CENTRE FOR
CYBER SECURITY

Threat Assessment

The threat of destructive cyber attacks

First edition, June 2021

Content

CENTRE FOR
CYBER SECURITY

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

First edition, June 2021.

Destructive cyber attacks

The purpose of this threat assessment is to inform Danish decision-makers, public authorities and private companies of the threat of destructive cyber attacks. Even though the threat level is **LOW**, successful attacks will have serious consequences. Thus, organizations must keep updated on the nature of the cyber threat in order to improve their cyber resilience. Information on the threat enables the individual public authority and private company as well as Denmark as a whole to prioritize possible steps to bolster cyber security.

Key assessment

- The threat of destructive cyber attacks against Denmark is **LOW**. Thus, Danish private companies and public authorities will less likely fall victim to destructive cyber attacks in the next two years.

- Several foreign states are likely developing their capacity to carry out destructive cyber attack. However, it is less likely that foreign states are currently intent on executing destructive cyber attacks against Denmark.

- Destructive cyber attacks are launched with the overall purpose of destroying or damaging data, physical objects, or inflicting personal injury or death. However, there are a number of more specific underlying motives behind destructive cyber attacks, including sabotage, retaliation, testing and signaling.

- Destructive cyber attacks against industrial control systems may disrupt the delivery of critical services and cause physical destruction.

- CFCS assesses that destructive cyber attacks are mainly used in connection with conflicts or geopolitical tensions between nation states. As a result, the threat level may increase in situations of heightened political or military conflict involving countries that hold destructive cyber attack capabilities.

- Foreign states also launch significant and far-reaching disruptive cyber attacks, whose repercussions are serious though the attacks are not destructive per se.

The threat of destructive cyber attacks against Denmark

CFCS assesses that the threat of destructive cyber attacks against Danish public authorities and private companies is **LOW**, making it less likely that they will fall victim to destructive cyber attacks within the next two years.

The low threat level is the result of foreign states currently being less likely to harbour intentions to execute destructive cyber attacks against Denmark. However, as several foreign states possess destructive cyber attack capabilities the threat level may increase if their intentions shift, for instance in connection with a heightened conflict or geopolitical tensions.

Successful destructive cyber attacks can have very serious consequences and hold the potential to paralyze the digital infrastructure in organizations, resulting in physical damage and disruption of critical services such as electricity or Internet connection. Even though the threat level is **LOW**, public authorities and private companies should stay updated on developments in the threat landscape, given the serious nature of destructive cyber attacks.

What is a destructive cyber attack?

The Centre for Cybersecurity (CFCS) defines destructive cyber attacks as cyber attacks that could potentially result in:

- death or personal injury
- significant physical damage
- destruction or manipulation of information, data or software, rendering them unfit for use unless extensive restoration is undertaken.

Destructive cyber attacks come in various forms, ranging from data deletion in administrative systems to destruction of physical components in industrial control systems, potentially causing personal injury.

Still a rare occurrence, destructive cyber attacks have so far mainly resulted in data destruction, either by deletion or encryption of data without the possibility of recovery.

So far there is no known incidents involving destructive cyber attacks specifically targeting Danish public authorities and private companies. However, in 2017, the A.P. Møller-Mærsk shipping company was among the victims of the global NotPetya attack that compromised numerous victims worldwide.

Foreign states develop destructive cyber attack capabilities

Several foreign states likely continue to develop destructive cyber attack capabilities. Russia, China, Iran and North Korea are among the countries that possess destructive cyber attack capabilities. Foreign states conduct cyber espionage, among other things with the purpose of facilitating destructive cyber attacks.

It is possible that foreign states have made attempts to compromise private companies that are vital to the functioning of Danish society with the intent to launch destructive cyber attacks at a later stage. Consequently, the fact that hackers made several targeted attempts in 2017 to gain unauthorized access to organizations in the Danish energy sector is a source of great concern to CFCS.

Preparation of destructive cyber attacks will often include reconnaissance of organizations, systems and network units, such as industrial control systems. By collecting information on organizations and systems, hackers are able to develop custom malware. Also, hackers are capable of installing so-called backdoors in compromised systems to be used in future destructive cyber attacks. Once a backdoor has been installed, hackers are able to launch destructive cyber attacks against the system. Thus, even a dormant backdoor could become a significant security vulnerability.

Examples of cyber attacks causing data deletion

Olympic Destroyer (2018) In February 2018, the Winter Olympics fell victim to the Olympic Destroyer Wiper malware that ultimately infected thousands of computers. The hackers had spent months preparing the attack by compromising and gaining access to networks connected to the Winter Olympics. The wiper malware was activated on the day of the opening ceremony. However, local authorities successfully restored the digital infrastructure and were able to limit the impact of the attack. US authorities have accused Russia of being behind the attack.

NotPetya (2017) In June 2017, the NotPetya malware shut down a large number of computers and servers across the world. The NotPetya attack originated from a compromised Ukrainian software company – the developer of the M.E.Doc. software. The hackers managed to spread the malware via a M.E.Doc. software update. The malware was a so-called worm, which subsequently quickly spread to other parts of the affected companies' IT infrastructure, infecting other companies as well.

Attack on Ukrainian power grid (2015) In 2015, several electricity companies based in western Ukraine were hit by cyber attacks. The hackers gained access to the energy companies' SCADA systems, leaving more than 225,000 Ukrainian residents without electricity. The hackers used the Killdisk wiper malware to delete logs and files. However, manual back-up systems were able to restore power within six hours.

The Sony Pictures hack (2014) In 2014, hackers broke into the computer systems of Sony Pictures Entertainment, destroying data and systems and leaking emails and copies of then-unreleased films.

Motives behind destructive cyber attacks

Though destructive cyber attacks are overall meant to cause destruction and harm, more specific motives may differ. Sabotage is one underlying motive, which may involve an attack aimed at disrupting or preventing an opponent's access to a system, technology or information. The motive may also be to punish the target in connection with a conflict by inflicting financial damage or other types of resource damage to the victim. In addition, a motive behind destructive cyber attacks may be to send a signal to the victim and other potential victims. Finally, a destructive cyber attack may serve as the basis for testing and potentially developing capacity or erase traces of other types of cyber attacks.

It is often difficult to assess the exact motive of a destructive cyber attack, just as such attacks likely serve multiple purposes.

NotPetya, one of the most destructive cyber attacks in the world, may have served different purposes. Starting in Ukraine in 2017, the day before the Ukrainian Independence Day, the attack soon spread to the rest of the world. Several countries have attributed the attack to Russia. The attacks can be interpreted as a punishment of Ukraine, which at the time was locked in a conflict with Russia. The attack could also be interpreted as a signal to the rest of the world of the risks involved in conducting business in Ukraine.

Destructive cyber attacks against targets in the Middle East

2012

Shamoon 1
In 2012, Saudi Arabian oil and gas company Saudi Aramco suffered a cyber attack that damaged more than 30.000 of its office computers and destroyed a large amount of data.

2017

Shamoon 2
In 2017, a number of organizations across different sectors in Saudi Arabia, including the energy, transport and financial sectors, fell victim to a new variant of the Shamoon wiper malware.

2018

Shamoon 3
In December 2018, another variant of the Shamoon malware was used in a cyberattack against organizations within the oil, gas and mine industry in Saudi Arabia and the United Arab Emirates.

2019

ZeroClear hits multiple victims
The ZeroClear wiper malware hit victims in the energy, oil and gas sector across the Middle East.

Attacks against Bahrain's energy sector
On 29 December 2019, Bapco, Bahrain's national oil company, was hit by a wiper attack involving the DUSTMAN malware, a new variant of the ZeroClear malware.

2020

Israel averted attack on power plant (January)
Hackers attempted to paralyze Israeli power plant.

Attack against water facilities in Israel (April)
Hackers attacked water facilities in Israel and tried to change the content of chlorine levels in the country's drinking water. The attack was thwarted before it caused any real damage.

Attack on Iranian port (May)
Hackers disrupted operations at Shahid Rajaee, one of Iran's biggest ports, causing chaos and delays.

New attacks on Israeli water facilities (June)
Israeli authorities publicly stated that they had averted attacks against two water facilities.

Attack against Iranian port authority (October)
Iranian authorities publicly stated that they had averted attacks against the country's port authority. According to Iranian authorities, the aim of the attack was to disrupt the transportation of goods.

Attacks can cause physical destruction

Destructive cyber attacks against industrial control systems supporting the delivery of critical services may have serious societal repercussions. Attacks on industrial control systems could cause disruption of critical services such as electricity and Internet connection, just as they may result in physical destruction and personal injury.

As industrial control systems monitor and control industrial processes, such as security mechanisms, dangerous and potentially destructive situations might occur if these security measures are disrupted, manipulated or disconnected.

Industrial control systems

The term industrial control systems covers both SCADA (Supervisory Control and Data Acquisition) and ICS (Industrial Control System).

SCADA and ICS are network-connected units controlling industrial systems. They are used for monitoring and controlling mechanical systems, also known as OT systems. Industrial Internet of Things is the term used when SCADA or ICS use IP networks or are connected via the Internet.

However, so far only few incidents have been recorded of destructive cyber attacks with the likely aim of causing physical destruction.

So far, the only known destructive cyber attack is the one that hit Iran when, in 2010, hackers used the Stuxnet malware to destroy Iranian uranium enrichment centrifuges.

Examples are rare of cyber attacks that would have proved physically destructive had they been successful. One such example is the 2017 cyber attack against the industrial control system Triconex in Saudi Arabia that possibly could have resulted in physical destruction. The attack was directed at a petrochemical industrial company and the Triconex system used by the targeted company. One of the Triconex system properties is to ensure the controlled and safe disconnection of production systems in the event of critical errors or problems. The attack could potentially have caused physical destruction, but the security systems closed down safely. The closing down of the system led to the detection of the installed malware. If the security mechanisms had been disconnected or manipulated, the risk of personal injury or death could have been higher as a result of deadly gas leaks or explosions.

Another example is the destructive cyber attack on Ukraine’s power grid in 2016 that could have resulted in physical damage on equipment. IT security experts have shown indications that the attack was intended to affect control switches and protective relays with DDoS attacks. Had the attack been successful, it might have caused long-term power outages. However, the hackers failed this part of the attack.

States are likely directing destructive cyber attacks against critical infrastructure, including industrial control systems with companies of societal importance, as such attacks would hit their opponents where it hurts the most. Many companies use the same kind of industrial control systems, allowing hackers to develop techniques that could be used in future conflicts to affect numerous targets in similar setups.

Destructive cyber attacks mainly used in conflicts

CFCS assesses that most destructive cyber attacks are launched by states in connection with conflicts or geopolitical tensions. Consequently, the threat may increase in connection with heightened political or military conflicts with countries that hold destructive cyber attack capabilities.

In conflict areas where states launch destructive cyber attacks against civilian targets the threat of destructive cyber attacks may be higher. Danish companies operating across the world may become collateral victims of cyber attacks against non-Danish companies operating in conflict areas.

The threat of destructive cyber attacks may also increase against Danish companies working for companies or states that are targets of destructive cyber attacks.

It is possible that Danish companies and authorities present in conflict areas, in particular in Ukraine and the Middle East, may be impacted by collateral effects of destructive cyber attacks such as power outages and network disruptions.

In connection with conflicts abroad, certain critical sectors have been hit by destructive cyber attacks. The energy, telecom, transport and financial sectors, in particular, have come under attack during crises. A few attacks against these sectors have been directed against industrial control systems.

Critical infrastructure hit by destructive cyber attacks in Ukraine

Ukraine has repeatedly fallen victim to cyber attacks in connection with its conflict with Russia. In addition to attacks against the energy sector in 2015 and 2016, Ukraine's financial and transport sectors have repeatedly been hit by cyber attacks. For instance, in 2016, the Ukrainian Ministry of Finance and Central Bank came under attack, which resulted in the disruption of 150,000 electronic money transfers. In October 2020, US authorities accused six Russian nationals of being responsible for the attack. According to the US authorities, the hackers were working on behalf of a Russian intelligence service.

In 2017, Ukraine's transport sector was hit by the BadRabbit malware. The attack caused flight delays at Odessa Airport and disrupted electronic payments in the Kiev metro. Earlier in 2017, several companies in Ukraine's transport sector were also hit by the NotPetya attack.

States behind far-reaching disruptive cyber attacks

States have also been known to conduct disruptive cyber attacks which do not fall within CFCS’ definition of destructive cyber attacks, yet still carry serious consequences. For instance, states use attack techniques such as denial-of-service (DDoS) attacks, and defacement attacks to carry out disruptive cyber attacks. These attack techniques are not considered destructive per se, as they do not destroy or cause harm to data or objects. Though far-reaching disruptive cyber attacks are rare, they have been known to result in disconnections or disruptions of the access to and operation of numerous or vital digital systems and services abroad.

In the autumn of 2019, Georgian web hosting provider Pro Service fell victim to a serious disruptive attack. US and British authorities have publicly accused Russian state-sponsored hackers of being responsible for the attack. According to the British authorities, one of the motives for the attack was to create instability and undermine Georgia’s sovereignty.

The cyber attack against Pro Service resulted in the defacement of more than 2,000 Georgian websites belonging to the Georgian government, presidential office, civilian courts, local city councils, banks, NGOs, large businesses and news agencies. Hackers replaced the original website content with a photograph of former President Mikheil Saakashvili saying ”I’ll be back” before shutting down the websites. However, all the websites were up and running again 24 hours later.

Between December 2011 and September 2012, the US financial sector was exposed to an extensive DDoS campaign that carried serious repercussions to the sector. Numerous websites were rendered inaccessible, customers were left unable to access their online bank accounts, and the financial institutions incurred millions of dollars in remediation costs as they tried to mitigate the attacks. In 2016, US authorities accused Iranian hackers of performing the attacks on behalf of the Iranian government.

Recommendations

When the likelihood is low but the impact high
An effective security organization and basic cyber security measures must be in place in order for an organization to be able to address destructive cyber attacks.

Worst case – impact assessment
Though the probability of an organization falling victim to a destructive cyber attack is less likely, such an incident may carry very serious consequences. If an organization chooses to prepare for a destructive cyber attack, CFCS recommends that a ”worst case” impact assessment be carried out that focuses on the incidents and situations that would have the most destructive consequences for the organization and that efforts are made to actively address these consequences.
The organization should review existing pre-emption, detection and mitigation strategies to determine if these strategies, and the resources they require, need to be adjusted based on what the organization can afford to lose and what must be protected at all costs.

Protect communication and critical systems
Lessons learned from destructive cyber attacks demonstrate the importance of being able to restore an organization's communication systems in order to effectively address incidents. IP telephony and emails are often affected in connection with destructive cyber attacks against critical systems. In addition, the ability to communicate internally and with customers and partners is key in such a situation. Also, it is vital to protect the critical IT systems on which many other IT systems depend. Such systems may include identity and access management structures that allow communication between employees and IT services. Without a reliable backup or redundant installation, re-establishing these systems may prove both costly and time-consuming.

Contingency plan shall address the unexpected
Destructive cyber attacks may have unpredictable consequences, accentuating the need for contingency plans that focus on general crisis management. It may be necessary to prepare different plans to provide for different scenarios. For example, one plan may be prepared that focuses on investigating defined incidents covering a short span of time, while another is formulated focusing on major incidents that run for extended periods of time. In the latter case, the contingency plan must allow for several practical challenges, for instance local and global transport, catering and temporary accommodation for the staff working on restoring the IT systems.

When the damage is done
Finally, the CFCS recommends that the organization reviews, adapts and tests its preparedness plans to ensure that contingency measures and crisis management regimes are fitted to handle the less likely yet very critical scenarios identified by the ”worst case” impact assessment. Effective preparedness regimes may help limit the consequences of destructive cyber attacks.

Measures related to outsourced solutions
If the entire or parts of the organization's IT infrastructure have been outsourced to external suppliers, the CFCS recommends the continuous involvement of suppliers in implementing measures aimed at protecting the organization against destructive cyber

attacks. Suppliers of IT services should also be closely involved in identifying threats, vulnerabilities and technical consequences, including in connection with implementation of basic security measures.

Basic security – a necessity

As mentioned above basic security measures must be in place as a precondition for addressing destructive cyber attacks. Any organization should as a minimum live up to the following:

- Cyber security must be anchored in the senior management
- The organization must have or be able to draw on the right technical competences
- Educate and train especially senior management, but also staff
- Contingency regime should be subject to testing

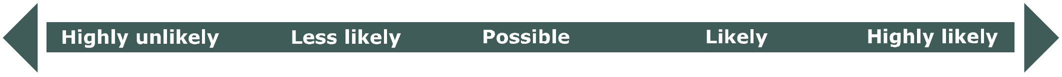
For further advice please see the CFCS's ″Cyberforsvar der virker″ (in Danish) and ″Informationssikkerhed i leverandørforhold″ (in Danish) as well as the CFCS's general guides and threat assessments.

Threat levels

The Danish Defence Intelligence Service uses the following threat levels.

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