CENTRE FOR
CYBER SECURITY

Threat assessment

The threat of cyber espionage against Danish research and universities

1st edition September 2021

Table of contents

CENTRE FOR
CYBER SECURITY

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

1st edition September 2021

Threat assessment: The threat of cyber espionage against Danish research and universities

The purpose of this threat assessment is to provide information on the cyber threat against Danish universities and research institutions. The threat assessment can be used in the institutions' risk assessment efforts. This assessment is mainly intended for executives and IT employees at Danish universities and research institutions.

Key assessment

- The threat of cyber espionage against Danish universities and research institutions is **VERY HIGH**. The threat has increased from **HIGH** to **VERY HIGH** since the last assessment, made in 2018.

- Universities and research institutions are exposed to a persistent threat of cyber espionage. The threat emanates from foreign states that target research institutions worldwide. The threat of cyber espionage is also directed at Danish universities and research institutions, which have been repeated targets of cyber attack attempts.

- Hackers often attempt to break into universities' interconnected IT networks such as email systems, potentially allowing them to gain unauthorized access to research across different subject areas within the individual universities.

- There is no clear picture of what kind of research the foreign states are targeting in their cyber espionage attacks. However, concrete incidents in Denmark and abroad indicate that foreign actors have a specific interest in certain subject areas.

- So-called dual-use technology and research in dual-use technology are of special interest to foreign states. As a result, research in technologies and use of technologies designed for both civilian and military purposes are prime targets for cyber espionage by foreign states.

- Danish universities and research institutions also face a **VERY HIGH** threat from cyber crime. Like targets in many other sectors, universities may, for instance, fall victim to targeted ransomware attacks.

Analysis

Danish and foreign universities and research institutions are continuously targeted by state-sponsored and criminal hackers.

This threat assessment mainly focuses on the cyber espionage threat against Danish universities and research institutions. The threat of cyber espionage against Danish universities was assessed in our 2018 threat assessment "*Danish universities are targets of cyber attacks"*. In this present threat assessment, the threat level is raised from **HIGH** to **VERY HIGH** as universities and research institutions in Denmark and abroad face a persistent threat from cyber espionage as reflected in cyber attacks against research institutions.

As a result, Danish universities and research institutions will highly likely become targets of a cyber espionage attempts within the next two years.

In addition to the cyber espionage threat, the threat of cyber crime against Danish research institutions and universities is also **VERY HIGH**. The threat from criminal hackers is described briefly at the end of this threat assessment.

The threat of destructive cyber attacks and cyber activism against Danish universities and research institutions is **LOW**. These two threats are not further described in this assessment.

The cyber threat level against Danish research institutions and universities is the same as the overall threat level against Denmark. The CFCS recommends that all Danish universities and research institutions keep up to date on developments in the cyber threat picture on the CFCS' website and also read the annual threat assessment on the cyber threat against Denmark.

Research is an attractive and constant cyber espionage target

The threat of cyber espionage against universities and research institutions is persistent. The threat emanates from several foreign states that target research worldwide. The threat of cyber espionage is also directed at Danish universities and research institutions, which have been repeated targets of attempted cyber attacks.

The motives of foreign states for conducting cyber espionage attacks against research institutions and universities may differ. In some cases, cyber espionage may be motivated by the prospect of gaining competitive and strategic advantages by stealing sensitive or valuable data. Some foreign states are likely also conducting espionage to promote their own national research efforts and development of functions vital to society such as critical infrastructure.

Hackers use a variety of attack techniques in their attempts to compromise Danish universities and research institutions. Research institutions and universities in Denmark and abroad have been specifically targeted in spear phishing and brute force attacks.

Iran likely behind cyber attacks against universities

Since 2013, the Silent Librarian hacker group (also known as Cobalt Dickens and TA407) has launched cyber attacks against universities worldwide, including Denmark. The hacker group uses a variety of attack techniques, mainly spear phishing, where the hackers created fake login sites to different IT systems connected to universities in an attempt to harvest login credentials.

In 2018, the US Department of Justice indicted alleged Silent Librarian members for attacking 144 US universities and for stealing 31,5 terabytes of data from approx. 340 universities worldwide, including the US universities. According to the US indictment, the Iranian hackers acted on behalf of the Iranian Revolutionary Guard Corps (IRGC).

Hackers often attack interconnected IT networks and systems

Hackers often try to break into interconnected IT networks, such as email systems. This enable them to potentially gain unauthorized access to research across different subject areas within the individual universities.

However, in other instances, hackers have launched more targeted attacks, such as spear phishing attacks directed against specific professors.

GRU accused of brute force attacks against universities
In July 2021, US and British authorities released a so-called Cybersecurity Advisory claiming that Russian military intelligence service GRU is behind extensive brute force attack campaigns against universities, as well as other types of targets.

According to the report, the attacks have been conducted since mid-2019 and are most likely still ongoing. The attacks have specifically been targeting Microsoft 365 cloud services, but email servers have also been targeted.

Certain subject areas are of special interest to foreign states

There is no clear picture of what type of research foreign states are after as hackers often attack interconnected targets such as email systems. However, concrete cases in Denmark and abroad indicate that foreign states could have a specific interest in certain subject areas.

This applies to research institutions working on security and foreign policy issues, that have influence on national decision-makers. It also applies to military research- and educational institutions and universities and research institutions engaged in Arctic-related subjects.

Thus, there is convergence between the issues that have caught the strategic attention of foreign states and their goal for cyber espionage against universities and research institutions.

Important events also affect the cyber espionage threat
During the COVID-19 pandemic, foreign states have also shown an interest in COVID-19 related research, illustrating how key incidents determine the type of research that foreign states spy against.

Foreign states focus on dual-use technology

So-called dual-use technology and research in dual-use technology are of special interest to foreign states. As a result, research in technologies and use of technologies that are developed for both civilian and military purposes are prime targets for cyber espionage.

The potential use of technologies for both civilian and military purposes may suggest that compromise of dual-use targets may allow foreign states to meet both commercial and security policy needs simultaneously.

Building capabilities in dual-use technology is a declared political objective of some countries holding significant cyber capabilities, for example, part of the modernization of the Chinese military defence involves "civilian-military fusion" (”junmin ronghe”) with focus on dual-use technologies. In Russia, the development of dual-use technologies is also a declared objective of the country’s military research agency, the Foundation for Advanced Research Projects (FPI).

Cyber crime constitutes a very high threat to Danish universities

The threat of cyber crime against Danish universities is also **VERY HIGH**. Just like potential targets in many other sectors, universities may, for instance, fall victim to targeted ransomware attacks.

Since 2019, several cyber criminal groups have focused on executing or supporting targeted ransomware attacks. In 2020, these hacker groups started expanding the scope of their extortion activities by threatening to leak sensitive data stolen in connection with ransomware attacks.

Several universities abroad have been victims of this type of targeted ransomware attacks. The CFCS assesses that Danish universities and research institutions are not immune to the threat of targeted ransomware attacks.

The most common type of cyber crime activities continues to be broad cyber attacks against a large number of potential victims across society, including phishing, exploitation of known vulnerabilities in popular IT systems and exploitation of weak remote access systems. As a result, Danish universities and research institutions can expect to fall victim to cyber crime attempts.

German university hospital was hit by a targeted ransomware attack

In September 2019, a university hospital in Düsseldorf suffered a Doppelpaymer ransomware attack. As a result, the hospital’s treatment capacity fell by about 50 per cent.

An ambulance on its way to the university hospital with a female patient was re-routed to another hospital due to reduced capacity caused by the attack. The woman passed away. Afterwards, the German authorities investigated whether the female patient’s death could be linked to the ransomware attack, the authorities concluded that there were insufficient grounds to prosecute.

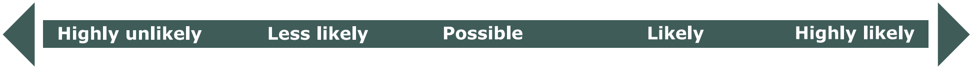
Criminals use tools and attack techniques typically developed for specific criminal purposes, including theft of personal data, extortion through ransomware or exploitation of IT systems for cryptocurrency mining. The diversity of the attacks indicates that cyber crime involves a range of illicit enrichment crimes, including theft, extortion and fraud.

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



Highly unlikely **Less likely** **Possible** **Likely** **Highly likely**

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

Further relevant readings

The Centre for Cyber Security (CFCS) regularly publishes guides and threat assessments. Below is a list of publications of relevance to the handling of the cyber threat against Danish research and universities. All publications are available on the CFCS website.

The threat from phishing mails
The threat assessment ”The Cyber Threat from Phishing Mails” describes how hackers use phishing and spear phishing mails in their attempts to compromise companies or steal sensitive information. Read the assessment her:
https://cfcs.dk/en/cybertruslen/threat-assessments/phishing/

Guide on how to counter phishing
The guide ”Reducer risikoen for for falske mails” (only available in Danish) is intended for executives, and it presents a series of concrete recommendations that contribute to organizations' efforts to protect against and counter phishing attacks. Read the guide here:
https://cfcs.dk/da/forebyggelse/vejledninger/reducer-risikoen-for-falske-mails/

The cyber threat against Denmark
The annual threat assessment ”The Cyber Threat Against Denmark 2021” describes the overall cyber threats against Denmark, and includes chapters on the threat from cyber crime, cyber espionage, destructive cyber attacks, cyber activism and cyber terror. Read the assessment here:
https://cfcs.dk/en/cybertruslen/threat-assessments/the-cyber-threat-against-denmark/

Cooperation between cyber criminals
The threat assessment ”Do Cyber Criminals Dream of Trusting Relationships?” describes how established cooperation relationships, division of labour and exchange services inside the criminal environment contribute to creating a high threat of cyber crime, in general, and targeted ransomware attacks, in particular. Read the assessment here:
https://cfcs.dk/en/cybertruslen/threat-assessments/organised-cyber-crime/

The threat from targeted ransomware attacks
The threat assessment ”Trusselsvurdering: Digitale gidseltagere på storvildtjagt” (only available in Danish) describes the threat from so-called targeted ransomware attacks. Read the assessment here:
https://cfcs.dk/da/cybertruslen/trusselsvurderin-ger/malrettet-ransomware/

The anatomy of targeted ransomware attacks
The investigation report” The Anatomy of targeted ransomware attacks” thoroughly describes how such attacks happen. The report also provides concrete recommendations on how to mitigate or counter the attacks. Read the report here:
https://cfcs.dk/en/cybertruslen/reports/the-anatomy-of-targeted-ransomware-attacks/

Guide to counter ransomware attacks

The guide ”Reducer risikoen for ransomware” (only available in Danish) provides a number of recommendations that organizations can follow to reduce the likelihood of being hit by a ransomware attack. The guide also provides guidance on how to handle the situation once an organization has been hit. Read the guide here: https://cfcs.dk/da/forebyg-gelse/vejledninger/ransomware/

The threat from cyber attacks against suppliers

The threat assessment ”Cyber Attacks against Suppliers” describes the cyber threats against suppliers. Read the assessment here:
https://cfcs.dk/en/cybertruslen/threat-assessments/supply-chain/

Guide on managing supplier relations

The guide ”Informationssikkerhed i leverandørforhold” (only available in Danish) contains a number of recommendations on how to manage the relationship between organizations and their suppliers. Read the assessment here:
https://cfcs.dk/da/forebyggelse/vejledninger/informations-sikkerhed-i-leverandorforhold/

The threat from intentional and unintentional insiders

CFCS and the Danish Intelligence and Security Service (PET) has published the threat assessment "The threat from intentional and Unintentional Insiders”. The threat assessment describes the threat and provides recommendations for mitigating initiatives. Read the assessment here:
https://cfcs.dk/en/cybertruslen/threat-assessments/insiders/

The threat against the defence industry

The threat assessment ”Cybertruslen mod forsvarsindustrien” (only available in Danish) describes the threat from different types of cyber attacks against the defence industry. Read the assessment here:
https://cfcs.dk/da/cybertruslen/trusselsvurderinger/forsvarsindustrien/

Cyber attacks against HR departments

The threat assessment ”HR Departments are also hit by targeted cyber attacks” describes how hackers attempt to use HR departments as an easy entry point to compromise organizations. The assessment also provides recommendations on how organizations can provide support to their HR departments, including both technical and measures and awareness. Read the assessment here:
https://cfcs.dk/en/cybertruslen/threat-assessments/cyber-threat-against-hr-departments/