CENTRE FOR CYBER SECURITY

Threat Assessment:

Energy sector companies are attractive ransomware targets

1st edition December 2021

Table of Contents

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

1st edition December 2021

Energy sector companies are attractive ransomware targets

The purpose of this threat assessment is to inform organizations in the Danish energy sector of the persistent threat from ransomware attacks following the May 2021 Colonial Pipeline attack. Even though the threat is not unique to the energy sector, the potential consequences of successful attacks are extensive and require a high level of preparedness.

Key assessment

- The threat from cybercrime against the Danish energy sector is **VERY HIGH**. Criminal groups continue to have the capability and intent to launch ransomware attacks against energy sector companies despite some hackers having claimed that they no longer will target critical infrastructure.

- Energy sector companies are attractive targets for cyber criminals for a number of reasons. Some cyber criminals use the potential consequences of operational disruptions as leverage to increase pressure on their victims.

- Despite significant focus on cyber security, operational technology (OT) systems are hit by ransomware attacks. Ransomware attacks against IT systems may also indirectly disrupt operations, as was illustrated by the 2021 Colonial Pipeline incident.

Darkside might be gone, but the threat from ransomware remains

The CFCS assesses that the threat from cyber crime, including ransomware attacks, against the Danish energy sector is **VERY HIGH**.

The threat level has not changed, even though in the spring and summer of 2021 following the Colonial Pipeline incident, several top-tier Ransomware-as-a-Service (RaaS) operators stated that they would refrain from attacking critical infrastructure in future. These statements were made at the same time as US authorities increased their focus on ransomware attacks, with the federal agencies now characterizing the threat from ransomware attacks as a serious threat to national security.

Even if some of the RaaS operators in question refrain from targeting critical infrastructure in, for instance, the energy sector, other groups will still have the capability and intent to deploy ransomware attacks against energy sector organizations. The fact that the threat remains unabated is further underlined by recent attacks, for instance, against Danish utility company Kalundborg Forsyning in late August 2021 as well as the Lockbit 2.0 incident against Italian renewable energy company ERG in late July 2021.

Ransomware-as-a-Service (RaaS)
RaaS enables cyber criminals to buy access, tools and infrastructure with the intent to deploy ransomware attacks rather than develop these themselves. RaaS has introduced a kind of platform economy to cyber crime in which affiliates use ransomware attacks to make a profit for themselves and also for the criminal owners of the platform. Illustrative of this is the Darkside RaaS platform, which was used in the Colonial Pipeline attack.

The aftermath of the Colonial Pipeline attack
US company Colonial Pipeline, which provides most of the US East Coast's fuel supply, fell victim to a ransomware attack in May 2021. The attack forced the company to shut down pipeline operations for six days, leading to long lines at petrol stations and widespread concern about fuel shortages. The attackers had deployed the Darkside ransomware, which had been obtained via a RaaS platform. The hackers had allegedly gained unauthorised access to Colonial Pipelines IT networks via a VPN access, which should have been deactivated. According to Colonial Pipeline, it subsequently took proactive steps to shut down the pipeline as a precautionary measure. Colonial Pipeline paid more than USD four million in ransom in the attempt to quickly restore operational services.

Following the Colonial Pipeline attack, US authorities, in particular, ramped up pressure on ransomware operators, forcing RaaS gangs to reorganize their activities. For instance, Darkside operators stated that they were not intentionally targeting critical infrastructure and would avoid doing so in future. Subsequently, Darkside operators shut down their platform operations entirely.

The changes in the RaaS landscape are described in more detail in our threat assessment "Old hackers, new platforms", which is available on the CFCS website. The threat assessment concludes that the changes have not reduced the overall threat level and that even though several top-tier RaaS platforms shut down in 2021, the vacuum left by the absence of widely used platforms was quickly filled by other platforms. In addition, the operators behind one of the platforms, the REvil platform, have reactivated their operations after the shutdown.

Anyone can fall victim to a ransomware attack, including the energy sector

Targeted ransomware attacks are financially motivated, they are opportunistic and can hit any type of organization and public authority, including energy sector organizations. This is due to many factors.

Firstly, the Danish energy sector comprises numerous companies – of which a considerable share generates relatively substantial revenues. The revenue alone makes these companies interesting targets for criminal gangs as they count on these organizations to be able to pay substantial ransom demands. Over the next few years, criminals will highly likely continue their malicious activities if the potential reward is believed to outweigh the risk of public scrutiny.

Secondly, another element that may make Danish energy sector companies high-profile targets is the risk of operational disruptions that put these companies and society as a whole under strong pressure. In order to restore business operations, paying the ransom may seem tempting to the company. However, paying the ransom does in no way guarantee that operations can be immediately resumed. For example, several media reported that Colonial Pipeline used its own backups to help restore the systems when the decryption key, for which ransom was paid, was too slow.

Some criminals actively use the threat of operational disruptions as leverage to force victims into paying ransom. For example, the Lockbit 2.0 RaaS gang has used the Colonial Pipeline attack as a worst-case scenario to exert pressure on a victim in the transport sector outside Denmark, threatening that if the company failed to pay the ransom demand, the consequences would be similar to those of the Colonial Pipeline attack.

Directly and indirectly targeted OT systems

A high level of cyber security makes it difficult for hackers to disrupt operations via Operational Technology (OT) systems but not impossible, as is repeatedly evidenced. Illustrative of this is the 2021 ransomware attack against a Danish company whose OT network computers were infected with a file-encrypting malware causing temporary system shut-down. The attack was conducted through a sub-supplier. 2021 also saw several examples of ransomware attacks outside Denmark that have compromised OT components, though without having a serious impact on production.

An increasing number of companies, including energy sector companies, use the option of monitoring and automating physical processes via "smart units" that connect parts of the industrial process to the IT system via the Internet, also known as the Industrial Internet of Things (IIoT). The move towards physical production systems going online creates a number of new security challenges and vulnerabilities.

Ransomware attacks against company IT systems may force organizations to close down OT systems in an effort to counter and contain the malware. As illustrated above, Colonial Pipeline was forced to shut down its OT systems in order to contain the malware and prevent it from spreading across its systems. Ransomware attacks against company IT systems may also force organizations to switch to manual production, as was the case with the 2019 ransomware attack against Norwegian energy company Norsk Hydro.

A directly or indirectly compromised OT system – or uncertainty about the scope of a compromise – may have significant financial consequences for the compromised company. If energy sector companies are attacked with ransomware, the consequences may not only affect the company but also citizens and society as a whole. The continuous fusion between IT and OT – between cyber and the physical world – may exacerbate the potential consequences of an attack.

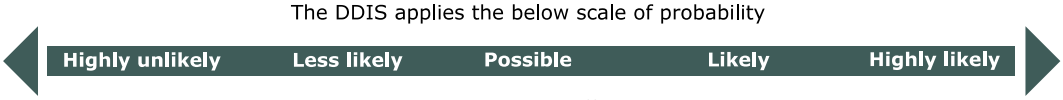
Threat levels

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.

Further relevant reading

The Centre for Cyber Security (CFCS) continuously publishes guidance and threat assessments. Highlighted below are a number of publications of particular relevance to the energy sector. All publications are available on the CFCS website.

Changes in the RaaS landscape in the wake of the Colonial Pipeline attack
The threat assessment "Old hackers, new platforms" describes how RaaS gangs have reorganized their activities following the Colonial Pipeline ransomware attack.
Read the assessment here: https://www.cfcs.dk/en/cybertruslen/threat-assessments/old-hackers-new-platforms/

The Cyber threat against Denmark (2021)
In this annual threat assessment, the CFCS describes the cyber threat against Denmark, ranging from cyber crime, cyber espionage, destructive cyber attacks and cyber activism to cyber terrorism.
Read the assessment here: https://www.cfcs.dk/en/cybertruslen/threat-assessments/the-cyber-threat-against-denmark/

Protect your company's production systems
In the guide "The executive board's roles and responsibilities in connection with protection of industrial control systems", the CFCS describes how company executives can protect its industrial control systems against cyber attacks.
Read the guide here (Danish):
https://www.cfcs.dk/da/forebyggelse/vejledninger/ics-ledelsen/

The Cyber threat against the Danish energy sector (2020)
In this threat assessment, the CFCS describes the overall cyber threats facing the Danish energy sector. This threat assessment is intended, in particular, for public authorities and private organizations that are part of the implementation of the national cyber and information strategy.
Read the assessment here (Danish):
https://www.cfcs.dk/da/cybertruslen/trusselsvurderinger/energi/

Collaboration between cyber criminals
The threat assessment "Do cyber criminals dream of trusting relationships?" describes how established division of labour and exchange of services inside the criminal environment contributes to creating a very high threat of cyber crime, in general, and targeted ransomware attacks, in particular.
Read the assessment here: https://www.cfcs.dk/en/cybertruslen/threat-assessments/organised-cyber-crime/

The threat of targeted ransomware attacks
The threat assessment "Criminals tighten the digital thumbscrew" describes the threat of targeted ransomware attacks that may potentially have serious repercussions for an organization.
Read the assessment here: https://www.cfcs.dk/en/cybertruslen/threat-assessments/double-extortion/

Guide to counter ransomware attacks

The guide "Reduce the risk of ransomware" presents a number of recommendations that organizations may follow to reduce the risk of ransomware attack. Also, the guide provides recommendations on how to handle a potential ransomware attack once the organization has been breached.

Read the guide here (Danish):

https://www.cfcs.dk/da/forebyggelse/vejledninger/ransomware/