CENTRE FOR CYBER SECURITY

4 June 2024

THREAT ASSESSMENT

The CFCS is raising the threat level for destructive cyber attacks against Denmark from **LOW** to **MEDIUM**

This threat assessment is intended to notify organizations and decision-makers in Denmark of the increased threat of destructive cyber attacks. Knowledge of the threat is relevant for the protection of digital systems in critical sectors.

KEY ASSESSMENTS

- The CFCS is raising the threat level for destructive cyber attacks against Denmark from **LOW** to **MEDIUM**, implying the possibility that organizations in Denmark will fall victim to destructive cyber attacks.

- The decision to raise the threat level is based on Russia's likely increased willingness to use destructive hybrid tactics against European NATO member states. The CFCS assesses that Russia’s risk appetite also includes destructive cyber attacks.

- The CFCS is raising the threat level for destructive cyber attacks against Denmark in general. Should Russia decide to direct destructive cyber attacks against Denmark, it will likely target a wide range of critical sectors.

- In the current situation, it is less likely that Russia is intent on launching destructive cyber attacks on Denmark with serious and far-reaching consequences for critical societal functions. However, small-scale cyber attacks could also have a serious impact on the victim and society at large.

- The threat of destructive cyber attacks primarily emanates from Russian state-sponsored hackers but also from non-state hackers with various degrees of ties to the Russian state.

ANALYSIS

The CFCS is raising the threat level for destructive cyber attacks from **LOW** to **MEDIUM**, implying the possibility that organizations in Denmark will fall victim to destructive cyber attacks.

The decision to raise the threat level is based on Russia's likely increased willingness to use destructive hybrid tactics against European NATO member states. The CFCS assesses that Russia's increased risk appetite also includes destructive cyber attacks. For years, destructive cyber attacks have been included in the toolkit of Russian state-sponsored hackers.

Increased threat of physical sabotage

On 8 May 2024, the Danish Security Intelligence Service (PET) announced an increase in the threat of Russian-directed physical sabotage campaigns against military and civilian targets in Denmark linked to the support to Ukraine.

According to PET, the reason for the increased threat is the fact that individuals with possible links to the Russian intelligence services have conducted sabotage against a number of European countries. Based on these activities, PET assesses that Russia is demonstrating increased risk appetite for using so-called hybrid tactics against targets in Europe. The purpose of the Russian activities is, among others, to create fear and uncertainty and to weaken popular backing for the continued support to Ukraine.

The threat applies to Denmark in general

The CFCS is raising the threat level for destructive cyber attacks on Denmark in general. The CFCS assesses that many different types of critical sector organizations could become designated as potential targets for destructive cyber attacks.

The reason is that the objective of destructive cyber attacks likely is to influence the population and decision-makers. For instance, the aim of destructive cyber attacks against Denmark is likely intended to weaken the Danish population's support for Ukraine.

The specific physical impact of the attacks will thus likely be secondary as the main objective is to generate attention, opening the possibility of a wide range of potential targets.

The hackers' selection of targets, however, will likely be influenced by factors such as already established entry points or ease of accessibility.

Destructive cyber attacks could carry significant consequences

In the current situation, it is less likely that Russia will launch destructive cyber attacks with serious and far-reaching consequences for critical societal functions. Even though this type of attack is less likely, the CFCS assesses that hacker groups linked to Russia are continually preparing the capability to launch this form of destructive cyber attacks on

Denmark. The likelihood of this type of attack could thus increase at short notice or without any warning.

Small-scale cyber attacks could still have a serious impact on the victim and on society as a whole. Such attacks could include attacks that have limited impact on critical societal functions. Even if destructive cyber attacks do not have any impact on critical societal functions, they could cause uncertainty and influence society.

CFCS' definition of destructive cyber attacks

The CFCS defines destructive cyber attacks as attacks that could result in:

- death or personal injury
- signficant property damage
- destruction or manipulation of information, data or software, rendering them unfit for use unless extensive recovery is initiated

Wiper malware attacks designed to delete, overwrite or encrypt data are the most common type of destructive cyber attacks.

Russian hacker groups have previously been linked to several destructive cyber attacks on not only Ukraine but likely also on other countries. For example, Ukraine has suffered numerous wiper attacks but also attacks on industrial control systems within its critical infrastructure, causing widespread power outages.

Russia's increased risk appetite could also be reflected in widespread DDoS attacks against critical systems. DDoS attacks are not destructive in themselves, but widespread DDoS attacks against key systems could potentially cripple or incapacitate critical functions for shorter or longer periods of time and thus influence the population and decision-makers in the same way as destructive cyber attacks.

The threat primarily comes from Russia

The threat of destructive cyber attacks primarily stems from Russian state hackers. The CFCS assesses that in the current situation, Russia will make efforts to hide its involvement in potential destructive cyber attacks, making it more difficult for the countries affected by hybrid activities to respond.

One way is for the hackers to launch attacks mimicking criminal ransomware attacks in which data is encrypted, however subsequent decryption will not be possible. There have been previous examples of such fake ransomware attacks.

However, the ransomware attacks that have hit Danish organizations within the past few years have highly likely been conducted by criminal hackers aiming to achieve financial gain rather than destroying data or infrastructure. The CFCS assumes that future ransomware attacks also, by and large, will be carried out by financially motivated criminal hackers.

State hackers could also try to conceal their involvement in destructive cyber attacks by posing as activist hackers, for instance by creating websites or accounts on different

platforms where they pose as cyber activists and claim responsibility for destructive cyber attacks.

The threat from non-state hackers

Another way for Russia to hide its involvement in destructive cyber attacks is to employ proxies to carry out the attacks. Consequently, non-state hackers pose a potential threat.

Pro-Russian cyber activists are a good example of how non-state hackers can support state interests. However, that does not mean that they work directly for the state. The CFCS assesses that some pro-Russian cyber activist groups are linked to the Russian state.

Cyber activism is typically motivated by ideological or political concerns and is for the most part conducted independently of states, making it difficult to assess a cyber activist actor's affiliation to foreign states. In some cases, it is not clear cut whether cyber activists are acting on their own initiative or on behalf of a state.

Iran also poses a threat

Even though the threat mainly comes from Russia, Iran also poses a potential threat.

For instance, a group calling itself CyberAv3ngers claimed responsibility for a number of destructive cyber attacks on poorly protected operational technology equipment, also called OT equipment, in Western countries. In this connection, the group designated all equipment produced in Israel as legitimate targets in response to the conflict between Israel and Hamas.

The US Cybersecurity and Infrastructure Security Agency has publicly linked CyberAv3ngers to Iran's Revolutionary Guards Corps (IRGC) and has sanctioned six individuals from IRGC over the group's destructive cyber attacks on the United States. The attacks are thus an example of how state hackers can disguise their attacks as activism.

THREAT LEVELS

The DDIS 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 carried out or attempted attacks/harmful activity.
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.