CENTRE FOR
CYBER SECURITY

Threat assessment: The cyber threat against the Danish telecommunications sector

Danish Defence Intelligence Service
Kastellet 30
DK-2100 Copenhagen

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

1st edition. October 2019.

This threat assessment outlines existing cyber threats to the Danish telecommunications sector. The Danish telecommunications sector is of vital importance to the functioning, stability and security of society. The threat assessment can be included in the risk assessment for companies in the telecommunications sector.

Key Assessment

- The threat of cyber crime against the Danish telecommunications sector is **VERY HIGH**. Cyber criminals primarily pose a threat to the business of the telecom providers, but they may also compromise the telecommunications infrastructure in their efforts to target telecom customers. Cyber crime may affect the availability of telecom services.
- The threat of cyber espionage against the telecommunications sector is **HIGH**. The purpose is to collect information on the telecom providers and the telecom infrastructure as well as their subscribers and subscribers' communication. It is less likely that cyber espionage will affect the accessibility of telecom services.
- The threat of cyber activism against the telecommunications sector is **MEDIUM**. Telecom-related issues discussed in the public debate may draw the attention of cyber activists, raising the possibility of cyber activism against the telecommunications sector.
- The threat of cyber terrorism against the telecommunications sector is **LOW**. CFCS assesses that even though militant extremists have occasionally expressed an interest in conducting cyber terrorism, they currently lack the capabilities to do so.
- It is less likely that foreign states will launch destructive cyber attacks against critical infrastructure in Denmark, including the telecommunications sector. However, the telecommunications sector may become a collateral victim of destructive cyber attacks against targets outside of Denmark.
- DDoS attacks still pose a serious threat to the accessibility of telecommunications services.

Introduction

This threat assessment describes the cyber threats against the Danish telecommunications sector and has been prepared by the Threat Assessment Unit under the DDIS Centre for Cyber Security (CFCS). This threat assessment replaces the previous assessment from February 2017.

The threat assessment outlines the cyber threats that may disturb the availability, integrity or confidentiality of the telecom services or damage the business of telecom service providers. From a societal perspective, the threats against the availability of telecom services are the most severe threats.

In this assessment the Danish telecommunications sector is defined as the commercial service providers that publicly provide the telecom services and infrastructure that allow public authorities, private companies and citizens to communicate electronically via fixed and mobile networks.

This threat assessment is based on the current threat landscape and operates with a warning horizon of 0-2 years. As cyber threats are dynamic in nature the threat landscape may suddenly change, both in general and in relation to the individual organization. The threat and probability levels applied in this threat assessment are defined at the end of the report.

What are cyber threats

CFCS defines cyber threats as malicious attempts by an actor who is using IT to cause disruptions or gain unauthorized access to data, systems, digital networks or digital services.

Cyber threats are multi-faceted. In this threat assessment CFCS assesses the threat based on the motivation behind the cyber attack as well as focus on individual attack techniques.

The threat levels are based on an analysis of the actors' intent and cyber capabilities. CFCS' assessment of an actor's cyber capability is based on its available human and material resources, ranging from technically skilled hackers, developers of malware and information on targets to IT infrastructure, time, funds and access to information.

Cyber crime

The threat of cyber crime against the Danish telecommunications sector is **VERY HIGH**. Danish telecom companies are thus highly likely to be exposed to attempted cyber crime.

Cyber crime is financially motivated. Most cyber crime against the telecommunications sector is not targeted specifically against the sector, but is caused by cyber criminals targeting a wide array of sectors across society.

The threat is complex, and cyber criminals employ a wide range of criminal activities. For example, telecom companies have to battle persistent forms of cyber crime launched by criminals targeting as many victims as possible in a bid to maximise their financial gain as well as tailored and advanced attacks by hacker groups against a few selected targets.

In addition, the telecommunications sector is exposed to the threat from advanced hacker groups trying to compromise the telecom infrastructure in a bid to affect customers and other mobile phone network and Internet subscribers. This type of compromise may affect the availability, confidentiality or integrity of telecom services.

Cyber criminals employ common hacking techniques and exploit well-known vulnerabilities, but are also quick to identify new vulnerabilities and develop new exploits and techniques.

Cyber criminals compromise client accounts and self-service solutions

Telecom providers often offer self-service solutions that allow private customers to administer their Internet- or mobile phone subscriptions, email services and movie and music streaming services. Self-service solutions are also available to business customers, allowing them to administer company mobile phone subscriptions, among other things.

Self-service solutions are attractive targets for cyber criminals, and cyber criminals will likely make efforts to gain access to them in order to resell credentials for streaming services or gain access to client data, usernames and passwords or email accounts that could be useful in future cyber attacks.

Stofa client accounts compromised

In September 2018, Danish provider Stofa temporarily suspended customers access to its self-service solution, because outsiders had gained access to approx. 2,000 customer accounts.

There have been examples abroad where cyber criminals have compromised customer accounts in order to hijack specific customers' mobile phone numbers. By hijacking a customer's phone number, cyber criminals gain access to any SMS text messages sent to the customer including messages containing two-factor authentication codes protecting access to online accounts like banking or webmail services. If the cyber criminals already know the username and password for such an account, intercepting the two-factor authentication code will grant them full access to the online service. Access to the self-service solution can allow cyber criminals to trick the telecom service provider into sending the customer a new SIM card, which can be intercepted by the criminals. In 2017, cyber criminals managed to gain access to hundreds of US T-Mobile customer accounts with the aim of hijacking customer phone numbers. It is likely that cyber criminals will make efforts to bypass security measures of Danish telecom providers with the aim of hijacking selected customer phone numbers.

Over the next few years, physical SIM cards will gradually be replaced by digital SIM cards, also called eSIM, which customers will download from their telecom provider and install on a chip on their mobile device. Certain telecom providers in Denmark already offer eSIM to customers using mobile devices that support the technology. CFCS assesses that cyber criminals will make efforts to look for holes in the security of eSIM as well as the ordering and delivery of procedures for eSIM, among other things for the purpose of hijacking customer phone numbers.

Cyber criminals try to exploit vulnerabilities in the SS7 network

One sophisticated method to intercept SMS text messages is to compromise the so-called SS7 network, which is used for interconnecting mobile networks worldwide, and redirecting specific customers' text messages to cyber criminals. The method was used in 2018 against British Metro Bank customers. Similarly, in April 2017, cyber criminals intercepted text messages containing two-factor authentication codes sent to a number of O2-telefonica customers in Germany trying to access their bank accounts.

It requires special knowledge to gain access to, and especially to compromise the SS7 network. CFCS assesses that only a few cyber criminal groups have the skills required. However, the risk exists that criminals who might be able to gain access decide to make their access available to other criminals for a fee.

Telecom infrastructure may be compromised in a bid to redirect user traffic to criminals

Advanced hacker groups exist that are trying to redirect Internet traffic to fake websites in order to steal passwords for digital services, spread malware or display ads that generate revenue to the criminals. Even though the users of the Internet are the ultimate victims, the attack is mainly directed against telecommunications infrastructure or key Internet services in the telecommunications sector.

So-called BGP hijacking can be used to reroute large amounts of Internet traffic to cyber criminals. The BGPStream.com website, which monitors BGP routing on the Internet, has registered some 200 potential BGP hijacks every month since 2016. In April 2018, foreign cyber criminals managed to steal cryptocurrency by means of BGP hijacking that redirected users of the service MyEtherWallet.com to a fake login page.

BGP hijacking

Is a malicious corruption of routing data in a so-called Border Gateway Protocol (BGP) router. BGP routers are used to connect the many networks that together make up the Internet. The router informs adjacent networks which IP addresses can be reached from the network.

Only few cyber criminals have the skills required to launch a BGP hijack, but due to the structure of the Internet, a BGP hijack may affect Danish Internet users irrespective of the geographic origin of the attack. BGP hijacks may have serious repercussions if a Danish telecom provider fails to filter the incorrect BGP routing information originating from or spread to adjacent networks. In addition to rerouting Internet traffic, a BGP hijack has the potential to slow down or even interrupt part of the internet traffic. Without effective monitoring of changes in the BGP routing, a BGP hijack, which does not generate traffic disruptions, may potentially last for days or weeks.

DNS servers
A DNS server contains information on webpages and their associated IP addresses. Internet browsers use the information when a user wants to access a website.

The compromise of an Internet Service Providers' (ISP) DNS servers may redirect customers to false websites. This could happen if cyber criminals gain unauthorized access to the server or if cyber criminals manage to alter or forge the data sent to and stored in the ISP's DNS server from other DNS servers on the Internet.

The threat has prompted an increasing number of websites to use DNSSEC, which is aimed at ensuring validity of the DNS query. However, on a global scale, less than 2.5 % of websites use DNSSEC.

Cyber criminals also target home routers, configuring them to use DNS servers controlled by criminals in order to redirect the users to false websites. In the summer of 2018, cyber criminals infected over 100,000 home routers in Brazil. The objective was to redirect users to a clone website of the Brazilian bank Banco de Brazil.

Customer equipment like home routers connecting the users' home network to the telecom infrastructure are not usually considered part of the telecom provider infrastructure. However, with respect to private customers, in particular, the equipment is often supplied and administered by the telecom provider.

Ransomware may threaten telecom services

Ransomware attacks are still prevalent, and companies in the Danish telecommunications sector are likely to fall victim to ransomware attacks. There are indications that the number of simple ransomware attacks has declined, while the number of targeted and advanced attacks has grown. This may imply that the risk of being hit by ransomware attacks has diminished, while better protection is required to defend against ransomware attacks.

Ransomware may be particularly harmful as it has repeatedly been used to paralyze parts of a company's administrative network or even the entire network, affecting the operational capability of the company. This happened to the Norwegian company Hydro when it was hit by a ransomware attack in March 2019. In 2017, the widespread Wannacry ransomware attack hit Spanish telecom provider Telefónica, paralyzing computers in its administrative network.

The attack on Telefónica did not affect telecom services. However, that might have been the case if key network functions like Domain Controller and Active Directory, which control the computers and employee access to the company network, had been hit by the attack. That would have locked employees out of the company's domain and prevented access, including remote access, to the telecom infrastructure and the tools controlling it.

Telecom services may also be affected if ransomware against administrative networks affect IT systems or databases supporting the telecom services, or if ransomware spreads to the management network used to configure and control the telecom infrastructure or spreads to the telecom infrastructure itself. The ransomware used in the attack on Hydro was programmed to encrypt database files.

Malware encrypting data, disguised as ransomware, can also be used for destructive purposes. A.P. Moller-Maersk was one of several companies worldwide that was compromised by the so-called NotPetya attack that originated in Ukraine in 2017. This attack was a testament to how cyber attacks can spread inside a company across national borders.

The telecommunications sector is susceptible to data theft, cryptomining malware and BEC scams

Internet-enabled data theft is a widespread phenomenon, and the telecommunications sector is not immune to this type of attack. Cyber criminals are looking to steal data and personal information that they can sell or otherwise exploit. Stolen data could also be used to blackmail the telecom provider into paying ransom in exchange for not disclosing the stolen data. Unlike ransomware, data theft may be difficult to detect unless the cyber criminals draw attention to the theft e.g. by attempting extortion.

Data theft against the telecommunications sector

In 2017, Danish telecom company ”3” was exposed to extortion attempts by cyber criminals threatening to publish customer data stolen from the company. However, the company managed to resolve the case without paying the cyber criminals.

In 2017, customer data was stolen from Swisscom in Switzerland due to a compromise of a sales partner's access to costumer data, emphasizing the risk that subcontractors may become points of entry for cyber crime.

Even though the value of cryptocurrency has dropped since its peak in 2018, it is still a popular target among cyber criminals who want to mine cryptocurrency without having to invest in the necessary hardware themselves. Consequently, a telecom provider's website or office network units may become infected by cryptmining malware. If the malware finds its way to equipment in the management network or telecom infrastructure, it could potentially tap into the computing power of critical network components. However, CFCS assesses it to be less likely that cryptocurrency mining malware will affect the telecom services.

The telecommunications sector is still faced with a threat from BEC scams.
The aim of BEC scams is to trick money from private companies and public authorities via fraudulent emails instructing the victim to transfer money to the perpetrator. The technique has become quite popular among cyber criminals as it does not necessarily require sophisticated IT skills. A BEC scam does not affect the telecom services directly.

An increasing number of companies in the telecommunications sector use office tools and email solutions provided as cloud computing services. As cyber criminals are eager to gain access to email accounts in order to exploit the content, send credible phishing emails or use the information in a future BEC scam, cyber criminals will highly likely target such solutions by means of phishing emails containing links to fake login sites, or by trying to guess the correct username and password. Solutions that do not have two-factor authentication are particularly vulnerable to this type of attack.

Cyber espionage

The threat of cyber espionage against the Danish telecommunications sector is **HIGH**. Companies in the telecommunications sector will likely become targets of cyber espionage.

The general threat level of cyber espionage against Denmark is **VERY HIGH**. CFCS assesses that even though foreign states have the intent and capability to conduct cyber espionage against the Danish telecommunications sector, the espionage activity level against the telecommunications sector is not as high as the activity level against some other sectors.

CFCS regularly detects cyber espionage attempts against public authorities and private companies in Denmark. Cyber espionage is aimed at collecting information that holds strategic, security political and economic importance to the attacker. Danish public authorities and institutions engaged in foreign and defence politics, as well as companies important to society and private research-heavy companies are particularly susceptible to cyber espionage.

The Danish telecommunications sector may become a target of cyber espionage as it supplies the telecom infrastructure and telecom services to the organizations mentioned above. There have been examples abroad where state-sponsored actors have compromised telecom providers in order to monitor communication or gain access to call data and SMS text messages. The tools and network units in the telecom infrastructure that allow access to communication are prized targets for an attacker.

Cyber espionage against the telecommunications sector may be used to map the IT or telecom infrastructure. Knowledge of the type of hardware or software used by the victim might facilitate a network compromise as such knowledge would allow an advanced actor to acquire identical equipment and identify so far unknown vulnerabilities that could be used in a future cyber attack.

Telecom infrastructure and customer equipment may serve as a platform for cyber espionage against telecom customers

Below is a number of examples of techniques that CFCS believes states have used against the telecommunications sector abroad with the aim of spying against telecom service users.

The BGP hijacks and cyber attacks on DNS servers mentioned in the section on cyber crime could also be used for cyber espionage purposes. By rerouting Internet traffic to a network or server to which the attacker has access, communication may be monitored before it is transmitted to the original destination. Suspicious BGP changes that reroute Internet traffic to networks in countries which CFCS believe have the capability to conduct cyber espionage are registered regularly, and it is possible that state-sponsored actors are using BGP hijacking or DNS server compromises as a platform for cyber espionage.

A state-sponsored actor may be looking for a way to gain access to the content of specific individuals' SMS text messages. CFCS assesses it highly likely that there are foreign states that have the capabilities to compromise the telecom infrastructure by means of malware designed to intercept and forward the content of SMS text messages to and from selected mobile phone numbers.

Also, there are states trying to spy against mobile phone subscribers by compromising the before-mentioned SS7 network. Weaknesses in the SS7 network design may be exploited by state-sponsored actors to monitor and listen in on the conversations of mobile network users domestically and abroad. CFCS assesses it highly likely that there are foreign states which attempt to use the SS7 network for espionage purposes.

The previously mentioned home routers that connect the telecom provider's infrastructure with the customer's own network may likewise serve as a platform to spy against telecom customers. For example, in May 2018, US authorities issued a warning that thousands of vulnerable home computers across the world had been infected by the VPNFilter malware. The malware, which also affected home routers in Denmark, may be used to monitor network traffic, thereby threatening the confidentiality of Internet communication.

Telecommunications subcontractors may become entry points for cyber espionage

As the Danish telecommunications sector uses subcontractors and outsources different service tasks, it is exposed to threats of cyber attacks against their supply chain. Subcontractors are prized targets as they may serve as a platform to gain access to multiple targets at once and may even have lower security requirements than the end target. In April 2017, the US-CERT issued the TA17-117A alert about ongoing cyber attacks against managed service providers in Norway, Sweden and Finland, among others. The goal was to spy against managed service customers, including telecom service providers. CFCS have no information that Danish telecom providers were affected by this cyber attack.

If an actor compromises the hardware or software from subcontractors, service providers may inadvertently install malware on their network.

In March 2019, it was revealed that unknown actors had compromised servers at ASUS containing software updates for their laptops and in 2017, infected CCleaner software from the company Piriform was downloaded more than two million times before the compromise was detected. An investigation into the incident demonstrated that the telecommunications sector, among others, was the target of the attack. CCleaner is widely used in Denmark, including in parts of the telecommunications sector.

Practically all types of software contain vulnerabilities that may potentially be exploited by an attacker. Thus, it is vital to ensure that subcontractors continuously maintain their products, regularly issue security updates and ensure that these updates are installed. If an attacker learns about the vulnerabilities before the subcontractor issues a security update or if the subcontractor is unable to issue security updates, the product in question may pose an even greater vulnerability over time. For instance, in May 2019, the US Bureau of Industry and Security (BIS) issued a list of entities that US companies are not allowed to export to without authorization from BIS. Chinese company Huawei has been added to the entity list. If enacted, the ban may in the short term prevent Huawei from delivering new products and issuing security updates which contain hardware or software supplied by US companies.

Not all cyber espionage attacks are sophisticated

Even though several foreign states hold advanced cyber espionage capabilities, they often use less sophisticated techniques and known vulnerabilities –which are also popular tools of choice among cyber criminals. Thus, a compromise, no matter how insignificant it seems, is a sign that a weakness exists that may potentially be exploited more efficiently by an advanced opponent.

Watering hole attacks

In a watering hole attack the attacker seeks to compromise one or several targets by infecting a legitimate website that the targets are expected to visit.

Simple techniques are often sufficient and they effectively disguise cyber espionage efforts and reduce the risk of exposing advanced hacker tools and so far unknown vulnerabilities. Phishing, social engineering and watering hole attacks are common techniques used in cyber espionage campaigns and cyber crime.

Technical staff in IT and security departments are alluring social engineering targets, as they often have administrative rights and access rights to the network and network utilities that the attacker may use in a future cyber attack against the organization.

Cyber activism

The threat of cyber activism against the Danish telecommunications sector is **MEDIUM**.

There have been examples of cyber activism against the telecommunications sector abroad, but CFCS assesses that cyber activists in general do not have focus on the Danish telecommunications sector. However, some hacker groups and cyber activist network members have the capabilities and resources to carry out cyber attacks. The threat level may thus suddenly increase, should companies in the Danish telecommunications sector for some reason land in the crosshairs of cyber activists.

The aim of cyber activism is to draw as much attention as possible to a specific cause and promote a political message. Consequently, social media is often used as a platform to warn of future attacks or call for attacks. Similarly, traditional political activism often goes hand in hand with cyber activism.

Cyber activism against CAT Telecom
In 2015, the activist group Anonymous was responsible for leaking data and launching a number of DDoS attacks against Thai telecom company CAT Telecom. The attacks were allegedly launched as a response to Thailand's plans to monitor Internet traffic in the country.

DDoS attacks against telecom providers in Sudan
At the end of 2018, Anonymous claimed responsibility for a number of DDoS attacks against telecom providers and authorities in Sudan. The attacks were motivated by the Sudanese government's introduction of laws restricting citizens' access to the Internet.

Cyber activists use a variety of techniques ranging from DDoS attacks to defacement attacks in which hacked websites and social media profiles are defaced with political messages. Another technique includes hacks and leaks of emails, for example, which could be used to paint the victim in a negative light.

Cyber activism against the telecommunications sector abroad has often been motivated by the fight for a free and open Internet. Though cyber activists have primarily targeted authorities that have introduced monitoring mechanisms or laws restricting citizens' access to the Internet, telecom providers forced to implement authority decisions have also been targeted.

Support for a free and open Internet has also been a topic in the public debate in Denmark. Issues such as net neutrality, legislation on telecom traffic monitoring and steps against illegal streaming services have been debated in public. Discussions on similar topics have previously resulted in cyber activism against political targets in Denmark. Currently, the upcoming 5G technology has caused debate on whether or not the technology is harmful to the environment.

Cyber terrorism
The threat of cyber terrorism against the Danish telecommunications sector is **LOW**.

CFCS assesses that even though militant extremists have on a few occasions expressed an interest in conducting cyber terrorism, they currently lack the capabilities for doing so. At present, they are only capable of conducting simple cyber attacks aimed at promoting and disseminating propaganda for ISIL and other militant extremist groups. Consequently, the threat of cyber attacks against Denmark aimed at obtaining the same effect as conventional terrorism, such as cyber attacks causing personal injury or extensive disruptions of critical infrastructure like the telecom infrastructure, is low.

Destructive cyber attacks

A number of countries are developing cyber capabilities that can be used in destructive cyber attacks against critical infrastructure like the telecom infrastructure, for example.

CFCS assesses it less likely that foreign states will launch destructive attacks against critical Danish infrastructure in the short term, including the telecommunications sector. However, the threat level may increase should Denmark find itself embroiled in political or military conflict with countries that have access to destructive cyber attack capabilities.

Destructive cyber attacks against targets outside of Denmark may end up having spill-over effects on Danish telecom providers, especially on those operating in countries such as Saudi Arabia, South Korea and Ukraine where foreign countries are believed to have launched destructive cyber attacks.

A targeted destructive cyber attack against a telecom provider requires detailed knowledge of the provider’s IT and telecom infrastructure. This knowledge may be obtained by means of cyber espionage, which in turn may indicate that a potential future destructive cyber attack is under preparation.

The telecommunications sector supports an increasing number of digital solutions connecting the digital and physical world. The upcoming 5G mobile technology is expected to contribute to further increase this connectivity, raising the risk in the medium term that a serious cyber attack against the Danish telecommunications sector could cause physical damage.

DDoS attacks

The Danish telecommunications sector is highly exposed to DDoS attacks, also known as overload attacks, which will be dealt with below.

DDoS attacks are a popular tool among malicious actors as they are easy to conduct. Motivation for DDoS attacks may range from excitement, extortion, harassment against a competitor or opponent over concealment of another cyber attack to disruption of online services.

The telecommunications sector is particularly exposed to DDoS attacks as any DDoS attack passes through telecom infrastructure on its way to the target, which may lead to the overload of the infrastructure, resulting in degradation or disruption in telecom services. Examples of vulnerable network components include routers, firewalls and Carrier Grade Network Address Translation (CGNAT) equipment. The latter enables the provider to share public IP addresses between multiple customers, raising the risk that a DDoS attack against a specific IP address may affect several customers.

Competitor orders a DDoS attack against rival telecom provider in Liberia

In January 2019, a British citizen was convicted of launching a powerful 500 Gbit/s DDoS attack against Liberia’s biggest telecom company Lonestar MTN. The attack was ordered and paid for by a competing telecom provider.

The same individual was convicted in Germany in 2017 of having created the botnet that was used in this and other attacks. The botnet consisted of units infected by the Mirai malware. An attempt to include home routers in the botnet prevented 900,000 Deutsche Telecom customers from connecting to the Internet in 2016.

Very powerful DDoS attacks may affect key functions in the provider’s network, ultimately affecting numerous customers. In 2017 and 2018, customers with Ålcom, a provider in the Finnish autonomy Åland, experienced disruption or degradation in services due to a number of DDoS attacks launched against other customers using the same telecom infrastructure.

Like other websites, the websites of telecom providers may be exposed to DDoS attacks. In addition to blocking access to the website, the attack may cause disruption in services delivered via the website or the network in which the targeted web server belongs.

Unlike the main part of the telecom infrastructure, the providers’ customer-directed DNS servers have public IP addresses and may thus become targets of a DDoS attack. A successful attack may imply that the provider’s customers will have difficulty accessing websites or online services.

The number and magnitude of registered DDoS attacks vary over time, but are generally at a high level. IT security companies register several million attacks worldwide every year.

Malicious actors continuously develop new attack techniques. In February 2018, a 1.7 Tbit/s DDoS attack against an unspecified US company set new records. This and other attacks used open Memcached servers as an enabler. Memcache is typically used to speed up dynamic web applications. IT security companies have also noted that attackers are now using the CoAP protocol, which have been developed for communication between Internet-connected physical devices (IoT), to amplify DDoS attacks.

Vulnerabilities in the increasing number of IoT units are utilized by cyber criminals to create large botnets capable of generating powerful DDoS attacks.

Open servers
Open servers are servers that respond to requests from any unit on the internet. An attacker may amplify a DDoS attack by directing responses from open servers to the IP address which the DDoS is targeting.

Botnet
A botnet is a network of Internet-connected units that have been infected by malware, rendering it possible to remote control the units from a so-called command and control server (C2). A botnet may form part of a coordinated DDoS attack.

The Mirai botnet is an example of a botnet that became notorious in 2016 for its ability to launch devastating DDoS attacks. Since then, new Mirai variants that are still active have been discovered.

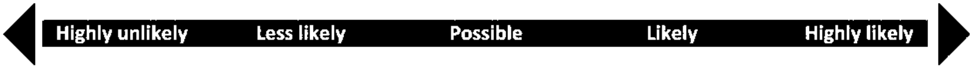
By registering IP addresses, which communicate with known C2 servers, and scanning the Internet for open servers, security companies are able to prove the existence of hundreds of units in the Danish telecom customer network that form part of a botnet and the existence of an even higher number of open servers that could be used to generate powerful DDoS attacks.

Threat levels

The Danish Defence Intelligence Services 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.

Below is the scale of probability the DDIS applies


Highly unlikely
Less likely
Possible
Likely
Highly likely