CENTRE FOR CYBER SECURITY

Threat Assessment:

Old hackers, new platforms

External pressure forces ransomware operators to reorganize their business

1st edition October 2021

Purpose
This threat assessment focuses on ransomware attackers. Parts of the ransomware community have come under pressure, among others, from US authorities, forcing cyber criminal ransomware gangs to reorganize their business. Thus, this threat assessment is intended to inform decision-makers in private companies and public authorities of the current threat of ransomware attacks.

Key assessment

- The overall threat from cyber crime remains **VERY HIGH.** It is it highly likely that Danish organizations will fall victim to targeted ransomware attacks within the next few years.

- Criminal hackers offering Ransomware-as-a-Service (RaaS) are reorganizing their business following the May 2021 ransomware attack on the US oil company Colonial Pipeline.

- Several RaaS operators have either permanently or temporarily closed down their platforms, and several top-tier dark-web forums have banned recruitment operations from their platforms.

- As a result, the number of RaaS attacks decreased for a short period of time over the summer of 2021. However, other RaaS operators have since been quick to take over.

- It is likely that some of these seasoned cyber criminals have not ceased their malicious activities but merely switched over to new platforms, causing the number of RaaS attacks to reach the same levels as seen before the Colonial Pipeline attack.

- Consequently, the fact that parts of the supply chain can be replaced without seriously disrupting or hampering criminal activities is a testament to the robustness of the supply chain in criminal networks.

- The US authorities' response following the Colonial Pipeline attack, among others, has likely deterred some criminal actors from deploying targeted attacks on US critical infrastructure, particularly in the short term. However, this is by no means a guarantee that attacks will not occur.

The United States has ramped up pressure on ransomware gangs
The threat from cyber crime remains **VERY HIGH**. It is it highly likely that Danish organizations will fall victim to targeted ransomware attacks within the next few years.

However, the criminal ecosystem behind RaaS attacks have undergone some reorganisation in the wake of the May 2021 ransomware attack on the US Colonial Pipeline oil company.

This attack was the first in a series of incidents in mid-2021 that caused changes in the RaaS landscape and added new nuances to the overall cyber threat landscape.

The attack, which was carried out by Darkside RaaS affiliates, led to widespread fuel shortages along the US East Coast – underscoring that the consequences of cyberattacks potentially extend beyond the financial losses of the targeted organization.

Following the Colonial Pipeline attack, US food giant JBS and IT company Kaseya fell victims to a comprehensive ransomware attack conducted by REvil ransomware operators.

The attacks have subsequently prompted US law enforcement agencies to crack down on ransomware gangs. As a result, efforts to counter the threat of ransomware attacks have moved to the top of the government's agenda, elevating investigations of ransomware attacks to a similar priority as terrorism. Consequently, efforts against the ransomware threat will become part of a whole-of-government approach aimed at facilitating cooperation and coordination between all US authorities.

At the same time, ransomware attacks were included in the US foreign and security policy agenda. The United States criticized the Russian government for not doing enough to counter the criminal gangs believed by the United States to reside in Russia. Also, US authorities announced that if Russian authorities fail to take action, the United States is prepared to pursue the criminal gangs even if these gangs operate out of Russia. In this connection, the United States has categorized ransomware attacks against 16 critical sectors as particularly serious, and the US authorities have reserved the right to respond with the means and at a time that they find appropriate.

In their attempt to neutralize hackers, US authorities are employing tools that can disrupt the flow of money to ransomware operators. Following the Colonial Pipeline attack, the authorities seized USD 2 million worth of bitcoins from the criminal actors behind the attack. In late September 2021, for the first time ever, the US Treasury Department sanctioned a specific cryptocurrency exchange, accusing it of facilitating ransom transactions in connection with ransomware attacks. The sanctions regimes will ban all trade between the Russian cryptocurrency exchange Suex and US entities and make it harder for hackers to receive payment for their attacks and services.

Ransomware attacks as platform economy
Both Darkside and REvil are examples of ransomware that have been sold as RaaS.

RaaS is a sub-model of Crime-as-a-Service (CaaS) that enables cyber criminals to buy access, tools and infrastructure to deploy ransomware rather than develop these themselves.

RaaS has introduced a kind of platform economy to cyber crime in which affiliates use ransomware attacks to make a profit for themselves and also for the criminal owners of the platform.

Recruitment operations to the platforms and cooperation between the criminal actors are conducted through, for instance, dark web forums.

RaaS gangs change tactics following the Colonial Pipeline attack
During the late summer of 2021, several RaaS gangs made significant changes to their tactics.

Most notably, the operators behind several top-tier RaaS platforms, including REvil, Avaddon and Darkside, shut down their platform operations. While Avaddon and Darkside operators remained shut down, REvil was reactivated in mid-September 2021 following a two-month break.

At the same time, Exploit and XSS, two key Russian-speaking dark web forums, banned RaaS operators from recruiting affiliates on their forums. These forums have previously played a key role in recruiting affiliates to RaaS platforms as well as exchanging services, access and tools used in targeted ransomware attacks.

Previous examples indicate that parts of the criminal cyber networks are continuously expanding or replacing their malware arsenal, as illustrated in the spring and summer of 2020 during the COVID-19 pandemic, when criminal hacker groups upgraded their tools and renewed their collaborations and activities.

The crackdown by US authorities on criminal groups following the Colonial Pipeline ransomware attack and the risk of targeted Russian measures against criminal cyber gangs in Russia have likely caused these relatively simultaneous and sudden changes in the RaaS landscape.

Hackers collaborate and continue operations from other platforms
The shutdown of several RaaS platforms and the ban on recruitment on top-tier forums led to a drop in the number of new ransomware victims during the summer of 2021.

The CFCS has previously reported that criminal hackers are generally successful in adapting to new situations and thinking outside the box when they are exposed to external pressure or eye new opportunities to make a profit. The vacuum left behind by the absence of widely used platforms has quickly been filled by other groups that have been eager to develop their RaaS platform.

This is in particular evident for the RaaS platform LockBit. LockBit has been used in several media covered attacks over the summer. Several of the criminals, previously affiliated with, for instance, Darkside, Avaddon and REvil, have likely switched over to the LockBit platform, contributing to the surge of LockBit attacks in recent months.

The current RaaS attack level is returning to the pre-Colonial Pipeline attack level, underscoring the robustness of the supply chain in criminal networks in which parts of the supply chain can be replaced without seriously disrupting or hampering criminal activities.

Platform operators are on a charm offensive to recruit affiliates

The operators of LockBit ransomware have been particularly open and public during the increase in their activities last summer. The operators behind the LockBit ransomware have given interviews to several media outlets, enabling them to promote their platform, their work division and their targets.

For instance, LockBit has been able to recruit affiliates via the Russian Anonymous Marketplace (RAMP) forum, likely established by former RaaS operators. RAMP is currently hiring members from Exploit and XSS, creating a perfect meeting spot for RaaS gangs and operators.

In recent media interviews, a LockBit operator claimed that they will not attack educational or healthcare institutions and that they will not target charitable organizations.

Several RaaS gangs made similar statements during the COVID-19 pandemic in 2020, saying that they would refrain from targeting the healthcare sector. However, during the pandemic, there were several examples of targeted ransomware attacks against the healthcare sector abroad.

Ransomware gangs are constantly weighing the risks and rewards of a potential attack. Illustrative of this fact is that most gangs steer away from attacking targets in Russia and post-Soviet countries, where many operators and their affiliates are believed to reside.

The statement made by LockBit operators is likely meant to serve as a demonstration of the gang's risk management capabilities and a promotion campaign to recruit new affiliates and collaboration partners rather than a display of community spirit.

The US response following the attacks on, for instance, Colonial Pipeline, has likely deterred some cyber criminals from targeting US critical infrastructure, in particular, in the short term.

Just as the COVID-19 pandemic did not stop cyber criminals from attacking the healthcare sector, criminal actors will not refrain from attacking the mentioned critical sectors unless they believe that the risk outweighs the reward.

Thus, critical sectors are by no means exempt from attacks just because cyber criminals claim that they will refrain from targeting certain sectors. Other criminal

actors may be willing to attack instead, or they may decide to do so anyway if they assess that the reward outweighs the risk.

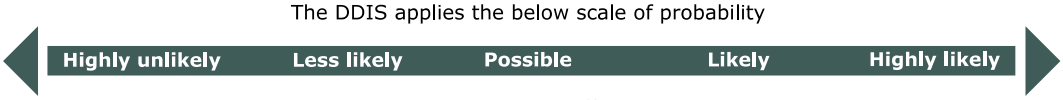
Threat levels

Definition of threat levels

The DDIS uses the following threat levels, ranging from **NONE** to **VERY HIGH**.

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.

Further relevant reading

The Centre for Cyber Security (CFCS) continuously publishes guidance and threat assessments. Highlighted below are a number of publications of particular relevance to the threat of cyber crime. All publications are available on the CFCS website.

Collaboration between cyber criminals
The threat assessment "Do cyber criminals dream of trusting relationships?" describes how established division of labour and exchange of services inside the criminal environment contribute to creating a very high threat of cyber crime, in general, and targeted ransomware attacks, in particular.
Read the assessment here: https://cfcs.dk/en/threat-assessments/organised-cyber-crime/

Cyber criminals advance their capabilities
The threat assessment "Cyber criminals advance their capabilities in the shadow of the pandemic" describes how cyber criminals have updated their tools and renewed their collaborations and activities. Read the assessment here: https://cfcs.dk/en/threat-assessments/cyber-criminals-rearm-in-the-shadow-of-the-pandemic/

The threat of targeted ransomware attacks
The threat assessment "Criminals tighten the digital thumbscrew" describes the threat of targeted ransomware attacks that may potentially have serious repercussions for an organization. Read the assessment here: https://cfcs.dk/en/threat-assessments/double-extortion/

The anatomy of targeted ransomware attacks
The investigation report 'The anatomy of targeted ransomware attacks' outlines how a typical targeted ransomware attack plays out and presents specific recommendations for protective measures. Read the report here: https://cfcs.dk/en/reports/the-anatomy-of-targeted-ransomware-attacks/

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