CENTRE FOR CYBER SECURITY

Threat assessment: The CFCS raises the threat level of cyber activism against Denmark from MEDIUM to HIGH

The purpose of this threat assessment is to inform of the CFCS' raising of the threat level of cyber activism against Denmark from **MEDIUM** to **HIGH** based on the strong activity among pro-Russian activist hacker groups and their intention and capability to attack Danish targets.

Key assessment

- The threat of cyber activism against Denmark is **HIGH**, prompting the CFCS to raise the threat level from **MEDIUM** to **HIGH**. The raising of the threat level of cyber activism to **HIGH** indicates that Danish private companies and public authorities are likely to fall victim to cyber activist attacks in the short term.

- The CFCS has raised the threat level of cyber activism based on the strong activity among pro-Russian activist hacker groups against NATO countries, including Denmark, as well as on their increased capabilities.

- Pro-Russian hackers regularly attack targets in sectors that they consider symbolic of other countries' support for Ukraine. The hackers have, in particular, targeted authorities and companies in the transport, financial and defence sectors.

- Simple DDoS attacks, in particular, are a common means of cyber attack among pro-Russian hackers. This type of attack disrupts and attracts attention but will leave no permanent or destructive consequences to the victims' systems.

- Pro-Russian hackers are motivated by patriotism as well as media coverage.

Analysis

It is likely that Danish organizations will once again become targets of cyber activist attacks. The reason for this is that the ever-growing tensions between Russia and the West have prompted pro-Russian cyber activists to launch a barrage of attacks on different targets selected within a wide range of NATO countries. Pro-Russian hackers regularly attack targets within sectors that they consider symbolic of other countries' support for Ukraine. As a result, the hackers have primarily targeted authorities and companies in the transport, financial and defence sectors.

The pro-Russian cyber activists do not specifically target Denmark over other NATO countries. However, the most recent cyber attacks against Danish targets indicate that cyber activists consider Danish organizations potential targets of cyber attacks.

Over the past year, pro-Russian cyber activists have more or less constantly conducted short-term cyber attack campaigns, dividing the targets into different groups according to specific themes. For instance, Danish targets have been included in a campaign targeting European defence ministries and in a campaign against the Danish financial sector.

Cyber activism is conducted by individuals and hacker groups who launch cyber attacks to attract maximum attention to their cause or to punish organizations.

Cyber activism is typically motivated by ideological or political concerns, ranging from single issues to opposition against rulers. Consequently, cyber activist attacks could also be launched in response to single events. A likely case in point is the DDoS attacks that were launched in late January 2023 against a number of Danish websites. Cyber activists have claimed responsibility on social media, arguing that their attacks were launched in response to, for instance, the Quran burnings in Sweden and Denmark.

Increasing support equals larger capabilities

Pro-Russian cyber activist hacker groups are increasingly formalizing their planning and execution of attacks. In addition, several of the most active pro-Russian groups have established platforms dedicated to raising resources for DDoS attacks.

DDoS attacks, in particular, are a common means of cyber attack among pro-Russian hackers. This type of attack disrupts and attracts attention but will leave no permanent or destructive consequences to the victims' systems

The CFCS assesses that the number of supporters and active participants in the pro-Russian cyber activist groups has increased following Russia's invasion of Ukraine.

It is likely that the increased support for pro-Russian activist hacker groups indicates that the groups achieve the capability to launch larger and more powerful attacks.

One result of the increasing support is an influx to the groups of members offering botnet resources used to launch DDoS attacks. The increased resources brought about by the support could increase the power of DDoS attacks and make mitigation more difficult. However, the DDoS attacks will still not cause permanent or destructive damage to the systems.

DDoS attacks

DDoS stands for Distributed Denial of Service and refers to cyber attacks in which hackers exploit compromised computers to flood the targeted website (webserver) with data traffic, making the website or network unavailable for legitimate traffic as long as the attack is in progress.

Patriotism and media coverage fuel the threat

The different pro-Russian hackers are all motivated by a shared patriotic agenda. It is likely that as long as the current crisis between Russia and the

West lasts, the pro-Russian activist groups will be motivated to attack targets in the West and in Denmark.

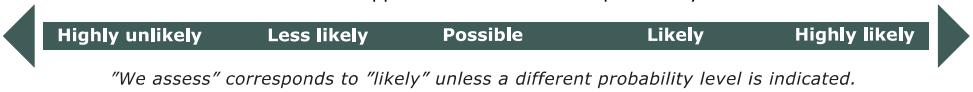
The hackers' specific group affiliation has little effect on the threat, as the groups launch attacks based on the same political agenda and using the same attack techniques.

The CFCS assesses that pro-Russian hackers are also motivated by media coverage, paying attention to the media coverage of their cyber attacks. The groups share posts regarding media coverage with their supporters. In addition, different pro-Russian hacker groups are embroiled in competition. The internal competition between these groups is evidenced by their insistence that they receive unequivocal credit for their attacks by the media and rival hacker groups. Thus, it is possible that widespread media coverage of cyber activist attacks against Danish targets could contribute to making Denmark an attractive target for pro-Russian cyber activists.

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



"We assess" corresponds to "likely" unless a different probability level is indicated.