CENTRE FOR CYBER SECURITY

Threat Assessment

Cyber criminals rearm in the shadow of the pandemic

Content

CENTRE FOR CYBER SECURITY

Kastellet 30
2100 København Ø
Telephone: + 45 3332 5580
E-mail: cfcs@cfcs.dk

1. edition November 2020.

Key Assessment

This threat assessment is intended to inform decision-makers in private companies and public authorities of the changes in several criminal hacker groups activities in 2020. As a result of these new activities, private companies and public authorities are faced with new, serious threats from criminal hackers.

- In 2020, several criminal hacker groups upgraded their cyber tools and renewed their collaborative relationships and activities. Even though these types of changes in cyber threats are common, they have been quite significant and happen more simultaneous than usual in 2020.

- As a result of the changes, Danish private companies and public authorities are faced with criminal networks equipped with new tools and attack techniques.
- The changes have caused some criminal groups to pause their normal activities during the spring of 2020. However, the groups have now resumed their usual activities.

- The COVID-19 pandemic, pressure from public authorities and security firms and also cyber criminals' interest in targeted ransomware attacks have all – each in their own right – contributed to the changes.

Analysis

During the spring and summer of 2020, several cyber criminal groups upgraded their tools and renewed their collaborations and activities.

The Centre for Cyber Security (CFCS) under the Danish Defence Intelligence Service assesses that even though these changes in cyber threats occur regularly, the changes in 2020 have been more comprehensive and seemed to happen more simultaneous than usual.

The changes have occurred in several areas. Some hacker groups have diversified their cyber attacks to also include new types of victims, or increased their focus on the financial gains that can be achieved through targeted ransomware attacks by threatening to leak stolen data.

Other hacker groups have changed their usual malware with new malware. This is a significant change as malware is generally the most important tool in their daily activities. For multiple groups the malware is also valuable for their criminal partners.

As a result of new tools and new attack tactics, hackers have grown stronger than they were in early 2020. Consequently, Danish private companies and public authorities are faced with new, serious threats from criminal hackers.

The CFCS assesses that the changes have been driven by a number of factors; The COVID-19 pandemic and pressure from both public authorities and private security firms have each had a significant impact. The move towards targeted ransomware attacks and data leakage threats for financial gain have also contributed to the changes in the 2020 cyber threat landscape.

The changes confirm the CFCS assessment that criminal hackers are generally successful in adapting to new situations and think innovatively when they are exposed to external pressure or eye new opportunities to make a profit.

Leading groups paused their activities during the spring
During the spring of 2020, some leading criminal hacker groups temporarily suspended their cyber attacks, including operators of Emotet, GetAndGo Loader, Ryuk and BitPaymer. The groups resumed their attacks in early summer and throughout the summer of 2020.

The suspension in activities somewhat coincided with the COVID-19 lockdowns in, for instance, Russia, where several criminal hacker groups are based, according to our assessment. The hackers' ability to launch attacks has likely not been significantly affected by the lockdowns as is evident from the fact that the hackers resumed their activities in May 2020 prior to the reopening of Russia in June 2020.

We assess that the period of inactivity was mainly a result of the groups' shutdown of normal activities, likely in an attempt to make time for the significant change in activities, as outlined in this threat assessment.

The pandemic forces cyber criminals to think innovatively

The COVID-19 pandemic has fundamentally reshaped societies and changed everyday life across the globe. These changes are also affecting the cyber criminals' income opportunities.

Criminal hacker groups that have previously targeted payment systems in the hospitality sector have diversified their activities to include other sectors and new attack techniques. The hospitality sector, in particular, has been hit hard by shutdowns and restrictions following the onset of the COVID-19 pandemic, likely disrupting the income streams of criminal hackers, and, as a result, forcing them to think innovatively.

This holds true in the case of a long-standing, well-established hacker group known as Carbanak. Over the years, the group has specialised in compromising payment

systems in the hospitality and retail sectors across the world with the aim of stealing credit card information.

Following the onset of the pandemic, the Carbanak hackers diversified their regular cyber attacks. The members of the group have likely also been behind targeted ransomware attacks in collaboration with other hacker groups.

Although the Carbanak hackers are new in the ransomware attack scene and new to collaborating with these groups, the changes in their cyber attacks have created new income opportunities for them.

Sanctions led to changes

Pressure from authorities has also affected cyber criminal activities in 2020.

In December 2019, US authorities coordinated joint efforts with British authorities to introduce economic sanctions against several named individuals and private companies in Russia alleged to be in league with a cyber criminal network known as Evil Corp. The sanctions were issued against the network for its role in the spread of the Dridex malware, which has been used in targeted ransomware attacks with Bitpaymer ransomware.

Since mid-March 2020, the hacker group temporarily suspended its targeted ransomware attacks. When the group resumed its activities with new ransomware attacks in May 2020, it had replaced its regular ransomware BitPaymer with new ransomware known as WastedLocker. The fitness brand Garmin was the victim of a highly publicised ransomware attack in July 2020. According to several open sources, Garmin paid a ransom in exchange for a decryption key to unlock its systems.

The sanctions against Evil Corp and the negative publicity in connection with the sanctions may deter victims who are considering paying ransom to recover access to their compromised IT systems from doing so.

The CFCS assesses that the sanctions and the sanctions-related negative publicity have contributed to the group’s decision to replace its known ransomware with a new and unknown type.

In October 2020, US authorities warned companies against paying ransom to Evil Corp citing the sanctions, though without mentioning the new type of ransomware. The announcement was likely intended to put pressure on organizations considering paying ransom.

Attack on malware affected criminal ecosystem

An attack on the world's most widespread malware has also had a direct impact on segments of the cyber criminal ecosystem in 2020.

In February 2020, hackers from an IT security company injected a script that disrupted the use of the Emotet malware. Emotet had over a number of years had been spread to thousands of computers and IT systems across the world. The attack on Emotet prompted a 5-month pause, after which it surged back, once again becoming the most widespread malware around the globe.

The attack on Emotet affected the criminal ecosystem given that Emotet is used as a distribution tool for other malware families. In recent years, the hackers behind the Trickbot malware, used in targeted ransomware attacks with the Ruyk ransomware, have been eager users of Emotet.

In April 2020, the hackers behind the Trickbot malware failed to re-establish their supplier's network by spreading Emotet through their own network of Trickbot-infected IT systems. Thus, the roles between the two cooperation partners were briefly reversed as a result of the attack.

The Trickbot botnet also suffered an attack in September 2020. The impact of the attack was short-lived as the hackers behind Trickbot used Emotet to recover the affected Trickbot botnet, once again highlighting Emotet's key role as a distribution tool for other groups' malware families.

The U.S. Cyber Command was behind the attack against the Trickbot botnet along with several private companies. The attack against the criminal network illustrates the US authorities' increasingly offensive approach to combatting cyber threats. The attack was part of a broader effort to thwart potential attempts to influence the 2020 US presidential election through this malware.

Hackers pause their attacks to develop new ransomware

In March 2020, the hacker group behind Trickbot and Ryuk paused their targeted ransomware attacks. Ryuk has been used in attacks targeting the healthcare sector, public schools and local authorities in the United States, in particular.

I May 2020, the group resumed activities, this time using a new family of ransomware known as Conti. The group has likely had Conti at its disposal since 2019 and fully

developed it during the spring pause. Earlier this year, the group also introduced a ransomware tool that automatically steals documents containing sensitive or classified information, which the hackers can threaten to leak or resell should the victims refuse to pay ransom.

The periods of inactivity indicate that the development of Conti has been a major investment for the group. In 2019, open sources reported of incidents in which victims of Ryuk ransomware infection struggled to recover access to their systems despite paying ransom. Given that the incentive for paying ransom rests on the prospect of recovering access to the compromised systems, Ryuk may have suffered a blow to its reputation – which, in turn, may have prompted the hackers to develop new ransomware.

The development of Conti has yet to put an end to Ryuk. Following a 6-month absence, Ryuk was used in a September 2020 ransomware attack against the US-based healthcare company United Health Services.

Criminals use data leakage threats as additional pressure

Since 2019, targeted ransomware attacks have become part of the cyber threat landscape – a development that has continued in 2020 as new hacker groups and ransomware have emerged.

In 2019, the hackers behind the Maze ransomware started a new trend called "double extortion". Under this new approach, the hacker group not only launched ransomware attacks against private companies and public authorities, but it also threatened its victims with data leakage.

This new tactic has since been copied by several hacker groups in 2020, and double extortion ransomware attacks have become increasingly common. Since the spring of 2020, Maze, REvil and DoppelPaymer operators have all adopted the double extortion model, as have at least fourteen other ransomware operators.

Double extortion requires resources in the form of websites that have to be set up where hackers threaten to leak the compromised data, and marketing efforts to sell the data from non-paying victims. In June 2020, the hackers behind Maze, Ragnar Locker and Lockbit formed a data leak cooperation called Maze Cartel – illustrating once again that cyber criminals are willing to think innovatively, including in the way they cooperate.

The DDIS applies the below scale of probability

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