CENTRE FOR CYBER SECURITY

THREAT ASSESSMENT

Criminals tighten the digital thumbscrew

DECEMBER 2020

Indhold

CENTRE FOR
CYBER SECURITY

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

1st edition December 2020.

Criminals tighten the digital thumbscrew

This threat assessment informs Danish public authority and private company decision-makers of the threat from so-called double extortion in which hackers threaten to leak information stolen in connection with ransomware attacks.

Key assessment

- Targeted ransomware attacks in which cyber criminals extort public authorities and private companies for large sums of money by encrypting data on vital IT systems are part of the threat landscape, also against Danish public authorities and private companies.

- Since the autumn of 2019, criminal hackers have expanded their extortion tactics, threatening to leak or sell sensitive information stolen in connection with ransomware attacks. Ransomware attacks combined with threats of data leak are called double extortion.

- The double extortion technique was first seen used in the United States. However, in September 2020 a Danish company fell victim to extortion, proving that Danish public authorities and private companies may also become victim to such attacks.

- Double extortion not only poses a very significant threat to the public authorities and private companies falling victim to ransomware attacks; it also threatens the clients, partners and citizens whose sensitive information is at risk of being leaked or sold.

Analysis: Double extortion is a new normal

In recent years, targeted ransomware attacks, in which criminals extort public authorities and private companies for large sums of money by encrypting data on essential IT systems, have spread to be a global phenomenon. Since 2019, there have been multiple victims of targeted ransomware attacks in Denmark.

The threat of targeted ransomware attacks has in recent years taken on a new dimension. Since the autumn of 2019, criminal hackers have expanded their extortion tactics in connection with targeted ransomware attacks to include threats from leaks or sales of sensitive information stolen in connection with the attack. This attack technique is known as double extortion in IT security vernacular.

The hackers behind the Maze ransomware launched a new trend by introducing the attack technique in 2019 with other criminal hackers soon copying the technique. Today, hackers behind most targeted ransomware attacks engage in this type of extortion.

Initially, double extortion attacks targeted public authorities and private companies in the United States, but have evolved to become a global phenomenon. Extortion against a Danish private company in September 2020 has demonstrated that Danish public authorities and private companies may also become targets of double extortion attacks.

Double extortion ransomware attacks allow cyber criminals to maximize their financial gain, placing new demands on Danish public authority and private company preparedness for such attacks.

Today, many public authorities and private companies have implemented back-up procedures for system restoration in preparation of ransomware attacks, making them less inclined to pay ransom to regain access to their IT systems.

However, cyber criminals can still make money from stolen information in connection with the ransomware attack, either by extorting money from the victim in exchange for not leaking the information, or by selling it to other criminals or interested parties.

Though leak of information in itself is no money-spinner for criminals, it serves the purpose of making the threat visible to other victims and putting pressure on future victims.

Hackers step up the pressure by threatening with damaging leaks

This type of extortion involves hackers threatening to sell or leak stolen information on special websites, so-called leak sites. Though such websites are broadly available to the public, they often require visitors to access the site via the TOR anonymization browser software.

On the websites, the hackers write about their victims and show examples of stolen documents, etc. On some of the sites, it is possible to bid on data put up for auction. Ransom amounts for stolen data vary significantly. The highest ransom the CFCS has observed so far is USD 42 million for information stolen from a law firm whose clients include famous musicians.

Hackers exploit the fact that leak of sensitive information could prove very harmful to the victim.

Data on hacker leak sites typically contain sensitive personal and customer information such as emails and information about the employees and customers. Leak of such information may prove damaging to the company itself, its employees and its clients. In addition to reputational damage, data leaks may also result in the victims being fined for violation of personal data protection regulations. Some hackers even mention violation of the General Data Protection Regulation (GDPR) as part of their extortion tactics.

There are also examples of intellectual property leaks, such as source code from software companies and technical descriptions from production companies. Leaks of this type of information may damage the companies' competitiveness and business foundation.

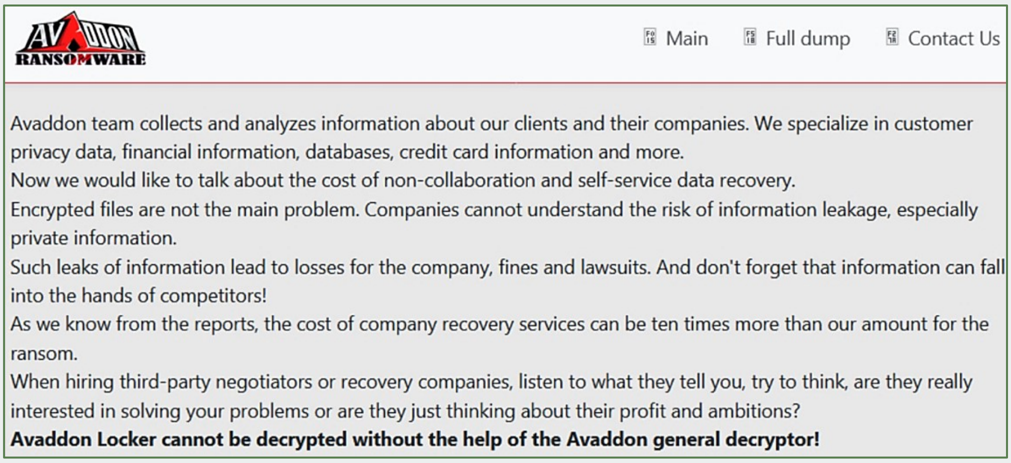
The public exposure has moved the often discrete ransom negotiations between victim and attacker into the public spotlight. Criminal hackers try to use this exposure as an entry point for keeping up the negative focus and pressure on their victims.

Hackers: We are the responsible ones

There are several examples of ransomware hackers referring to themselves as responsible hackers or IT specialists, who just want to charge a fee for identifying security vulnerabilities in the victims' systems. The victims are often not referred to as victims but rather as clients or partners.

Victims who refuse to pay ransom are labelled as irresponsible or greedy, whereas the tone against victims willing to discuss payment is positive. Some hackers initiate negotiations by offering reductions in ransom demands, for instance in the form of ”Corona discounts”.

This narrative is likely aimed at convincing their victims that on the one hand, the hackers are professional enough to provide access to the encrypted IT systems if the victims pay; however, on the other hand, they are also ready to leak stolen data if their terms are not met, placing responsibility for the leak on the victims.



Avaddon team collects and analyzes information about our clients and their companies. We specialize in customer privacy data, financial information, databases, credit card information and more.
Now we would like to talk about the cost of non-collaboration and self-service data recovery.
Encrypted files are not the main problem. Companies cannot understand the risk of information leakage, especially private information.
Such leaks of information lead to losses for the company, fines and lawsuits. And don't forget that information can fall into the hands of competitors!
As we know from the reports, the cost of company recovery services can be ten times more than our amount for the ransom.
When hiring third-party negotiators or recovery companies, listen to what they tell you, try to think, are they really interested in solving your problems or are they just thinking about their profit and ambitions?
Avaddon Locker cannot be decrypted without the help of the Avaddon general decryptor!

Hackers behind the Avaddon ransomware describe who they are and threaten their victims on the "Avaddon Info" page (screen dump).

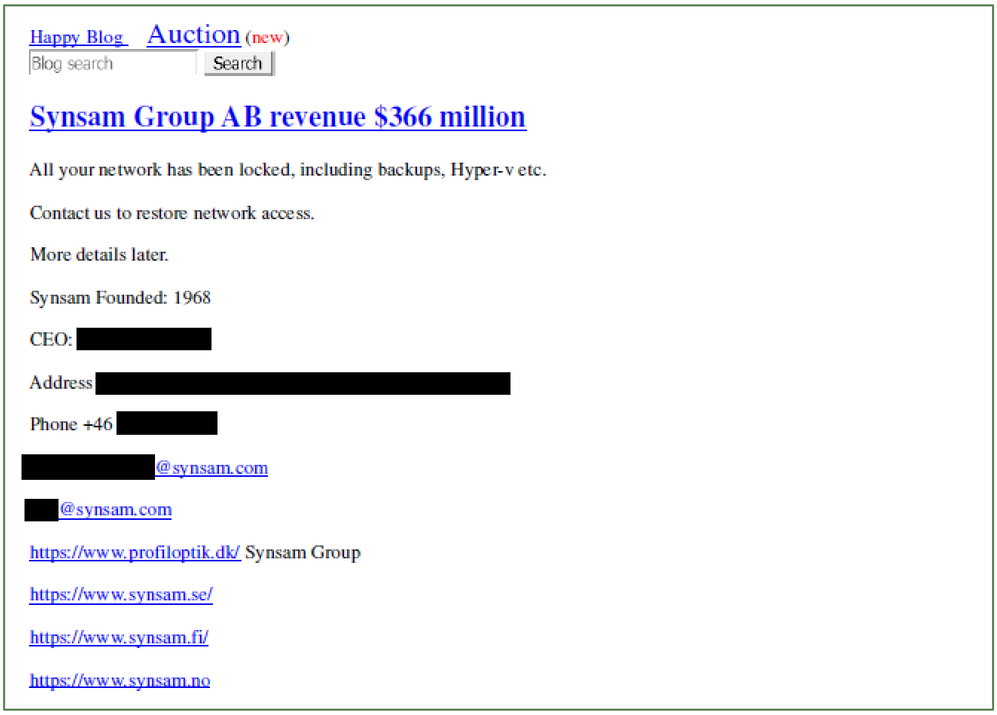
In order to strengthen the narrative that they are responsible and professional, some groups are even trying to forestall negative media coverage on their attacks. A case in point is the pledge by Maze ransomware hackers to leave hospitals alone during the COVID-19 pandemic. Other groups have since made similar promises. However, since the outbreak of the pandemic, there have been several examples of targeted ransomware attacks on the healthcare sector abroad.

A new and significant threat that is also directed against Denmark

Double extortion attacks not only pose a very significant threat to the public authorities and private companies targeted in the attacks. They also pose a threat to affiliated customers and partners as well as citizens who risk that business or sensitive personal information is exposed to the public or sold to criminal networks.

It is important that Danish public authorities and private companies take the threat from leaks and sale of confidential information into account when implementing preventive measures against ransomware attacks. They should address attacks directed against their own organization as well as leaks of any sensitive information from the organization that may be stored with suppliers, partners or authorities that become targets of ransomware attacks.

In September 2020, the hackers behind the ”Happy Blog” site claimed that they had attacked the Nordic optical retailer chain Synsam Group, which includes the Danish retailer Profil Optik. The incident showed that Danish public authorities and private companies may also become victims to this type of extortion.



Synsam Group AB revenue $366 million

All your network has been locked, including backups, Hyper-v etc.

Contact us to restore network access.

More details later.

Synsam Founded: 1968

CEO: [redacted]

Address [redacted]

Phone +46 [redacted]

[redacted]@synsam.com

[redacted]@synsam.com

https://www.profiloptik.dk/ Synsam Group

https://www.synsam.se/

https://www.synsam.fi/

https://www.synsam.no

Synsam Group featured on the "Happy Blog" leak site
(screen dump, contact and personal information has been removed by the CFCS)

For more information on the threat from targeted ransomware attacks and preventive measures against ransomware visit the CFCS website.

Below is the scale of probability the DDIS applies

Highly unlikely
Less likely
Possible
Likely
Highly likely