providers may decide to shut down the domain based on the information provided by the CFCS. The NC3, in cooperation with Danish telecom providers, is capable of blocking COVID-19-related domains.

The CFCS has repeatedly detected photos of Danish NemID key cards that are uploaded to phishing sites. The CFCS informs Danish payment solution company Nets of such incidents, which then blocks the compromised NemID key cards.

Below is an example of a fake website identified by the CFCS. The website exploited the name of Danske Bank, likely in an attempt to lure Danish citizens into sharing their NemID information. The domain was activated on 10 November 2020 and on the same day the CFCS notified NC3, the Decentralized Unit for Cyber and Information Security for the Financial sector (Finance DCIS), the Danish Agency for Digitisation and the hosting provider. The domain was subsequently shut down by the hosting provider.



An example of a fake website likely aimed at stealing NEMID information

Malware infection delivered through email spam may ultimately become part of a targeted attack

If an organization is hit by an opportunistic phishing attack, it may pave the way for large-scale and more targeted cyber attacks, causing serious consequences for a financial institution.

Some cyber criminal groups have specialized in gaining unauthorized access to as many targets as possible. They sell or pass on the access to other hackers who subsequently launch more targeted cyber attacks against the already compromised organizations.

"Targeted" does not necessarily mean that the hackers select specific organizations in advance and actively target them. Rather it means that hackers review the targets they have gained initial access to and then devote their time and effort to the victims they want to compromise further. For instance, this could be companies the hackers assume will be able to pay very large ransom demands.

The Emotet malware is an example of a malware often spread through spam emails, but which may ultimately lead to a cyber attack with serious consequences. For a number of years, Emotet has been used to target the financial sector to steal bank information. However, as of recent, the malware is used as a source of income for criminals who sell or facilitate access to increasingly targeted attacks. Generally, Emotet is a very popular malware that has compromised a great many victims worldwide, including victims in Denmark.

Like many other cyber criminals, operators of Emotet constantly develop their malware and change their cooperation partners. In 2020, for instance, Emotet has increasingly been used as a payload delivery mechanism for the Qakbot malware rather than Trickbot. Qakbot can be used to install the ProLock ransomware on the victim's system.

The actors behind ProLock have demanded up to USD 660,000 in ransom, and they have destroyed victim data as the decryption key provided by the attackers did not work properly, indicating just how serious an infection with Emotet may ultimately be for a company.

The threat of targeted ransomware attacks has increased

In recent years, targeted ransomware attacks have been on the rise, and the threat from targeted ransomware attacks is also relevant for the financial sector. All kinds of companies worldwide fall victim to extensive ransomware attacks almost on a daily basis.

In targeted cyber attacks, the hackers take their time to move deeper into the systems of compromised organizations. Rather than using automated hacking tools, hackers execute targeted ransomware attacks manually. Their aim is to encrypt large or vital parts of the organization's systems with the intent to extort large amounts of money from their victims.

The CFCS does not know of any successful targeted ransomware attacks against Danish financial organizations, though attempts have been made. At least one

organization has been compromised by malware that is mainly used ahead of a targeted ransomware attack. However, the organization's in-house IT security department quickly contained the attack.

In 2020, financial sector organizations abroad have been hit by several ransomware attacks. There have also been successful ransomware attacks against foreign suppliers to Danish financial institutions. Among others, software supplier Software AG and it-service provider Sopra Steria fell victim to ransomware attacks in the fall of 2020. However, the attacks did not seem to have spread to the systems of Danish institutions. The supply chain threat is described in detail later on in this assessment.

The most recent trend in targeted ransomware attacks is that hackers also steal data from their victims for extortion purposes. Several criminal groups thus threaten to leak sensitive information unless the ransom is paid. Others try to sell the stolen data to interested buyers. For example, the ransomware operators known as Sodinokibi or REvil have created an auction site used to sell stolen data to the highest bidder.

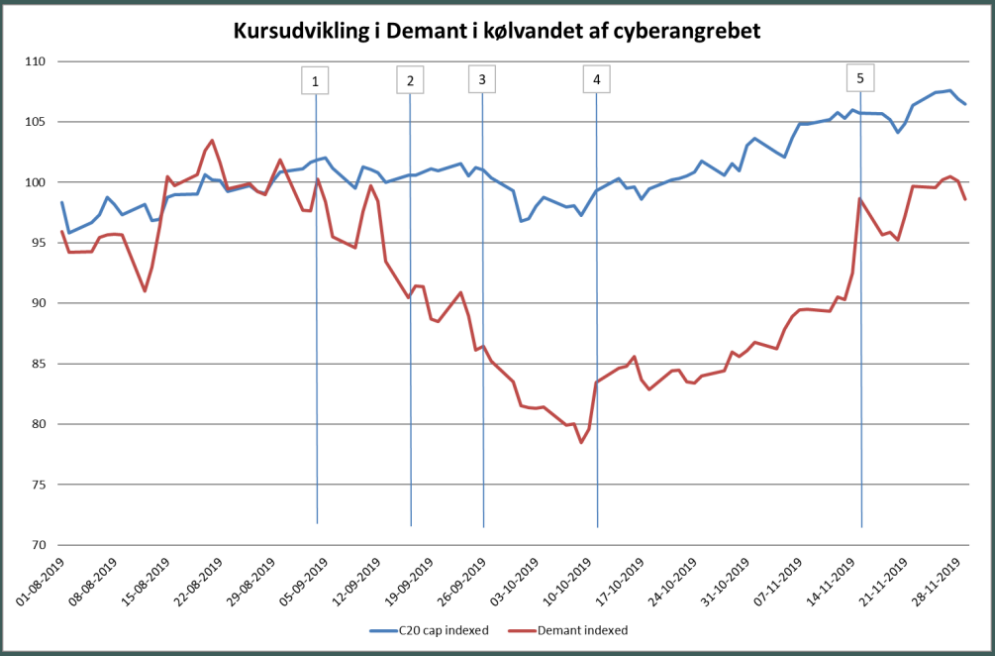
Cyber criminals are highly likely aware of the value of particularly sensitive information held by the financial sector because data leaks related to financial companies and their clients, such as the so-called FinCen files, have received a lot of media attention. Cyber criminals will likely attempt to access such information to leverage pressure on their victims.

European bank victim of data leak in a ransomware attack
Open sources report that in early 2020, the Kosovo-based bank Banka Ekonomike was compromised by the DoppelPaymer ransomware. The hackers leaked more than 70 GB data, including information on financial transactions such as client names, credit card numbers, and information on income and client loans. The leak also contained sensitive bank employee information.

The financial impact of cyber attacks on some of the targeted Danish and international companies in other sectors has been quite significant and includes downtime costs, revenue loss, recovery and uncertainty in the post-attack period. The attacks and the following damage control have also affected stock performance of listed companies, as shown by the example below.

Cyber attacks and the handling of them can affect stock market share prices

Hearing aid company Demant fell victim to a ransomware attack in September 2019. Below is a chart of the pre-and post-attack stock performances of the Demant shares (red line). In order to show how the Demant stocks performed compared to the rest of the market (blue line), it is illustrated in the context of the general Danish C20 Cap index.



Data source: Nasdaq. The development of Demant's shares can also be held up against the C25 index based on data on Nasdaq's website

1: Demant publicly discloses that the company has been hit by a cyber crime-related IT incident.
2: Demant reveals that incident severely affected its systems, but that the company was able to restore its critical IT infrastructure.
3: Demant reveals an estimated loss of up to DKK 650 million, and that the company has been able to restore most of its system to its original state.
4: Demant reveals that it has fully completed its system recovery process.
5: Demant releases a positive financial report, in which the loss related to the ransomware attack roughly aligns with previous estimates by Demant.

In the wake of the attack, the stock value dropped considerably over a period compared to the general index, possibly reflecting the markets' response to the level of uncertainty surrounding Demant prior to the company's system recovery and estimated overview of the scale of damage. Demant estimated its total loss in the range of DKK 550-650 million; though the stock lost approx. 10 billion of its overall market value in the period from the attack was publicly announced to Demant's full recovery. However, the stock gradually recovered some of its loss, and following the positive financial report in November, the stock value increased to the same pre-attack level.

The threat of digital bank robberies persists

There is a potential threat of targeted cyber attacks in the form of so-called digital bank robberies against organizations in the Danish financial sector. The CFCS assesses that state-sponsored hackers conduct this type of attack in some cases.

The CFCS is aware that hackers, who may have the capability to conduct digital bank robberies, have attacked institutions in the Danish financial sector in 2019. In one of these attacks, the hackers successfully gained initial access before the attack was detected and stopped.

One of the actors linked to digital bank robberies impersonated an employee from the Danish Financial Supervisory Authority (FSA) in phishing emails. The hackers had created domains that looked strikingly similar to the original FSA page, and they exploited real FSA employee names.

Hackers spoofed the FSA website for data submission

In May 2020, the FSA warned of a website that tried to spoof the FSA's English data submission portal for financial companies. The link was likely used in a phishing campaign.

Exploitation of financial authorities in phishing attacks are likely motivated by the fact that financial institutions often have to respond quickly to requests from authorities, increasing the likelihood that the recipient responds to phishing emails. Cyber criminal actors, for instance, often exploit the European Central Bank (ECB), in campaigns.

Lazarus has long profited from hacking

The Lazarus hacker group has long actively targeted the financial sector, among others. The group has significant capabilities to launch cyber attacks. It has conducted well-planned and sophisticated cyber attacks, most recently involving the use of fileless attack techniques. In fileless attacks, hackers do not use their own executable files, but instead exploit legitimate files already on the victim's system. For this reason, these attacks are hard to detect. Lazarus is also known for allocating considerable resources to their social engineering. Among other things, they manipulate their victims with fake job adverts and occasionally even fake job interviews.

In addition to digital bank robberies, the group has attacked cryptocurrency exchanges and crypto wallets. Lazarus may be targeting cryptocurrency because cryptocurrency is easier to launder than ordinary currency. Open sources have reported that Lazarus is now using other lucrative tactics such as targeted ransomware attacks, web skimmers and BEC scams.

Lazarus was likely behind the 2016 attack against Bangladesh Central Bank, resulting in the theft of USD 81 million. The bank subsequently managed to recover USD 15 million from a casino in the Philippines, which the hackers had used to launder a portion of the stolen money. PHOTO: Jason Arlan Raval/AP/Ritzau Scanpix

DDoS attacks may disrupt the financial sector's online services

Distributed Denial of Service attacks, so-called DDoS attacks, continue to threaten the Danish financial sector. Organizations in the sector frequently fall victim to small-scale DDoS attacks, and as a result, many financial organizations have adequate protection against these attacks.

DDoS attacks have multiple purposes, ranging from online service disruption to the thrill of the challenge, harassment, cyber attack camouflage or extortion, among others.

In the second half of 2020, several European financial institutions fell victim to extortion attempts as perpetrators demanded payment in Bitcoin for not carrying out a DDoS attack. The ransom size varied depending on the victim. In most cases, the DDoS attacks against European institutions were short and the organizations' DDoS protection systems mitigated the attack.

However, in late August 2020, the New Zealand Stock Exchange (NZX) was hit by a DDoS attack that disrupted the services of the Stock Exchange. Stock trades were repeatedly disrupted over a period of several days.

Cyber criminals may exploit the capital market

Cyber criminals may also attempt to gain unauthorized access to information from Danish listed institutions for insider trading purposes. A case in point is a 2016 attack in the United States. According to US authorities, two Ukrainian men gained unauthorized access to the U.S. Securities and Exchange Commission (SEC) and stole internal information on US listed companies. The hackers profited from selling the information and passed it on to stockbrokers and companies with whom they collaborated, allowing them to profit from insider trading as well. SEC is responsible for storing information on listed companies. Its Danish counterpart is the Financial Supervisory Authority.

In the medium term, cyber criminals may attempt to compromise and exploit financial and capital market infrastructures, as the profit margin is potentially higher. Security firms point out that the complex and extensive infrastructure of capital markets seems as an attractive target for hackers.

There are multiple potential ways to exploit capital markets, for instance, by fabricating trade orders or by compromising ownership infrastructure related to securities and by manipulating ownership data. The CFCS has no information of the occurrence of this type of attack. The CFCS assesses that it would require many resources and in-depth knowledge of financial and capital markets to exploit capital market infrastructures in a cyber attack.

Cyber espionage

The CFCS assesses that the threat of cyber espionage against the financial sector is HIGH. This means that it is likely that organisations in the financial sector will be subjected to attempts at cyber espionage within the next two years.

Financial institutions abroad regularly face cyber espionage attempts. The CFCS assesses it likely that this is also the case in Denmark. Cyber espionage is more difficult to detect than, for instance, cyber crime, whose immediate effects are plain to see as they often result in value loss or downtime for the victim. Consequently, attempts at cyber espionage may not be detected.

Foreign states have significant capabilities
Cyber espionage is mostly conducted by foreign states or state-sponsored hacker groups. Hackers working for foreign states have access to extensive resources, including sophisticated malware and information on vulnerabilities that have not yet been made public or patched, also called zero-day vulnerabilities.

Even though state-sponsored hacker groups have access to these resources, they often use the same, relatively simple, but effective attack techniques that they have used for years. This is because many public authorities and private companies remain vulnerable to these techniques. For instance, state-sponsored hackers launch brute force attacks and exploit known vulnerabilities.

Scanning of the financial sector
Scans of organizations are a common occurrence in the Danish financial sector. Both cyber criminals and state actors have likely conducted reconnaissance, using scanning against targets in the Danish financial sector. Even though scanning as such is harmless, it may be a warning sign of an impending cyber attack.

Some state-sponsored hackers also use publicly available tools, making it increasingly harder to distinguish between actors and their purpose. Some of the tools that states use are originally developed for white-hat hackers to perform IT security tests of organizations, including Cobalt Strike, Empire Powershell and Mimikatz. These tools are also widely used by cyber criminals and in some cyber activist networks.

Typically, an organization is able to reduce the risk of compromise by making it difficult for hackers to use simple attack techniques against them. The harder it is for hackers to compromise their targets using simple attack techniques, the more resources they need. Custom malware and information on zero-day vulnerabilities are usually very valuable and are thus only used relatively rarely.

Foreign states often use an attack technique known as “living off the land” that involves exploiting the victims’ own programmes to launch a cyber attack. The technique is effective and is used to achieve the same end goal as if hackers had

attacked with malware. It is difficult to detect because the hackers exploit legitimate programmes on the victim systems. In recent years, there have been many examples of this type of attack abroad, and a few examples in Denmark.

Politically and financially motivated cyber espionage
Financial sector authorities and institutions hold valuable information of relevance to foreign states, partly because this type of information may be exploited by foreign states to obtain knowledge of political and strategic policies, and partly to promote their national economy and strengthen their own national companies.

The political interest in espionage against the financial sector may be directed at sensitive information on bank clients and at information relevant for states' economic policies. Foreign states may also attempt to access information on the financial sector's organizational structure, resilience or individual issues related to institutions. In addition, Personally Identifiable Information (PII) may be valuable to foreign states given that they could have an interest in collecting information on specific individuals. PII on an individual may also facilitate targeted cyber attacks against the individual in the future.

Information related to foreign states' economic interests might include trade agreements and investments. Foreign states could also strengthen their economy by copying systems, technologies or by collecting internal data on Danish companies from public authorities and institutions in the financial sector. This information could potentially be exploited during negotiations or passed on to national companies that are competing with Danish companies.

Cyber espionage may precede other threats, such as destructive cyber attacks, hack and leak attacks. These threats are further described later in this assessment.

First-ever EU sanctions against hackers
In response to a number of cyber attacks against European-based companies and public authorities, the EU imposed the first ever sanctions against cyber attacks, see Council Implementing Regulation (EU) 2020/1125 of 30 July 2020. The sanctions came amid a series of accusations claiming that groups and individuals from Russia, China and North Korea had conducted cyber espionage. Some of the sanctioned groups have attacked financial sectors abroad.

The supply chain threat

Both in Denmark and abroad, there have been several cyber attacks against private companies and public authorities through suppliers and cooperation partners. The CFCS assesses that cyber attacks against suppliers and cooperation partners will continue.

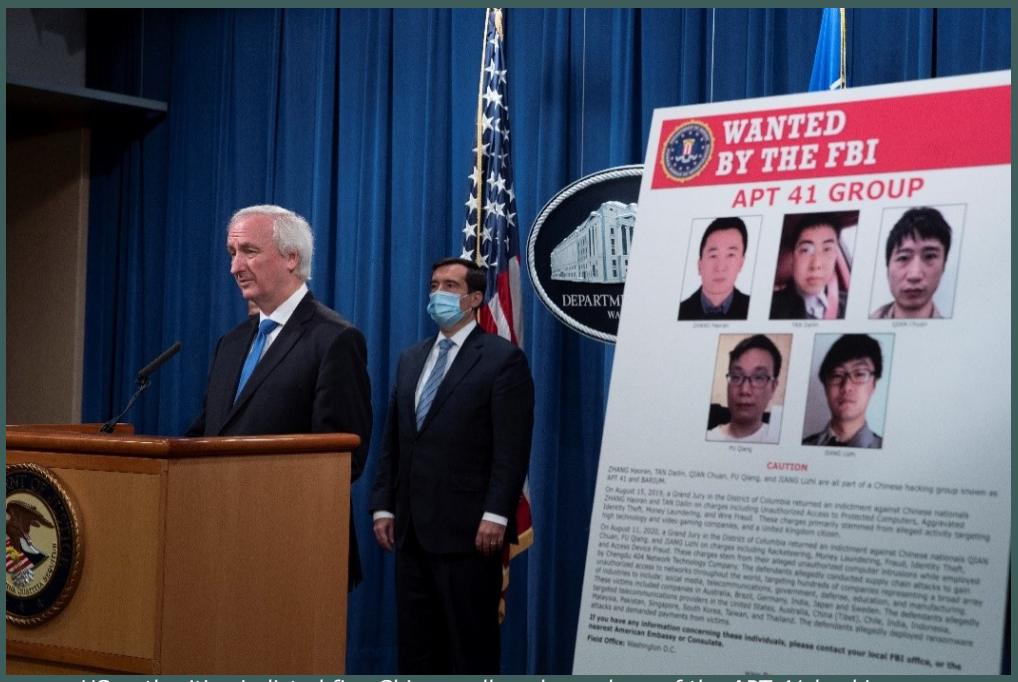
The CFCS assesses that both cyber criminals and foreign states might attempt to compromise financial sector organizations through the supply chain.

Several examples from abroad indicate that attacks or attempted attacks against financial institutions have taken place via the supply chain. A case in point is the GoldenSpy campaign. In June 2020, IT security company Trustwave released a report on a backdoor malware called GoldenSpy. According to Trustwave's report, GoldenSpy provides full access to victim systems, allowing attackers to install additional malware or run malicious programme. GoldenSpy has been hidden and installed with legitimate and mandatory tax payment software required for companies conducting business in China.

Although an attack against a supplier may occasionally be random, some hackers specifically target suppliers in order to gain unauthorized access to their client networks or systems. Thereby, hackers can exploit a supplier to access information or systems that belong to the hackers' intended target.

The attack technique is effective because by compromising a supplier, hackers are able to gain access to multiple targets, to client data or access to vital parts of a sector's infrastructure.

Chinese nationals charged with hacking supplier and its clients
In mid-September 2020, US authorities indicted members of the APT 41 hacking group, accusing them of hacking over 100 different victims across the world. The hackers had attacked some of the companies through a supplier. Three of the Chinese nationals were charged with both hacking into organizations for the benefit of the Chinese government and for their own personal financial gain.



US authorities indicted five Chinese alleged members of the APT 41 hacking group. PHOTO: Tasos Katopodis/EPA/Ritzau Scanpix

If a supplier with trusted, privileged access is compromised, hackers typically target remote administration solutions and accounts that the supplier uses to access their clients. Once the hackers gain access to these solutions and accounts, they are able to compromise the network belonging to the supplier's clients with the same privileges as those of the supplier. Hackers are also able to exploit the supplier's email account to send spear phishing emails to the supplier's clients, as already described.

Delivery of ransomware via supply chains is a possibility
In 2020, there have been several successful ransomware attacks against large international financial suppliers, including several successful ransomware attacks against suppliers used by financial sector companies in Denmark. According to CFCS information, the attacks did not spread to the systems of Danish companies.

Ransomware attacks may, at worst, spread to organizations in the Danish financial sector. Even if the attacks do not spread, they may have serious repercussions, including disruptions and delays to supplier services and leak of sensitive information stored or processed by the supplier.

American Bank Systems hit by Avaddon ransomware
In November 2020, the hackers behind the Avaddon ransomware leaked more than 50 GB which they had allegedly stolen from American Bank Systems (ABS). The data, which was leaked, was stolen in a ransomware attack against ABS. The hackers proclaimed that they had decided to leak the information due to ABS not paying the demanded ransom. Among ABS' costumers are several American financial institutions. Some of the costumers' sensitive data were leaked.

American Bank Systems INC - They do not want to pay and thinking that we are bluffing.
How can other companies do business with this hacked company? Know that by working with this company you are at risk of being hacked!
We also collected a client base of e-mail boxes of companies with which American Bank Systems worked, to which all kinds of mailings with the aim of hacking will be sent!
4 GB leak is now available, but more coming soon.We have over **50 GB** of information this company.
To be more precise:Declarations, statements, contracts, electronic negotiations, access to online banks of other banks, applications and their source codes
If you do not pay the ransom, we will do leaks this information, what will happen next, you yourself know!

The hackers behind the Avaddon ransomware claimed that ABS' costumers are in risk of being hacked. Furthermore, they claimed that mails of ABS' costumers would become targets of phishing campaigns. PHOTO: Screenshot of Avaddon DLS.

Cognizant hit by Maze ransomware
In April 2020, Cognizant announced that it had fallen victim to the Maze ransomware, while also recommending its clients to cut off connection to Cognizant to avoid infection. In addition to causing downtime and malfunctioning, Cognizant subsequently announced that sensitive data was stolen in the attack, including sensitive client data and employee credit card information. Cognizant is a global company, which delivers IT services to the financial sector. It facilitates products both to banking operations and capital markets. Cognizant also has an office in Denmark.

Finastra (former Mysis) hit by Ryuk ransomware
In March 2020, Finastra was likely victim of a Ryuk ransomware attack. Hundreds of foreign banks notified that they were affected by the attack. Open sources reported that Finastra successfully restored the compromised systems without paying ransom. Finastra is a service provider to the global banking sector, facilitating vital components to financial services, ranging from websites to back-office systems.

Cyber activism

The threat from cyber activism against the Danish financial sector is **MEDIUM**, which means that Danish financial sector companies and authorities may possibly fall victim to cyber activism attempts within the next two years.

CFCS has raised the threat level of cyber activism against the backdrop of a number of cyber activist attacks launched against European NATO countries in response to the war in Ukraine. Though the global number of cyber activist attacks has declined in recent years, Russia's invasion of Ukraine has galvanized some elements of the cyber activist community into action. While most cyber activist attacks were initially launched in direct continuation of the war and were mainly focused on Russia, Ukraine and Belarus, European NATO countries are now also increasingly becoming targets of cyber activist attacks.

The financial sector abroad has also been hit by cyber activist attacks. Pro-Russian cyber activists, for example, have claimed responsibility for DDoS attacks against banks in Germany, Romania, Latvia and Ukraine.

The aim of cyber activism is to draw as much attention as possible to a specific cause. Cyber activists are capable of launching various types of cyber attacks, ranging from simple DDoS attacks and website defacement attacks to more resource-intensive hack and leak operations.

As the threat level has been raised based on specific activities conducted by pro-Russian cyber activists in response to the war in Ukraine it also means that the threat level can change again with little warning depending on the development of the war.

Cyber activism is conducted by individuals or groups seeking to draw attention to single issues or punish organizations. Cyber activists are typically motivated by ideological or political concerns, ranging from political single issues to resistance to political powers. Cyber activists often target individuals or organizations that are perceived as symbolic targets as well as opponents to their cause. Thus, financial companies should always remain attentive to the risk of cyber activism if negative issues related to a specific company or the sector as a whole have put them in the crosshairs of cyber activists, or if cyber activists have threatened to launch cyber attacks.

Some activism campaigns run for years. Danish financial companies, however, are less likely to become targets in such campaigns. An example of a long running campaign is the anti-capitalistic campaign #OpIcarus. In previous campaigns, a Danish target was included on the target list along with many other foreign targets.

Cyber activist hacked a bank and offered bounty
An example of a cyber activist with significant resources is the group or the individual behind the alias Phineas Fisher. Phineas Fisher became infamous in 2014 and 2015 for hacking into the companies Gamma Group and Hacking Team, which sold surveillance software to states. Phineas Fisher leaked 400 GB of company data from Hacking Team, including hacking tools.

In late 2019, Phineas Fisher claimed that it had hacked into Cayman National Bank, stealing money and data from the bank. The bank confirmed that data had been stolen in a cyber attack. Phineas Fisher leaked the bank's data and described how the data was stolen and encouraged others to launch similar hack and leak attacks. Phineas Fisher even offered USD 100,000 bounty in cryptocurrency to hackers who break into banks and leak information of public interest.

Phineas Fisher has repeatedly published descriptions of how the victims were compromised.
PHOTO: Raphael Satter/AP/Ritzau Scanpix

Destructive cyber attacks

The CFCS assesses that the threat of destructive cyber attacks against Danish public authorities and private companies is **LOW**. Meaning that in the short term it is less likely that foreign states will launch destructive cyber attacks against Denmark, including the Danish financial sector.

However, the Danish financial sector may become collateral victim of destructive cyber attacks directed at targets outside of Denmark. This holds especially true for Danish private companies operating in Ukraine and Saudi Arabia. Companies operating in these countries may also occasionally be singled out as specific destructive cyber attack targets.

Danish private companies may also be affected by attacks targeting key international cooperation partners, which the sector directly or indirectly relies on. Such a scenario may ultimately affect the institutions and their vital services due to supplier downtime.

What is a destructive cyber attack?
The CFCS defines destructive cyber attacks as attacks that could potentially result in:

- death or personal injury.
- significant physical damage.
- Destruction or manipulation of information, data or software, rendering them unfit for use unless extensive restoration is undertaken.

Destructive cyber attacks are a technique that is mainly used in political and military conflicts. Several states have destructive cyber capabilities. The majority of destructive cyber attacks conducted so far have destroyed data by deleting or encrypting them without the possibility of restoration.

There are several examples of foreign financial companies falling victims to destructive cyber attacks. A case in point is the 2016 attack against the Ukrainian Ministry of Finance and Central Bank, which resulted in the disruption of 150,000 electronic transfers. In October 2020, US authorities accused named Russian nationals of being behind the attack. According to US authorities, the hackers were linked to a Russian intelligence agency.

Cyber terrorism

The threat of cyber terrorism against the financial sector is **NONE**.

The CFCS assesses that militant extremists have limited capabilities and resources to launch large-scale cyber attacks. Also, there are only a few examples of militant extremists encouraging cyber terrorism.

Consequently, the threat of cyber attacks against the Danish financial sector with the intent of causing the same serious repercussions as more conventional terrorist attacks, for example cyber attacks resulting in personal injury or property damage or widespread disruption of the financial sector's infrastructure, is none.

Relevant reports from the CFCS

The CFCS regularly publishes reports, guides and threat assessments. Below is a list of publications of particular relevance to the finance sector. All publications are available on the CFCS website.

The Cyber Threat from Phishing Mails
This threat assessment describes the threat from phishing emails. The assessment concludes that most cyber attacks today starts with a phishing mail. Read the assessment here: https://cfcs.dk/en/cybertruslen/trusselsvurderinger/phishing/

Cooperation between cyber criminals
The threat assessment "Do Cyber Criminals Dream of Trusting Relationships?" has the purpose of informing decision-makers on the development of organized cooperation between online criminals. Read the assessment here: https://cfcs.dk/en/cybertruslen/trusselsvurderinger/organised-cyber-crime /

The Anatomy of Targeted Ransomware Attacks
This investigation report describes each stage in a typical targeted ransomware attack and presents recommendations to public authorities and private companies on how to further improve their defence against them. Read the report here: https://cfcs.dk/en/cybertruslen/rapporter/the-anatomy-of-targeted-ransomware-attacks/

The threat from the attack technique "living off the land"
The threat assessment "Hackers leverage legitimate programmes in cyber attacks" highligts an attack technique that different threat actors use in their cyber attacks. The report includes advice on how to mitigate this kind of attacks. Read the assessment here: https://cfcs.dk/en/cybertruslen/threat-assessments/legitimate-programmes/

Cyber attacks against suppliers
Foreign states and criminals often attack their targets through the supply chain. This can be damaging to suppliers and clients both. Read the assessment here: https://cfcs.dk/en/cybertruslen/trusselsvurderinger/supply-chain/

HR departments are also a target for hackers
HR departments are popular targets for hackers. They will attack HR departments to both use them as an entry way into the organisation, and as a target in itself. The report includes advice on how to mitigate cyber attacks against HR departments. Read the assessment here: https://cfcs.dk/en/cybertruslen/trusselsvurderinger/cyber-threat-against-hr-departments/

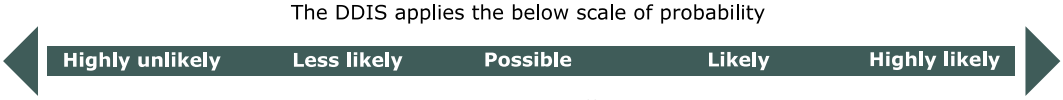
Threat levels

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.