CENTRE FOR
CYBER SECURITY

THREAT ASSESSMENT

Do cyber criminals dream of trusting relationships?

Increasingly professional criminal actors collaborate on extensive and advanced online attacks

Purpose
This threat assessment has the purpose of informing decision-makers on the development of organized cooperation between online criminals and its impact on the threat of cyber crime.

Key assessment

- The CFCS assesses the threat of cyber crime to be VERY HIGH. The threat is supported by cyber criminals who cooperate and exchange services under market-like conditions, so-called Crime-as-a-Service.

- Crime-as-a-Service provides criminals with access to services, tools and infrastructure that facilitate cyber attacks, sparing them the effort of developing the means themselves.

- The collaboration increases the specialization and effectiveness of the cyber-criminal environment, creating robust and organized supply chains that serve to support cyber attacks, including targeted ransomware attacks.

- The use of cryptocurrency drives this development towards a more commercialized and specialized cyber-criminal environment.

- Ransomware-as-a-Service has introduced a kind of platform economy for cyber crime in which hackers use ransomware attacks to earn money for themselves and for the operators that own the platform.

- This development has resulted in more targeted and professionalized approaches by some criminal groups, in turn contributing, among other things, to an increase in the threat of targeted ransomware attacks.

Analysis

The CFCS assesses the threat of cyber crime to be VERY HIGH. The threat is supported by criminal hackers selling and buying services online. This mutual exchange of services – known collectively in IT security speak as Crime-as-a-Service (CaaS) – is no new phenomenon. However, in recent years this collaboration has evolved and changed, impacting the threat picture.

The exchange of goods and services takes place on closed Internet forums and through established personal collaboration relationships. Here, a broad palette of tools is sold and exchanged such as malware, infrastructure – including botnets – compromised accesses and distribution through phishing and downloaders. CaaS thus enables hackers to procure the services and accesses needed to conduct cyber attacks, sparing them the effort of developing the means themselves.

This creates value chains between the criminal hackers that in various ways serve to increase the profit from cyber crime.

The trade in criminal services is sometimes limited to specific services at a fixed price, in which case the exchange is akin to the transfer of goods in a traditional market with well-defined roles for both buyer and seller. A typical example of this kind of trade is online black markets, where criminals sell goods such as stolen personal and financial information, including credentials in the form of usernames and passwords.

Access to compromised RDP sold online

Cyber criminals often abuse vulnerable Remote Desktop Protocol (RDP) connections in cyber attacks, for instance in connection with targeted ransomware attacks. The transfer and sale of compromised RDP connections are thus common in criminal circles.

Criminal actors often compromise a large number of RDP connections simultaneously, for instance through brute force attacks. Subsequently, they sell specific accesses to other hackers who use them as entry points for more targeted cyber attacks.

In 2018, a security company identified a value chain that involved the SamSam cyber-criminal group buying stolen RDP credentials to IT systems for as little as 10 US dollars. The group then used the credentials to encrypt the systems, demanding up to 40,000 US dollars in ransom for their decryption.

Fixed cooperation relationships streamline production

CaaS sometimes takes the form of prolonged cooperation relationships between criminals, due, in part, to the obvious fact that the exchange of services is unregulated and takes place outside the law. The risk of the scammer being scammed is thus usually present when criminals exchange services, and criminals have been known to use different Internet forums to fraud fellow criminals. Similar to conventional cooperation relationships, CaaS is thus built on trust among criminals, and building up trust takes time, but only a moment to destroy.

At the same time, the risk exists that incompetent hackers who use other hackers’ services negligently expose not only themselves but also the skilled cyber criminals.

Criminal networks are thus in the market for longer-lasting cooperation affiliations with other actors with whom they have built a relationship of trust.

Examples of such relationships include criminals who target specific victims cooperating with criminals who launch indiscriminate attacks affecting thousands of victims, for instance through phishing. Targeted ransomware attacks are thus often launched following an initial compromise of the victim via malware spread through phishing campaigns.

In such cases, the initial, and typically automated, attempt at compromise distributed to numerous recipients through botnets is followed by more targeted manual attacks by other actors against specific victims.

This type of cooperation is typically more organized and established than is the trade with specific services on online markets, etc.

Cooperation comes at a price
In December 2019, US authorities, acting in coordination with their British counterparts, introduced economic sanctions against several named individuals and companies in Russia suspected of colluding with a cyber-criminal network named Evil Corp.

The sanctions cite the network's responsibility for the spreading of the Dridex malware. Since 2012, Dridex, whose earlier variants were known as Bugat and Cridex, has been spread through massive phishing attacks, bringing in the equivalent of more than half a billion Danish kroner. Assisting in the spread are the networks behind known botnets such as Crap2P and Cutwail, both of which are used as infrastructure in the phishing attacks. Dridex has also been used in targeted attacks with BitPaymer ransomware.

The indictment also illustrated how criminals who are willing to pay can buy access to infrastructure and malware run by networks such as Evil Corp. According to the indictment, an individual based in Great Britain paid an initial sum of 100,000 US dollars and then minimum 50,000 US dollars a week for access to the Dridex and Evil Corp services.

In the case of more formalized cooperation, the involved hacker groups or networks will often be specialized in narrowly defined parts of the attack or in providing defined services. This contributes to create a formal division of labour inside the criminal environment.

The division of labour enables the individual hackers or hacker group to specialize within a particular field. In many ways, this is comparable to classic production enterprises that use specialized suppliers in order to work more effectively.

Cooperation between Emotet, Trickbot and Ryuk shows how cyber criminals develop organized supply chains
Emotet and Trickbot are two known so-called Trojans that were originally developed and used independently. However, in recent years, examples have occurred of the two malwares being used in concert with the Ryuk ransomware as a kind of three step rocket.

While Emotet malware was originally designed to steal financial information from online bank clients, it is now mainly used as a tool which facilitates other cyber attacks. One of Emotet's uses includes distribution of Trickbot as a bridgehead in targeted ransomware attacks committed with Ryuk.

In July 2019, a ransomware attack cost Lake City, Florida, 460,000 US dollars in ransom. An analysis of the attack showed that Emotet had acted as the initial attack vector. Following the initial compromise, Emotet was used to distribute Trickbot, which subsequently downloaded the Ryuk ransomware. After this stage in the attack, the operators behind Ryuk were likely responsible for the actual encryption and the subsequent ransom negotiation with the victim.

The division of labour also promotes a general improvement of skills in the cyber-criminal environment, pushing the trend that specialists rather than generalists conduct cyber attacks.

The lift in competencies serves to increase the extent as well as the profit of cyber crime attacks. This is reflected in increasing profits from targeted ransomware attacks that have the potential to generate millions in ransom to the cyber kingpins.

While the trade in specific services contributes to lowering the threshold for who can commit cyber crime, it also results in a level of professionalism and specialization that increases the productivity of the actors already involved in cyber criminal activities.

The specialization also has the potential to increase the robustness of the criminal networks. For instance, rather than affecting the entire attack chain, authority crackdowns on a supplier will often only impact a limited and replaceable part of the supply chain.

Cyber criminals may harm the democratic process
US authorities have warned that ransomware attacks are one of the main threats to the November 2020 US presidential election. Attacks against authorities and software providers, including those handling voter data, could potentially sow chaos and distrust in the democratic process.

Cyber criminals are not usually driven by the prospect of influencing the US election. However, their actions may still undermine the public's trust in democracy and the electoral process. This would be the case if they choose to sell hacked accesses to state-sponsored hacker groups that want to influence the election, or if they coincidentally encrypt systems belonging to authorities that play key roles in the election.

Cyber crime, including Crime-as-a-Service, may thus indirectly pose a threat to national security. Prompted by this threat, the U.S. Cyber Command (USCC), followed by Microsoft in collaboration with a number of international actors, directed attacks in late September 2020 against the infrastructure around the TrickBot malware. Even though the disruptions caused by the attacks are likely only temporary, one of the goals of the attacks is to reduce the scope for influencing the US election through this malware.

The attacks against the TrickBot criminal network is one of the offensive measures adopted under what the U.S. Cyber Command terms as ”persistent engagement”, which is part of the US authorities' strategy to combat cyber threats. This strategy takes a more offensive approach to fighting the cyber threat – including the threat posed by criminal online groups.

Cryptocurrency contributes to the commercialization of the cyber criminal industry

Technologies such as cryptocurrency and anonymization tools have provided a profitable setting for a more advanced criminal environment with improved scope for cooperation.

The anonymity offered by cryptocurrency transactions makes it harder for authorities and IT security enterprises to track hackers via their financial transactions.

Common currency units across markets and countries also facilitate comparison of prices and trade between hackers. In this way, the use of cryptocurrency facilitates the exchange of services between criminal actors.

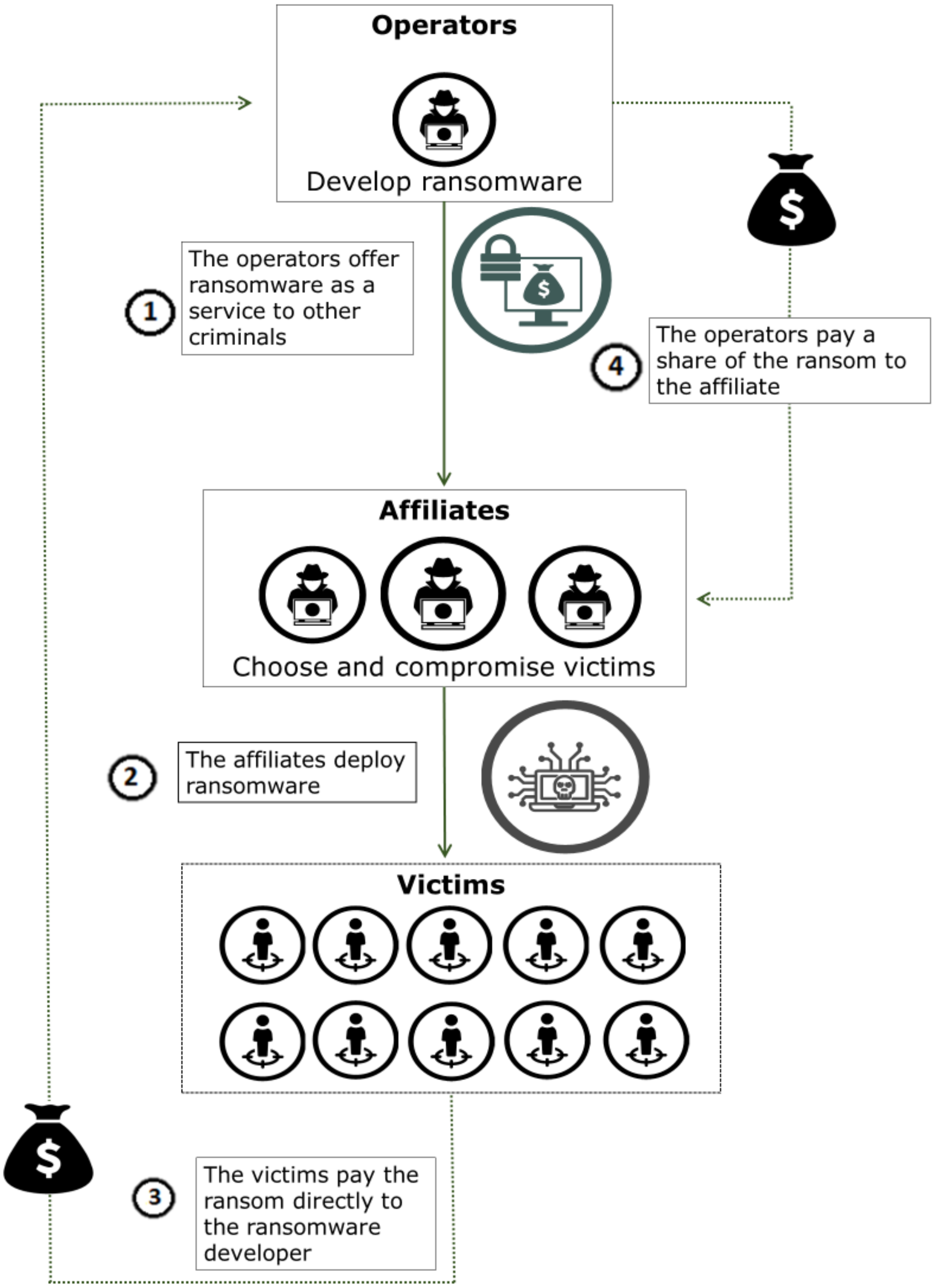
Most payments by victims of ransomware and other types of digital blackmail are made in cryptocurrency, keeping the money stream anonymous and digital throughout the cyber-criminal value chain.

Cryptocurrency also helps promote a more commercialized and specialized cyber-criminal environment as it facilitates easier access to payment for the specific cyber-crime contributions by individual actors in the supply chain.

Ransomware attacks as platform economy

Ransomware-as-a-Service (RaaS) is another example of how hacker cooperation has become more organized and long-term. In some respects, the business model behind RaaS mimics the platform economy found in legitimate markets. Transport company Uber is an example of an enterprise specialized in providing a platform for affiliates in return for a percentage of their earnings. In RaaS's case, the earnings stem from ransom payments from successful attacks.

RaaS is based on operators running a platform – primarily malware or infrastructure – that they rent out to a network of affiliated partners who use the platform for ransomware attacks. Ransoms from successful attacks are often paid directly to the operators, who subsequently funnel a percentage of the ransom back to the affiliates. Each network is different in relation to the closeness of the affiliation between affiliates and operators and in terms of specifics such as responsibility for victim contact, etc. However, in most cases, the business model will be akin to the one illustrated below:


Operators
Develop ransomware
1
The operators offer ransomware as a service to other criminals
4
The operators pay a share of the ransom to the affiliate
Affiliates
Choose and compromise victims
2
The affiliates deploy ransomware
Victims
3
The victims pay the ransom directly to the ransomware developer

Ransomware-as-a-Service business model

This business models offers advantages to both operators and their criminal affiliates. To the operators developing the malware, the model is less risky and cumbersome as their affiliates are responsible for the spreading of the malware. RaaS thus offers the operators steady earnings at a comparatively low risk.

Some ransomware is programmed not to function in specific countries, likely those where the operators are based, including the post-Soviet states. This is presumably to protect the operators against legal repercussions. In 2019 and 2020, the United States has accused Russia and China of cooperating with local cyber criminals.

To the affiliate using the malware, the platform model also offers several advantages, mainly that they are spared the effort of developing the malware used in the attacks, enabling even low-level hackers to launch cyber attacks.

GandCrab network stole platform model

GandCrab was one of the first examples of a RaaS as a platform model. Before GandCrab, ransomware groups had mostly worked behind the scenes, generally trying to avoid attention. This changed in early 2018 with the launch of the RaaS programme by the operators behind GandCrab.

The business model behind RaaS presupposes that recruited affiliates use the platform made available by the operators. GandCrab ransomware was thus launched – complete with branding, marketing and individuals managing the communication with affiliates and victims.

GandCrab thus became one of the first publicly known examples of how criminal operators make money offering a platform to affiliates who then do the manual and risky work compromising victims.

In recent years, the trend towards more professional and organized cooperation has spread to the criminal elements offering RaaS. This has made the operators behind some RaaS operations tighten their criteria when selecting affiliates to use their malware.

This is the case with the REvil ransomware that was used in several profiled attacks in 2019. REvil is based on the GandCrab concept, and much suggests that there are several overlaps between operators and affiliates involved in the two RaaS platforms. However, REvil is different from GandCrab in that the former has a stronger focus on affiliate selection. REvil is thus based on a network of handpicked qualified affiliates.

A likely contributory factor to this development is the major uncertainty related to CaaS and RaaS. As mentioned, the exchange of services among criminal elements carries the risk of the criminals themselves being scammed or exposed.

REvil is mainly used for targeted ransomware attacks in which the perpetrators blackmail public authorities and private companies for large sums by encrypting data on central IT systems. This places higher demands on the technical skills of potential affiliates and their ability to handle victims, for instance in connection with blackmail.

The tighter selection criteria thus likely focus on both trust and skills.

International cooperation to fight ransomware
The National Cyber Crime Center (NC3) under the Danish National Police cooperates with several international partners to combat ransomware.

Among its activities, NC3 is involved in the "No More Ransom" project, whose purposes include helping victims of ransomware getting their encrypted data back without having to pay ransom. The "No More Ransom" project also focuses on educating the general public on ransomware.

In the summer of 2019, Europol described how the "No More Ransom" project had helped more than 200,000 victims of ransomware, preventing more than 100 million US dollars from ending up in criminals' pockets.

Read more about the project on: www.nomoreransom.org

Development enhances threat from targeted ransomware attacks

In previous assessments, the CFCS has warned of the increasing threat from targeted ransomware attacks. The attacks are, for one thing, targeted in the sense that the hackers specifically target large or critical public authorities and private companies in the expectation that such organizations are willing to pay substantial ransoms.

The development in CaaS and RaaS platforms has contributed to increasing the threat of targeted ransomware attacks.

RaaS platforms such as REvil specialize in targeted ransomware attacks with great profit potential. Ransoms demanded in ransomware attacks with REvil far exceed the ransoms demanded in operations using GandCrab. One ransom demand went as high as 42 million US dollars in a single attack with REvil.

This reflects a general trend. In October 2019, Europol reported a drop in the overall number of ransomware attacks. However, the same period saw an increase in the average ransom amounts paid by ransomware victims to have their data decrypted.

Though these figures are subject to some uncertainty, due to the victims rarely publicizing how much they have actually paid in ransoms, the CFCS assesses that several of the publicly known cases seem to substantiate this trend.

The threat is supported by the continuous perfecting and development of products and methods. Criminal networks thus continuously update encryption tools and malware, enabling them to circumvent security measures adopted by their victims to counter such attacks.

Based on the division of tasks, the criminal industry will maintain its ability to launch broad attacks, including organized phishing campaigns, against all Internet users. At the same time, the development will likely result in some types of criminal cyber attacks becoming even more targeted. The successful attacks will thus likely become more profitable for the perpetrators and more financially damaging to the victims.

Want to read more?
For more information on the general threat of cyber crime, see "*The Cyber Threat against Denmark 2020*".

Publications are available on the CFCS website.