CENTRE FOR CYBER SECURITY

Threat assessment

# The ransomware threat against manufacturing companies

## Table of contents



CENTRE FOR CYBER SECURITY

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

1st edition January 2024

# The ransomware threat against manufacturing companies

The purpose of this threat assessment is to inform manufacturing companies of the very high threat from cyber crime. The assessment is directed towards manufacturing company decision-makers and can form part of the organization's risk analysis process.

For the purpose of this assessment, manufacturing companies are defined as companies engaged in the manufacturing of tangible goods such as machines and pharmaceutical products.

# Key assessment

- The threat from cybercrime against Danish manufacturing companies is **VERY HIGH**. As ransomware actors are indiscriminate in their choice of victims, critical manufacturing companies too fall victim to ransomware attacks.

- Manufacturing companies mainly fall victim to targeted ransomware attacks because ransomware actors work under the assumption that such companies are able and willing to pay large ransoms for the decryption of their data and systems.

- Ransomware attacks can interrupt manufacturing operations and lead to complete operational shutdowns, inflicting financial losses on the company.

- As data travels across many interconnected systems in manufacturing environments, attacks on company IT have the potential to impact operational processes. At the same time, lack of segmentation makes it easier for hackers to carry out harmful attacks, the very fear of which can lead to a self-imposed production shutdown by the company.

- Manufacturing companies also face the threat of extortion in attacks where criminal cyber actors steal data without encryption, subsequently threatening to leak the stolen sensitive information.

- In their attempt to extort the targeted companies, criminal actors often publicly expose their victims.

# Criminal actors attack manufacturing companies

The CFCS assesses that the threat from cybercrime, including ransomware attacks against Danish manufacturing companies, is at the level **VERY HIGH**.

The threat mainly emanates from the capability and intention of criminal actors to conduct targeted ransomware attacks against European manufacturing companies, including companies in Denmark. The CFCS knows of several Danish manufacturing companies falling victim to ransomware attacks in 2023.

As ransomware actors are opportunistic in their targeting, attacks are conducted across industries that all have manufacturing as a common theme. Manufacturing companies exist in all sectors, with some holding critical functions such as the production of food and pharmaceuticals. Common features of these companies are the multiple processes required to manufacture a physical product, and the fact that a ransomware attack can disrupt or shut down their manufacturing operation. The ramifications of such an attack can extend beyond the company if the goods it produces are critical to society.

Attacks from organized Ransomware-as-a-Service (RaaS) groups especially dominate the threat landscape. When looking at the types of manufacturing companies that have fallen victim to ransomware attacks, it seems that the actors do not discriminate between whether or not the products manufactured by the companies are critical to society. As an example of this, in 2023 the LockBit 3.0 RaaS group claimed responsibility for attacks on targets as diverse as Swedish brewery Åbro Bryggeri, and Rosenbauer, an Austrian manufacturer of fire engines and firefighting equipment.

### RaaS: Specialized cyber criminals work together to obtain ransoms

Ransomware-as-a-Service (RaaS) is an illegal business model akin to the platform economy found in legal markets.

Ransomware operators develop ransomware and offer it as a service to criminal affiliates who launch the actual attack against the victims. The ransom is often paid directly to the operators who pass on a share to their affiliates.

**Manufacturing companies make attractive targets for ransomware actors**
RaaS groups first focus on obtaining initial access to an organization, frequently through the use of broader campaigns such as phishing attacks or compromises based on random vulnerability scans that are not targeted against specific victims or industries. Once initial access has been obtained, the groups target their efforts against organizations that they expect will be able and willing to pay high ransoms.

Ransomware actors often look for targets with strong revenues that are in a financial position to pay high ransoms. This motivation makes manufacturing companies attractive targets for ransomware gangs.

Hackers can also assume that manufacturing companies are more inclined to pay ransoms, as they have a low tolerance for downtime due to the potential financial losses involved in a shutdown caused by a ransomware attack.

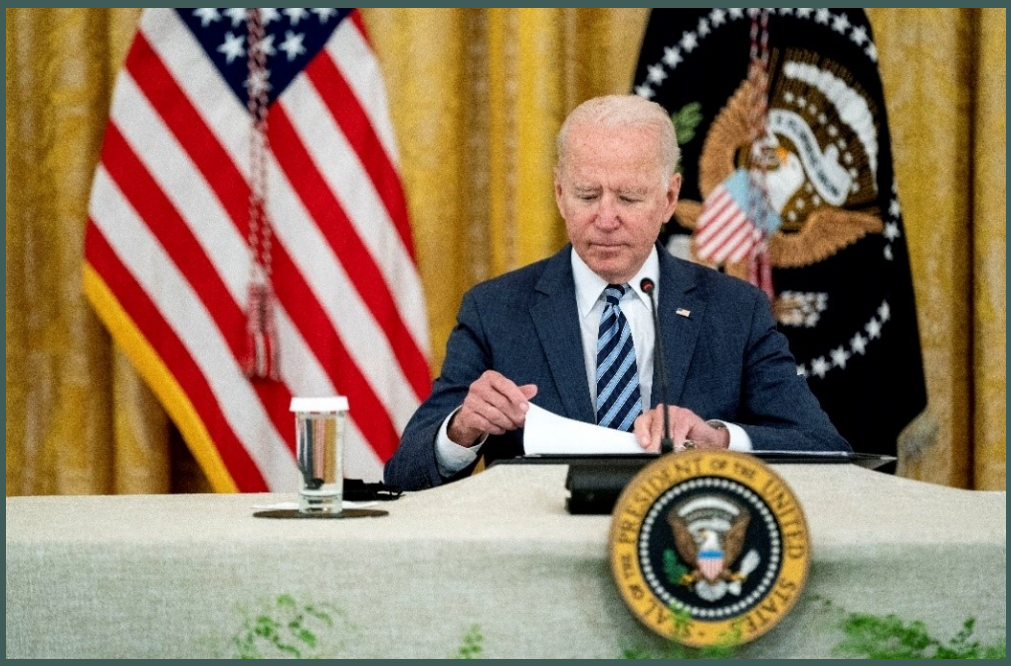

*Photo: Pool/Shutterstock/Ritzau Scanpix*

### United States: Increased focus on the threat of ransomware

Following the 2021 ransomware attacks against the Colonial Pipeline oil company and global food company JBS Foods, US authorities ramped up efforts against the threat from ransomware actors. Ransomware attacks can now be investigated as a threat to national security on a par with the threat from terrorism.

The efforts against cyber crime remain a priority to US authorities. In late August 2023, the FBI conducted an internationally coordinated operation against the Qakbot malware variant. Qakbot was often used in ransomware attacks for the exfiltration of victim data. Access to units compromised with Qakbot malware was traded extensively on criminal forums.

# Ransomware attacks can potentially impact operational processes

IT and OT systems (operational technology) are often connected in modern production environments to meet the demand for a given product. At the same time, the sharing of data between different systems in the production line increases the companies' attack surface. This makes the companies more vulnerable to ransomware attacks impacting their production operation and thus their core business.

While ransomware is typically designed to encrypt traditional IT infrastructure, attacks can still impact company OT assets. Encryption as a result of a ransomware attack can impact the IT systems controlling company OT assets, resulting in downtime without the attack directly targeting OT assets.

Ransomware attacks can also result in downtime because the companies themselves choose to shut down systems controlling the manufacturing process. This is typically the case if the company fears that the hackers are able to move laterally inside the company's IT network. A self-induced shutdown was, for instance, used as a security measure when Norsk Hydro, a manufacturer of products such as aluminium, was hit by an attack in 2019, and in the February 2023 attack on Dole Food Company.

Regardless of whether a shutdown occurs as a result of the ransomware itself or as a preventative security measure taken by the company, the financial consequences can be significant.

**Self-induced shutdowns in response to ransomware attacks**

Norsk Hydro, one of the leading global aluminium manufacturers, fell victim to a ransomware attack against the company's IT systems. As a preventative security measure, Norsk Hydro decided to shut down production and forcibly switch over to manual production. The attack cost Norsk Hydro close to an estimated DKK 500 million.

On 22 February 2023, the Dole Food Company announced that it had fallen victim to a ransomware attack. In response to the attack, Dole temporarily shut down several of its factories in North America, and put all distribution on pause. As a result, some US super-markets were out of stock on specific Dole products for more than a week after the attack.

# RaaS groups can use different extortion methods in the hunt for ransoms

While run-of-the-mill ransomware attacks include the encryption of data and systems, some RaaS groups have developed the attack method further. One such example is the Karakurt cyber criminal group that steals victim data but does not encrypt data or systems. After stealing the data, the group threatens to leak or sell the stolen data unless the ransom is paid. Requiring less work and fewer technical skills, data theft and extortion without encryption can be an attractive method for RaaS groups.

Even though companies that fall victim to such an attack will avoid the perils of a sudden shutdown, leaked data still has the potential to harm the company. Exfiltrated data may contain sensitive personal data, sensitive customer data or trade secrets that can damage the company's competitive position or reputation if leaked or sold. While encrypted data can be restored from a good backup, there is usually nothing that can be done if data has been exfiltrated from the company's systems. In addition, it can be necessary to shut down parts of the production to cut off hackers' access to company systems.

**Public shaming as a tool for extortion**
In contrast to the more traditional criminal methods, in which criminals most often try to avoid detection, organized RaaS groups often announce their attacks very directly to their victims and, at times, to the outside world. The groups typically use two methods for this approach:

The first method is implemented at the final stage of the ransomware attack after the encryption or theft of the victim's systems or data. A this stage, hackers often leave a note with instructions and ransom demands. Some RaaS groups leave instructions for the victim on how to communicate directly with them.

The second and more public way for the hackers to announce an attack is through their Dedicated Leak Site (DLS), which is a website controlled by the ransomware actors dedicated to publication of victim data. If a company refuses to pay the ransom or fails to meet the deadline for payment, the next step for several ransomware groups is to publish the name of the company on their DLS. If the hackers have stolen data, they can also choose to leak the data simultaneously, the motive being to expose the victim as a way of scaring future victims into paying the ransom asked. DLS is also known as a *victim shaming blog*.

Public shaming is a useful tool for criminal actors, as it can be harmful to a company's reputation and business if it is made public that it has fallen victim to a ransomware attack. In addition, leak of sensitive customer or staff information can make the company liable to fines.

## Ransomware actors are creative in their efforts to shame victims into paying ransoms

Criminal actors will go to great lengths to put pressure on companies to pay for the release of the encrypted and/or stolen data.

One such example is an ALPHV RaaS group affiliate which following a ransomware attack posted a comment on a victim's LinkedIn post containing some of the exfiltrated data. The link in the comment was accompanied by a threat to publish the remainder of the stolen data if the victim failed to contact the group to negotiate a ransom.

RaaS groups have also been known to call and threaten staff, initiate remote printing of ransom notes on printers in the compromised network, and threaten to conduct Distributed Denial-of-Service (DDoS) attacks against victim websites as part of their extortion strategy.

# Threat levels

The Danish Defence Intelligence Services uses the following threat levels.

| | |
|---|---|
| **NONE** | There are no signs of a threat. There are no actors with both the capacity and intention for attacks/harmful activity. |
| **LOW** | There are one or more actors with the capacity and intention for attacks/harmful activity. However, either the capacity or the intention or both are limited. |
| **MEDIUM** | There are one or more actors with the capacity and intention for attacks/harmful activity. However, there are no indications of specific planning of attacks/harmful activity. |
| **HIGH** | There are one or more actors that have the capacity for and are specifically planning attacks/harmful activity or that have already |
| **VERY HIGH** | There is either information that one or more actors are initiating attacks/harmful activity, including information about time and target, or that one or more actors are continuously initiating attacks/harmful activity |

*An applied threat level reflects the DDIS's assessment of the intention, capacity and activity of one or more actors based on the available information.*