CENTRE FOR CYBER SECURITY

Threat Assessment: The Cyber Threat Against Denmark During the COVID-19 Pandemic

Date: April 2020
1. edition

Centre for Cyber Security
Kastellet 30
DK-2100 Copenhagen

Tel.: +45 33 32 55 80
E-mail: cfcs@cfcs.dk
www.cfcs.dk

The purpose of this threat assessment is to update the threat landscape for the most serious threats, cyber crime and cyber espionage, in light of the COVID-19 pandemic.

Key Assessments

- The cyber threat remains a serious threat to Denmark.
- Hackers try to take advantage of the COVID-19 pandemic. This constitutes a new element in the general threat landscape, but the overall threats have not changed significantly. The pandemic has primarily affected the threat landscape in regards to which attack vectors hackers use.
- However, the changes in working conditions that many authorities and companies experience these days due to the pandemic may increase the risk that hackers succeed in their cyber attacks.
- The threat from cyber crime is **VERY HIGH**. No one is exempt from the threat. Independently of the COVID-19 pandemic, there is a growing threat from targeted ransomware attacks against Danish authorities and companies, and if they hit vital parts of Danish society, such as the healthcare sector, they can have severe consequences.
- The threat from cyber espionage is **VERY HIGH**. The threat is especially directed against public authorities dealing with foreign, security and defence politics as well as private companies who have valuable information of interest to foreign states. Among other sectors, the health sector has such knowledge.

Introduction

The threats from cyber espionage and cyber crime are still **VERY HIGH**. The cyber threat thereby remains a serious threat against Denmark. It will continue to be a serious threat in the future as the digitalisation and reliance on digital services continue to increase.

There are always hackers trying to exploit current events, developments, or circumstances to their advantage. This is also the case with the COVID-19 pandemic, where hackers, for instance have used

COVID-19 as a lure in phishing-mails. The exploitation of COVID-19 constitutes a new element in the general threat landscape, but the overall threats have currently not changed significantly. The COVID-19 pandemic has primarily changed the threat landscape in regards to which attack vectors the hacker are using.

However, the changes in working conditions that many Danish authorities and private companies experience these days due to the pandemic may increase the risk of hackers succeeding in their cyber attacks. This is addressed in the following section.

There is an increased risk of cyber attacks succeeding during the COVID-19 pandemic

Authorities and businesses may be more vulnerable during the ongoing COVID-19 pandemic. The cybersecurity in many authorities and companies is under pressure from the changing usage pattern in the form of new home offices, and because the availability of the systems is given high priority. The new working conditions can give hackers easier access to corporate systems and make it harder to detect the hackers in the systems.

Therefore, even though the threat landscape is unchanged, Danish authorities and companies might face changes in their risk landscape.

One of the factors that might make organizations more vulnerable is, if the usual precautionary measures are not maintained or performed routinely. This might, for example, be system- and software updates or deselection of VPN connection or multi-factor authentication. In addition, resource constraints may be a problem with regards to, for example, detection and handling of cyber attacks.

It can have particular severe consequences for Denmark if vital parts of the Danish society are hit by, for example, ransomware attacks during the pandemic.

The Danish Centre for Cyber Security (CFCS) have written several guides on how you can improve your cyber security. They can be found on CFCS' web page, www.cfcs.dk. They are currently only available in Danish.

Cyber Crime

The threat from cyber crime is **VERY HIGH**. As a result, it is highly likely that Danish private companies and public authorities will be targets of attempted cyber crime within the next two years.

To the purposes of this assessment, the term cyber crime is used collectively to describe actions in which hackers use cyber attacks to commit crimes for financial gain.

In this threat assessment, the term cyber crime refers to actions in which hackers use cyber attacks to commit crimes for financial gain.

Cyber crime constitutes a persistent and active threat to all Danish public authorities, private companies and citizens.

Cyber criminals most often launch relatively simple attacks against multiple targets simultaneously, for instance through phishing attacks. However, networks also exist that have the capability to launch more complex and time-consuming cyber attacks, including targeted ransomware attacks.

Cyber attacks by criminal groups typically start without the actor having singled out a specific target. Most cyber attacks start off as attacks of opportunity. Attacks may include phishing emails being spread to thousands of victims, or IT systems and units with known vulnerabilities being abused by cyber criminals.

Cybercriminals try to exploit the Danes' interest in COVID-19

CFCS have knowledge of a rise in phishing emails sent to Danish authorities and companies during the COVID-19 pandemic. Several IT security companies also report an increase in phishing attempts in other countries over the past month.

Many of these phishing mails use COVID-19 as a lure in order to enhance the likelihood that the receiver opens the email and clicks on links or attached files. The hackers are thereby trying to exploit the Danes' demand for knowledge about COVID-19 and the current health crisis.

During the COVID-19-pandemic there has also been created a fairly large amounts of new, fake domains. Cyber criminals have among other things used these domains to trick Danish citizens into disclosing their NEMID-information or login information. Some of the fake domains resemble legitimate health authorities' home pages and names. CFCS collaborates with other entities in order to take down known fake domains.

Furthermore, there are fake applications and malware for mobile devices using COVID-19 as a theme. The false apps can for example steal information from the mobile device.

CFCS assesses that criminals will also try to take advantage of public compensation schemes as a theme in their phishing emails.

Cybercriminals exploit vulnerabilities and the fact that many work from home

Cyber criminals continuously exploit new vulnerabilities. When a new technical vulnerability emerges, it is often only a matter of weeks before it is exploited in hacking attempts against Danish targets.

The high frequency of attacks makes it vital for the IT departments of Danish public authorities and private companies to be timely in updating systems and programmes or in adopting mitigating measures in those instances when it is not possible to patch a vulnerability. This is also the case during the COVID-19 pandemic. For example, in relation to securing remote accesses, such as VPN-solutions, as well as securing the clients who can use these accesses.

There are media reports on hackers trying to exploit the increased need for remote access, VPN solutions, and online communications and collaboration platforms.

For example, cyber criminals have developed a new module for the widely used malware TrickBot. The new module is designed specifically to make brute-force attacks against Remote Desktop Protocol (RDP). TrickBot is used for different types of attacks, including targeted ransomware attacks.

According to IT security companies there are hackers offering fake VPN solutions. There are also reports of several new fake domains resembling the communication and collaboration platform Zoom's domains.

In addition, there have been examples of employees and citizens being called by criminals pretending to be IT personnel or employees from legitimate companies or authorities. The criminals try to trick sensitive information out of employees or get them to download files infected with malware.

Besides changes in attack vectors, it is possible that there will be a rise in certain types of attacks that the hackers think will be more effective because many work from home. This could, for example, be BEC-scams, also known as CEO-fraud, where hackers try to trick organizations into transferring money to them. The hackers often send fraudulent emails where they impersonate CEOs or colleagues in order to make the employees believe that they are transferring money after orders from the management.

Another type of attack that could be on the rise is denial of service attacks, such as DDoS attacks, where the hackers demand a payment in order to stop the attack. Many authorities and companies are currently more dependent on the internet, which can enhance hackers' interest in this type of attack.

CFCS assesses that most DDoS attacks are launched by individuals, who want some excitement or to harass others. Even though most of these attacks are small-scale without the potential to threaten critical functions, this group also includes actors that have the capabilities to launch or buy powerful DDoS attacks.

The threat from targeted ransomware attacks is on the rise

There is a growing threat from targeted ransomware attacks against Danish public authorities and private companies. This rise happens independently of the COVID-19 pandemic.

A tageted ransomware attack may have a severe impact on critical functions in the Danish society. This has been seen in connection with ransomware attacks against the healthcare sector in the United States and Great Britain, among others, where downtime in administrative systems resulted in the cancellation of patient appointments. A successful targeted ransomware attack on the Danish healthcare sector could enhance the strain the sector is under due to the COVID-19-pandemic.

In targeted ransomware attacks, criminals try to extort public authorities and private companies, demanding huge sums of money by using ransomware to encrypt key parts of the victim's IT systems.

Since late 2019, hackers behind targeted ransomware attacks have occasionally also threatened to leak sensitive data from the affected systems if the victims fail to pay the ransom.

A few Danish private companies have fallen victim to targeted ransomware attacks. In the autumn of 2019, the Danish companies Demant and GlobalConnect became targets of separate ransomware attacks. According to Demant's own estimates, the attack on the company resulted in losses running as high as DKK 650 million. In February 2020, the global service company ISS became the victim of a ransomware attack that also affected its Danish branch and had major financial consequences.

Cybercriminals sell accesses to networks, which are later used in targeted attacks

Cooperation takes place between criminals who launch more targeted attacks and criminals who target thousands of victims, for instance through phishing. Targeted ransomware attacks are for instance often launched following an initial opportunistic compromise of the victim network via malware distributed through phishing. Sharing and sale of such initial compromises are called "access-as-a-service".

Consequently, mass compromises through phishing are not only a threat in themselves; they also facilitate the increasing threat from targeted cyber attacks launched by criminals.

Cyber espionage

The threat from cyber espionage is **VERY HIGH**, meaning that Danish public authorities and private companies will highly likely become targets of attempted cyber espionage over the next two years.

Denmark is the target of both politically and commercially motivated cyber espionage by foreign states.

The threat from cyber espionage is persistent and also applies during the current COVID-19 pandemic. Like cybercriminals, foreign states

also abuse COVID-19 as a lure in their phishing and spear phishing emails.
Foreign states know that Danish public authorities and private companies have different working conditions during the crisis and that it can make them vulnerable. Foreign states are quick to exploit vulnerabilities.

The threat is also during the COVID-19 pandemic particularly directed against Danish public authorities involved in foreign, security, and defence policy, as well as Danish private companies who have valuable information of interest to foreign states.

Foreign states may also try to target suppliers and partners to the above-mentioned types of public authorities and private companies, using them as entry points for access to the public authorities and private companies that are the ultimate targets. Though some sub-suppliers or partners may not have knowledge of interest to foreign states, they may have access or credibility that can be exploited by hackers to compromise their intended targets.

Cyber espionage may result in pressure on Danish decision-makers
Foreign states likely try to use cyber espionage as a means to gain insight into Danish interests, deliberations and decisions on major international issues or foreign policy negotiations. The states may exploit this knowledge as leverage against Danish interests or to put Danish negotiators and decision-makers under pressure.

Russia and China in particular have access to substantial cyber capabilities, which both countries use actively on a global scale. It is likely that some countries, including Iran, also conduct cyber espionage and other types of cyber attacks against targets in their immediate vicinity and beyond.

Cyber espionage may jeopardize Danish competitiveness and economy
States also resort to cyber espionage to strengthen their own national development and competitiveness. This particular breed of cyber espionage specifically targets private companies and institutions whose knowledge or intellectual property is valuable to foreign states.

The states may use the stolen information to promote the development of their own national sectors, as it allows them to skip several steps in their innovation and development process.

Cyber espionage may thus damage the competitiveness of Danish private companies and, by extension, the Danish economy, in particular if the espionage targets businesses that hold a competitive edge.

Research related to the COVID-19 pandemic is an example of knowledge that can be valuable to foreign states. Independently of the COVID-19 pandemic, CFCS assesses that foreign states have an interest in parts of the Danish healthcare sector with access to research

data or valuable intellectual property. This is, for example, companies and universities involved in bio chemistry, bio technology and pharmaceuticals.

The boundaries between commercially motivated and security policy motivated cyber espionage may overlap.

Threat levels

The Danish Defence Intelligence Service uses the following threat levels

NONE	No indications of a threat. No acknowledged capacity or intent to carry out attacks. Attacks/harmful activities are highly unlikely.
LOW	A potential threat exists. Limited capacity and/or intent to carry out attacks. Attacks/harmful activities are less 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 highly likely.

The DDIS applies the below scale of probability