Federal Office
for Information Security

RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

Fourth edition of the Franco-German Common Situational Picture

Introduction

In recent years, ransomware, the encryption of data and subsequent extortion, has become one of the major threats for our modern, interconnected life. In contrast to other cyber-threats, ransomware usually has an immediate effect on the availability of services that are provided or enabled by the affected information technology (IT). Depending on the services, ransomware cannot only threaten the means of existence of a whole organisation, but in fact also an individual's life. Ransomware is therefore of high importance to both the French National Cybersecurity Agency (ANSSI) as well as the German Federal Office for Information Security (BSI).

Ransomware is commonly associated with cybercrime, because it is primarily used for financial gains. The use of ransomware by states or state level actors is of course possible, but has been observed to a much lesser extent. In this fourth edition of the Franco-German Common Situational Picture (CSP) the focus lies on the aforementioned cybercriminal use of ransomware and especially on the developments observed by ANSSI and BSI regarding the use of ransomware for maximal effect and extortion since 2019.

At the beginning, ransomware was widely used against individual users with relatively low ransom demands. Over time, particularly in recent years, ransomware became a major threat to networks of large organisations in so-called Big Game Hunting (BGH) attacks. BGH commonly refers to a ransomware attack that affects a significant part of an organisation's network. Therefore, the attackers preferably target organisations with reasonable financial solvency in order to maximise their ransom yields. Furthermore, extortion operations are often prepared in advance, in some cases even months before the actual deployment of the ransomware itself.

Since the end of 2019, the extortion attempts in BGH attacks have been amplified by the combination of encryption with other malicious methods. This so-called double extortion model was observed across different ransomware strains and cybercriminal groups. In those cases, the attackers additionally exfiltrated possibly sensitive data of the targeted organisations before starting the encryption in order to threaten the victims with either the public release of the stolen data or the auction/sale of them to undisclosed interested third parties.

These and other developments will be highlighted in this fourth edition of the CSP. In order to reflect the different challenges and risks posed by ransomware, each agency presents selected cases separately. Additionally, ANSSI and BSI summarise their national responses to the ransomware threat respectively. At the end, an outlook will be given on the risks ransomware and its accompanying extortion methods will pose in the future, and what further actions ANSSI and BSI are calling for.

Advancement of Cybercrime-as-a-Service

Cybercrime-as-a-Service (CCaaS) describes the division of work between cybercriminals: the specialisation of some cybercriminals on specific parts of the "cybercrime supply chain". The supply chain can entail virtually any part of a cybercriminal attack. From malware to bulletproof hosting[1] of infrastructure to the actual extortion, there is a threat actor that provides it as a service. Those services allow criminals with limited to no knowledge at all about malware and malware development to conduct their own cybercriminal campaigns.[2]

Ransomware-as-a-Service (RaaS) is one kind of CCaaS and consists in offering access to a ransomware, its payment and distribution infrastructures as well as a set of back-office services, all in a „ready-to-use" form. Cybercriminals who subscribe to the services of a RaaS are referred to as "affiliates". It allows them to conduct effective extortion operations at a lower cost, without necessarily having the technical skills to develop a ransomware and maintain its command and control (C2) and payment infrastructure. In exchange, a certain percentage of the earnings generated by these affiliates goes to the RaaS operators, usually less than 50%.

The RaaS can be operated in a public, restricted or private fashion. Public and restricted RaaS usually advertise on cybercriminal underground forums in order to attract new affiliates. Restricted RaaS furthermore check new applicants and require certain skills and proof before accepting them as affiliates. Private RaaS, on the other hand, operate in closed channels and commonly do not advertise their services publicly. In fact, the exclusion of RaaS-related announcements on some prominent underground forums following the US response to the DarkSide ransomware attack on Colonial Pipeline in May 2021 may increase the privatisation of RaaS in the long term.[3]

Especially since 2020, RaaS has been thriving, with more and more ransomware variants adopting this operating model. Hence, this phenomenon partially explains the continuous rise of ransomware. While this ransomware model is partially more risky for the operators, because operators have not much control over the actions of their affiliates, in general, it provides multiple benefits for the operators and affiliates alike.

If an operator actively uses the ransomware himself, the attacks by his affiliates can act as a cover for his own cyber-attacks. Furthermore, the more cybercriminals use the same malware, the more difficult it becomes to differentiate between them. This covering effect also works for the benefit of the affiliate.

Additionally, the developers of the ransomware raise their return on investment. Similar to legal software development, there are upfront costs for developing and maintaining a ransomware.

[1] Bulletproof hosting refers to network infrastructure and data centres that are established, managed and maintained to keep their users and administrators anonymous. They allow the hosting of illegal content on their infrastructure, including malware.

[2] A campaign describes an attack or an array of attacks with similar techniques over a selected timeframe. For example, multiple spam-emails for the distribution of the same malware with a similar lure are therefore seen as one spam-campaign.

[3] https://therecord.media/three-major-hacking-forums-ban-ransomware-ads-as-some-ransomware-gangs-shut-down/

General chain of infection observed since 2019

Through their routine use of legitimate post exploitation tools and the final deployment of encryption malware, ransomware attacks follow a similar infection chain.

The infection vector describes the tactics, techniques and procedures (TTPs) used by the attackers for the initial infection. Once a system or host has been successfully compromised, the attackers will usually establish some kind of backdoor in order to enable constant access to the victim's network. From here on, the attackers explore the network, compromise further hosts, and try to elevate their privileges in the network. This exploration and lateral movement is also called post exploitation, since it occurs after the initial infection. In a ransomware attack, the deployment of the ransomware and the subsequent encryption of the data commonly mark the end of the post exploitation phase, which is followed by the extortion attempt.

a. Infection vector

There are various infection vectors for ransomware attacks:

- Phishing emails: it is not uncommon for phishing emails to distribute an initial loader or banking Trojan, which is responsible for deploying the final ransomware payload[4] after propagation in the network. This type of loader can be used when the ransomware does not have the ability to automatically lateralise within a network. For example, the Clop ransomware, operated by TA505,[5] is distributed at the end of the SDBbot-Get2 infection chain. Such distribution can take place as an email attachment or a link to a malicious website in the email body. Phishing emails for the distribution of malware should be differentiated from phishing emails with the intent to harvest credentials.

- Compromised websites (watering holes): visiting a compromised website, either directly or via an email URL, can lead to the distribution of the ransomware or an intermediate payload. For example, Evil Corp uses the SocGholish framework that masquerades as a fake browser update and downloads a ZIP archive file containing the malicious Javascript file "FakeUpdates", which then initiates the infection chain.[6] In addition, a watering hole can lead to the distribution of an exploit kit: in this case, the kit seeks to exploit a vulnerability in the victim's browser and executes a payload. This payload can in turn distribute the attackers' malware.

- Poorly secured RDP access: ransomware operators particularly favour RDP access as an infection vector. For instance, compromised RDP accesses can be purchased from marketplaces on the Dark Web. Thus, some DoppelPaymer,[7] MountLocker[8] or even ProLock[9] chains of infection started by RDP hijacking.

[4] Payload is a general term that refers to malware, malicious documents and other malicious file types delivered, downloaded or distributed during a cyber-attack.

[5] https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-009.pdf

[6] https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-008.pdf

[7] https://blog.avast.com/doppelpaymer-ransomware-resurgence-avast

[8] https://blogs.blackberry.com/en/2020/12/mountlocker-ransomware-as-a-service-offers-double-extortion-capabilities-to-affiliates

[9] www.group-ib.com/blog/prolock

- Vulnerability exploitation: an organisation's network commonly hosts multiple servers and services that are accessible via the public Internet, such as Citrix servers, VPN software or even remote monitoring and management software (RMM). The exploitation of vulnerabilities in those servers and services is one common infection vector that often can be exploited in an automatic fashion. For instance, in 2020, some RagnarLocker's chains of infection started by the exploitation of Citrix server vulnerabilities or by the exploitation of vulnerabilities within RMM such as ConnectWise and Kaseya software.[10]

- Supply-chain attacks: although less frequent, these attacks should not be overlooked. They can be differentiated into network-supply-chain and software-supply-chain attacks. In a network-supply-chain attack, a threat actor compromises its victim via the network of for example the service provider of the victim. In 2019, some Sodinokibi (also known as REvil) affiliates compromised an IT service provider and through it, were able to compromise the information systems of 22 cities in Texas.[11] In a software-supply-chain attack, a threat actor compromises its victim via a malicious software update. A prominent example for such an attack is the distribution of the NotPetya malware in 2017.[12]

Access brokers represent another kind of CCaaS that is especially attractive to cybercriminals who use ransomware. Access brokers, as the name implies, provide access to a system or network. Therefore, they fulfil one essential task for any cyber-attack, that is, to break into the target's network in the first place. Since most access brokers do not engage in follow-up-activities, they can specialise on initial infections instead. A prime example for an access broker were the cybercriminals behind the malware Emotet (named TA542 by Proofpoint or Mummy Spider by CrowdStrike) that provided access to multiple different other cybercriminal groups. These cybercriminals were heavily specialised on phishing- and spam-emails for their self-developed malware Emotet.[13]

Similar to other cybercriminals, access brokers can be roughly differentiated by their skill level. On the one side, there are access brokers who commonly rely on readily available malware from for example Malware-as-a-Service (MaaS) and provide just basic level access to one or more systems. On the other hand, there are specialised access brokers who develop their own malware, craft specialised campaigns and more often than not provide a much higher level of access. Those cybercriminals, in some cases, try to target administrator accounts and central systems like the active directory. A higher level of access usually translates into easier follow-up-activities and can therefore be sold to other cybercriminals for a higher price. It is common for access brokers to cooperate with cybercriminals who use ransomware.

Because of their vital role in the cybercrime ecosystem, access brokers are here to stay. Furthermore, the cooperation between access brokers and BGH cybercriminal groups is beneficial to both of them. The access broker can expect more money for his services, since the focus of BGH is on maximising ransom payments. BGH cybercriminals, on the other hand, can focus more of their time on intensifying their extortion methods.

[10] www.bleepingcomputer.com/news/security/ragnar-locker-ransomware-targets-msp-enterprise-support-tools/

[11] https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/texas-municipalities-hit-by-revil-sodinokibi-paid-no-ransom-over-half-resume-operations

[12] https://eucyberdirect.eu/wp-content/uploads/2020/11/2017-notpetya.pdf

[13] https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-003.pdf

b. Post exploitation

Ransomware is deployed either manually or through automatic processes, allowing rapid lateralisation within the victim network: for instance, while Ryuk ransomware used to be deployed manually, a Ryuk version discovered by ANSSI in 2021 has self-replication capabilities.[14]

Even though some ransomware-attacks are prepared months in advance, in general the attackers‘ speed of execution after a successful initial infection increased overall. For example, the time from initial infection to encryption of an attack involving the loader malware BazarLoader and the ransomware Ryuk reduced in the second half of 2020 from days to just three hours in some cases.

Prior to the post exploitation phase, a specific loader or banking Trojan can be distributed as the first payload. This malicious code then allows attackers to retrieve information that facilitates subsequent lateral movement and the download of other malicious payloads. Commonly an attacker will perform the following actions before deploying and executing the ransomware:

- Privilege escalation: to escalate their privileges, attackers can perform brute force attacks, exploit software vulnerabilities or use penetration testing tools, such as for example Mimikatz, to recover legitimate credentials.

- Active Directory (AD) mapping: to discover critical information about the infected network environment like the connected devices and the roles and rights of user accounts, attackers perform AD mapping, typically by using penetration testing tools such as for example ADFind.

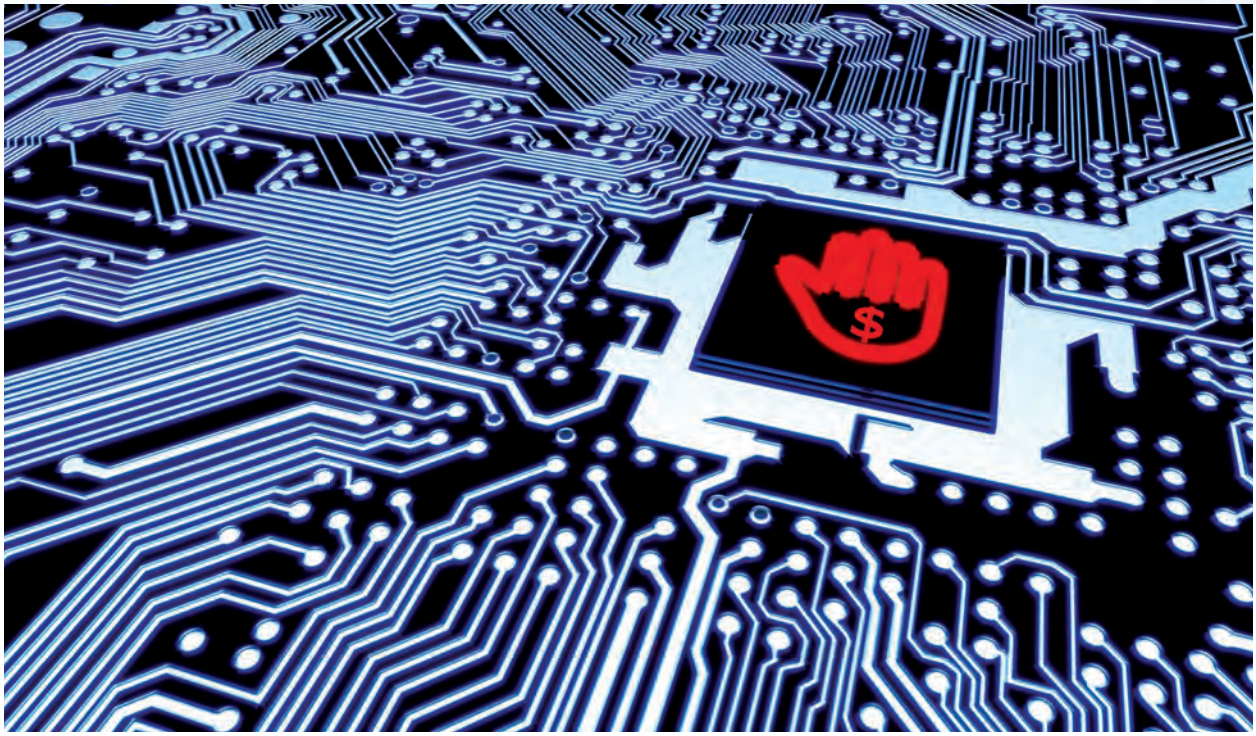
- Lateral movement: in order to move through a network laterally, an attacker may rely on penetration testing tools such as for example Cobalt Strike, Metasploit or Powershell Empire. Furthermore, an attacker may abuse legitimate tools that are built into the operating system or are commonly used for administration purposes. This kind of abuse can go unnoticed since those legitimate tools are expected to be executed in the victim’s network.

- Data exfiltration: some cybercriminals collect and exfiltrate data from a victim’s network prior to an encryption, for example via the command line tool Rclone in the form of a 7ZIP archive file to cloud service sites.

To deploy the ransomware, the attackers can use various methods like for example loaders, Trojans or scheduled tasks. Once deployed in the network, a ransomware usually stops many processes, including those related to security software, remote IT management software, remote access tools or database servers. In conjunction with data encryption, ransomware typically deletes hidden copies, which could otherwise be used to restore some of the encrypted data.

While most ransomware attacks are targeted at systems running a version of the Microsoft Windows operating system, a small yet growing number of cybercriminals has begun to deploy Linux versions of their ransomware, specifically tailored to compromise VMware ESXi servers.[15] Since it is common practice to host numerous corporate systems on just a few ESXi servers, a ransomware deployed on these hosts has the potential to significantly increase the speed and scope of the attack and therefore also the potential damage. The cybersecurity company CrowdStrike has named this new technique “Hypervisor Jackpotting”.[16]

[14] https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-006.pdf



The first known ransomware of this kind was Defray777 (also known as RansomExx or Ransom X). However, driven by the extremely high potential for damage, other cybercriminal groups have also started to deploy ESXi-targeting Linux versions of their ransomware and more are expected to follow. Currently, there are known or announced Linux versions of at least:

- DarkSide
- BlackMatter
- Sodinokibi (also known as REvil)
- HelloKitty
- Vice society
- Mespinoza (also known as Pysa)
- Babuk Locker.

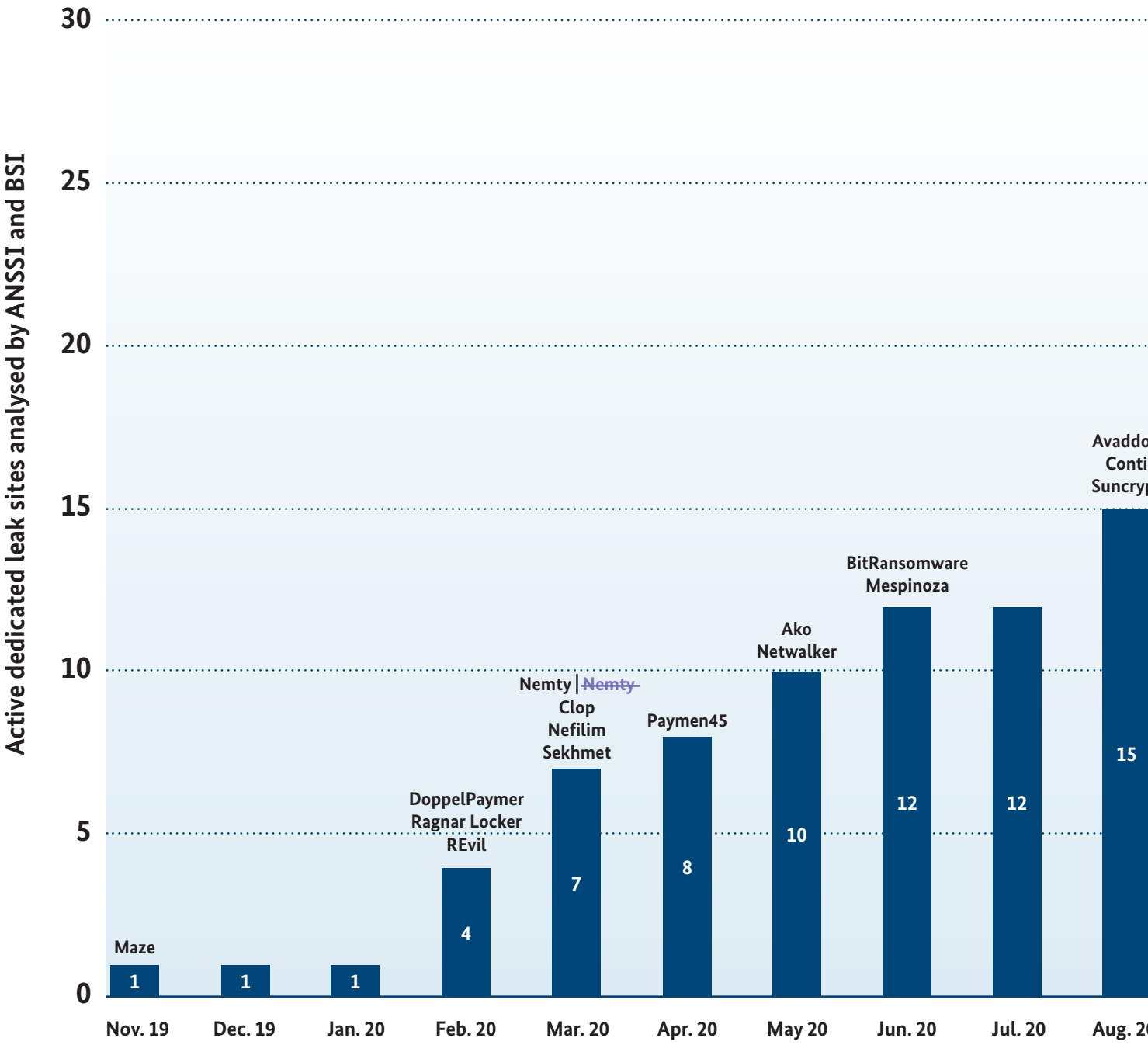
BSI has already observed several successful attacks with the ransomware Defray777 against ESXi servers of German companies since the beginning of these kind of attacks in the second half of 2020. The attackers have made forensic investigations almost impossible by demonstrating high operational security (OPSEC), using sophisticated attack methods (e.g. by staging payloads on internal servers or deploying tools in-memory-only), and often encrypting log files, which were stored on the same ESXi servers.

[15] VMware ESXi is a Type-1 hypervisor (aka "bare-metal hypervisor") and part of VMware's virtualisation platform vSphere. ESXi hypervisors are often centrally managed through the Server-Management-Software VMware vCenter.

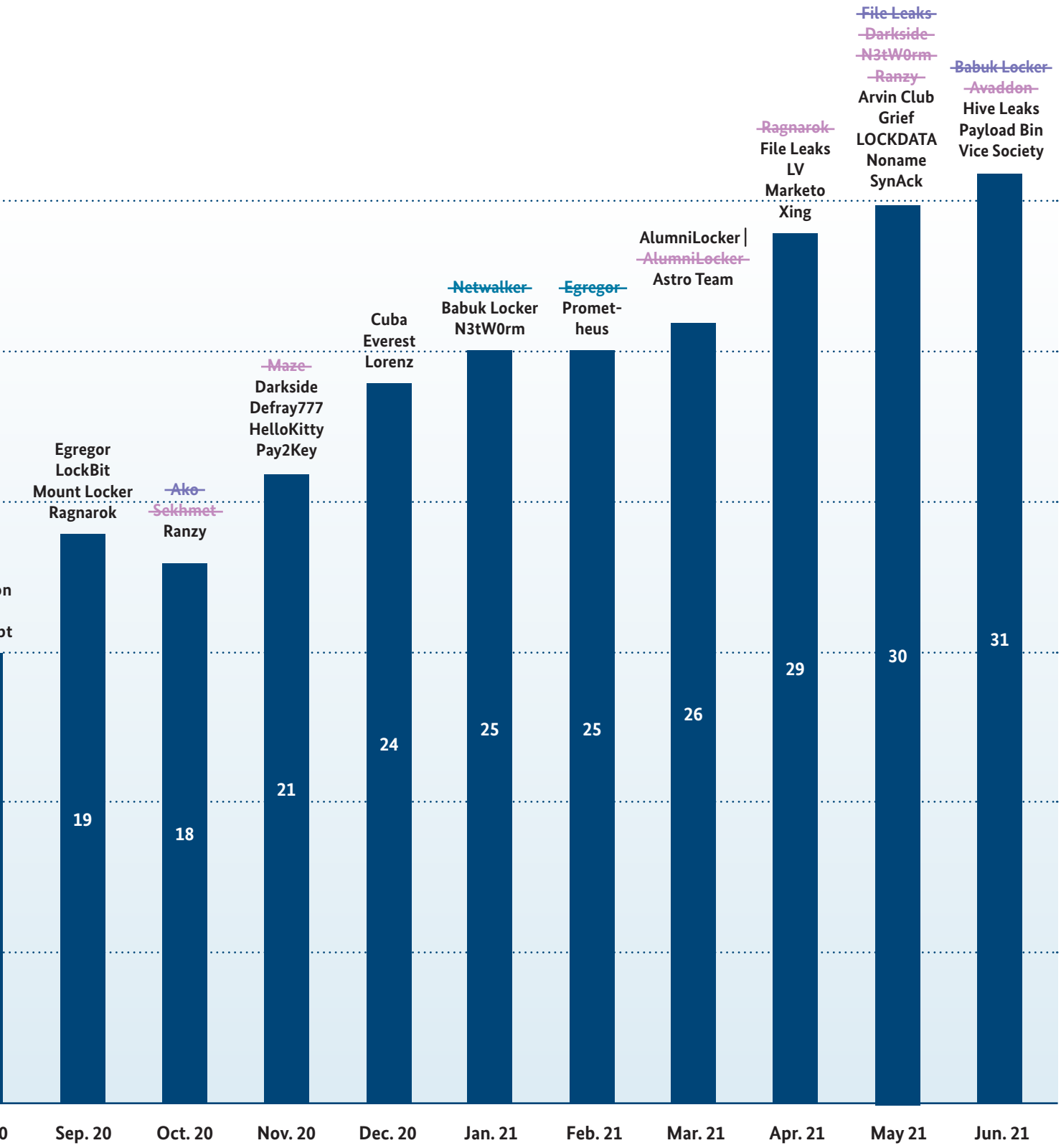
[16] https://www.crowdstrike.com/blog/carbon-spider-sprite-spider-target-esxi-servers-with-ransomware/

Active dedicated leak sites analysed by ANSSI and BSI over time

Diagram 1: The diagram shows the adoption of dedicated leak sites for ransomware attacks over time. The diagram only includes active leak sites analysed by ANSSI and BSI and is therefore considered an extract of all possible dedicated leak sites. The presented chronology is an approximation.



DLS identified: DLS name
DLS seized: ~~DLS name~~
DLS rebranded: ~~DLS name~~
DLS abandoned: ~~DLS name~~



Extortion

Once the encryption is complete, a ransom note is dropped on the encrypted systems coercing the victim to contact the attackers either by email, or through an .onion site associated with the ransomware, or via an alternative site that does not require Tor[17] to be installed. Payments can be made through a payment gateway hosted on an .onion site or by sending funds directly to the cryptocurrency wallet address provided by the attackers in the ransom note or during the negotiation with the victim.

The amount of ransom varies depending on both the ransomware and the victim. Ransomware operators, especially those who carry out BGH attacks, are often open to negotiating the ransom amount. For example, the DarkSide data leak site had an exclusive access dedicated to negotiation companies in 2021, offering discounts on the amount of ransom demanded from their customers. Negotiation companies, as the name implies, act as a negotiator between the victims and cybercriminals.

The vast majority of the attackers demands payment in convertible virtual currency (CVC), specifically Bitcoin. Although Bitcoin transactions can sometimes be traced and allow law enforcement to track the recipients, it remains the preferred choice of the attackers as it is the most common one and, hence, the easiest to obtain for the victims. However, some ransomware operators sometimes ask for payments in anonymising cryptocurrencies, such as Monero. Transactions in this type of cryptocurrency are known to be less traceable. Sometimes, attackers even offer discounts on the ransom amount to victims who are willing to pay in this way. For example, since April 2020, ransom demands after a Sodinokibi encryption could be paid in Monero. If the victim wished to pay in Bitcoin, the ransom amount increased by 10%.

To incentivise victims to pay the ransom, the operators of the Maze ransomware introduced the principle of double extortion with a dedicated leak site (DLS) in November 2019. A dedicated leak site is essentially a website that is operated by cybercriminals in order to publicly extort victims and in some cases communicate with the public in general. As such, a DLS mainly consists of a list of alleged victims. If those victims refuse to pay the ransom, the cybercriminals often publish an ever-increasing amount of stolen data from the alleged victim's network. In some cases, the cybercriminals try to sell or auction the data to the highest bidder first.

Even though Maze popularised the combination of ransomware with a DLS, it is not the first ransomware that tried double extortion. The US City of Baltimore confirmed a major cyber-security incident on 7 May 2019.[18] Large parts of the city's network were infected by the ransomware RobbinHood and subsequently encrypted. During the negotiation phase of this ransomware attack, the perpetrators temporarily published screenshots of potentially sensitive information in reaction to a public statement that no sensitive data had been stolen. The City of Baltimore eventually decided against paying a ransom. It is unknown whether the attackers actually stole data before encryption or not. Nevertheless, to date this is the first observed case in which the threat of a data leak was raised during a negotiation phase of a ransomware attack.

[17] Tor, short for The Onion Router, is free and open-source software for enabling anonymous communication. Websites hosted via Tor are referred to with .onion addresses.

[18] https://statescoop.com/robinhood-ransomware-knocks-out-city-services-in-baltimore/; https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1/

The diagram shows the amount of active DLS over time that have been analysed by ANSSI and BSI and are known to publish data stolen during a ransomware attack or were operated by threat actors that are usually associated with ransomware. In many cases, it is impossible to determine the exact date a DLS became active or inactive. For a particular DLS, the publicly available dates may vary between sources; therefore, the chronology of the identifications depicted in the diagram is an approximation. Furthermore, not every ransomware that is known to steal and publish data, maintains a DLS. For example, the ransomware Prolock and Snake (also known as Ekans) are known to also steal data and publish it via posts on cybercriminal underground forums, but there is no known DLS thus far.

Since February 2020, the count of dedicated leak sites has been steadily rising. The rise of active DLS reflects how more and more cybercriminals adopted double extortion as an extortion threat over time. This proliferation of methods and techniques is an overarching trend in the cybercriminal ecosystem.

To further pressure victims, ransomware operators may:

- Threaten to release some of the stolen information to the media, as the operators of Egregor did.[19]
- Auction the exfiltrated data on a dedicated auction space, as the operators of RagnarLocker and Sodinokibi did.
- Threaten victims with retaliation in the form of Distributed Denial of Service (DDoS) attacks, as the operators of SunCrypt and Avaddon did.
- Harass victims, their customers, partners and sometimes their service providers over the phone, as the operators of DoppelPaymer did.[20]
- Threaten to inform General Data Protection Regulation authorities about the compromise and data leak.

Data exfiltration ahead of encryption has become so commonplace that it could evolve into a recurring substitute for encryption in the future. Indeed, in December 2020, cybercriminal attackers exploited several 0-day vulnerabilities in Accelion's file transfer application to install the Dewmode webshell. Beginning in January 2021, several Accelion customer entities received emails threatening them to publish exfiltrated data from Accelion's application on the Clop dedicated leak website if a ransom was not paid.[21] Similarly, in mid-2021, Babuk operators hinted that they would stop encrypting information systems and focus on data exfiltration, always for extortion purposes.[22]

It should be noted that paying a ransom does not ensure the eviction of attackers from the compromised system, meaning that clean-up operations and the implementation of measures to raise the security level of the information system will be necessary in all cases. Furthermore, paying the ransom does not guarantee that the victim will receive the decryption key or that the potentially exfiltrated data will be deleted or not used for malicious purposes in the future.

[19] https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-007.pdf

[20] https://www.zdnet.com/article/fbi-says-doppelpaymer-ransomware-gang-is-harassing-victims-who-refuse-to-pay/

[21] https://www.bleepingcomputer.com/news/security/global-accellion-data-breaches-linked-to-clop-ransomware-gang/

[22] https://www.bleepingcomputer.com/news/security/babuk-quits-ransomware-encryption-focuses-on-data-theft-extortion/

Victimology

Regarding non-targeted ransomware attacks, no industry or geographical area is spared. Any company, institution or individual with access to the Internet can be infected by ransomware if they have not implemented basic security measures.[23] Regarding BGH attacks, companies and institutions whose business interruption may lead to important economic, industrial or social consequences are particularly targeted by cybercriminal groups. Nevertheless, it is commonly reported that most ransomware does not target entities located in the countries of the Commonwealth of Independent States (CIS).

ANSSI and BSI have observed the recurring targeting of the following business sectors or entity types in particular:

- Local governments: they have been particularly targeted by attackers since 2019. For example, during 2020, the DoppelPaymer ransomware compromised at least five cities, including two French town halls. Possible reasons for this increasingly frequent targeting may be the low level of security of information systems in this type of organisation, a history of ransom paid by cities, making these targets attractive and profitable for attackers, the presence of sensitive data that may weigh in favour of paying the ransom, as well as the fact that the disruption of business is difficult for city councils to bear given the rapid social and political impact.

- The education sector: in the United States, it is the second most coveted target after local authorities.

- The healthcare sector: in 2020, especially in the context of the COVID-19 pandemic, hospitals may have been more prompt to pay the ransom given the critical need for business continuity. Some Ryuk operators are particularly targeting the sector, having been responsible for nearly 75% of the ransomware attacks on the US healthcare sector in October 2020, as well as attacks on two French hospital centres in February 2021[24]. Nevertheless, several ransomware operators have pledged not to attack healthcare facilities.[25]

- Digital services companies: an entity of this category can be targeted to reach one or more specific victims among its customers, as well as being an end victim itself, with the impact of encrypting its data and potentially those of its customers. The consequences can be particularly serious if the provider has not properly partitioned its infrastructure and customer data. For example, in January 2020, a French IT provider, specialised in services dedicated to small and medium-sized enterprises (SMEs), was compromised by a ransomware, which spread on its customers' networks through a monitoring tool. 200 companies in Central-Eastern France were affected to a greater or lesser extent.[26] Those attacks illustrate the danger of a systemic impact of ransomware that, by targeting subcontractors or key companies in a sector of activity, could one day destabilise several large enterprises, an entire sector of economic activity or even a specific geographical area.

[23] E.g. cold backups, phishing awareness, software updates on their connected machines, antivirus, etc.

[24] https://www.france24.com/en/europe/20210216-cyber-attacks-hit-two-french-hospitals-in-one-week

[25] https://www.bleepingcomputer.com/news/security/ransomware-gangs-to-stop-attacking-health-orgs-during-pandemic/

[26] https://www.channelnews.fr/des-clients-de-xefi-attaques-par-un-cryptolocker-94901

Selected Cases

On an international scale, ransomware attacks have become a daily occurrence with ever-increasing frequency and impact. ANSSI and BSI will therefore only highlight some of the more notable ransomware attacks.

Ryuk ransomware attacks against French hospitals

In the month of February 2021, two French hospitals were paralysed by Ryuk ransomware attacks. Ryuk is a ransomware that appeared around August 2018, is dedicated to BGH attacks and devoid of DLS. One of its users, the activity cluster named UNC1878 by FireEye, discovered early 2020 and responsible for 83% of Ryuk ransomware's attacks in 2020, is particularly inclined to target hospitals and is believed to be the source of these attacks against two French hospitals.[27]

Not only were the attacks conducted within a short time frame, with only a week between both, but they also shared common characteristics. Both of the targeted hospitals were of similar size; between 1,000 and 2,500 beds. While neither were spearheading regional efforts, each was of significant local importance, notably because the COVID-19 vaccination campaign was underway. The attackers also used heavily obfuscated code in each attack.

Both attacks differed in one crucial aspect: the methodology used to spread the malware. In one case, the attacker opted for a – now common – way of deploying their ransomware. That is to say, they illegitimately connected to an account with administrative privileges and used a legitimate system administration tool (PsExec) to deploy the ransomware on each machine of the compromised active directory domain. The method used in the other attack proved to be fairly uncommon. The ransomware was set up to act as a worm, which means it had self-replicating capabilities. This novelty made it difficult for the hospital's IT staff to explain and remediate the situation.

Despite this difference, both attacks had critical impacts for the hospitals. The encryption of data rendered medical and administrative applications useless or prevented the staff from accessing them altogether. This had very real consequences for patients. As their health records became unavailable, checking on their prior hospitalisations or current treatments became impossible or very time consuming, with medical staff returning to pen and paper for this tracking. This turned out to be particularly difficult in the case of critical and time sensitive prescriptions such as those of chemo and radiotherapies. The number of emergency patients and surgeries had to be limited, as the sterilisation machines were functioning at a slower pace and planning could not be automated. The impact of the unavailability of administrative applications, that register billing and social security data, should also not be underestimated, as they are usually key for transferring data between different services within the hospital. Another important point is that the usual communication channels used to supply the hospital or exchange medical data with third parties were also down, which hampered even further daily operations.

ANSSI experts were able to initiate the recovery process and later on guide both hospital teams through the successive challenges the process entails. This lengthy process took over a month before the medical staff could return to business as usual.

[27] https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-006.pdf

DoppelPaymer ransomware attack against German university hospital

One German university hospital became victim of a major incident in September 2020. This hospital treats around 50,000 inpatients and around 300,000 outpatients per year. It is therefore above the defined thresholds according to the BSI-KritisV and hence considered as critical infrastructure.

On 10 September 2020, a cyber-attack including the deployment of ransomware was detected. Multiple central servers were affected by the ransomware known by the name DoppelPaymer. Following the outage of services provided by those central servers, the hospital was forced to close its accident and emergency department, cancel operations and other medical treatments.[28]

However, the ransom demand left behind by the perpetrators was addressed to a different institution, which led to the assumption that they falsely attacked the university hospital. Considering this possibility, German law enforcement contacted the attackers and informed them about their actual victim. According to the Ministry of Justice of the state of North Rhine-Westphalia,[29] the attackers handed over the necessary decryption keys, likely after realising their mistake. With backups and the decryption keys at hand, the university hospital started to rebuild their IT infrastructure. After 13 days, the hospital was able to provide emergency services again on 23 September 2020.

Ryuk attack against a major French municipality

Mid-January 2021, a major French municipality informed ANSSI of an ongoing ransomware attack. A strand of the Ryuk ransomware was deployed on the urban community's network and locked all servers, domain controllers and about a third of all workstations. Due to the network configuration, this breach and the following wave of encryption impacted not only the town hall offices, which had to turn back to pen and paper when dealing with citizen affairs, but also multiple other municipal establishments. Furthermore, some services related to the city's video surveillance system, automatic instrumentation for monitoring water management and optimization of traffic light sequences were also rendered unavailable.

Major disturbances arose from this attack and it was crucial to recover, as quickly as possible, the most critical services. With the assistance of ANSSI and a commercial partner, the municipality initiated a recovery plan. A new infrastructure was put in place with various environments isolated within the network. 11 days after the ransomware was activated, those environments were functional and the critical services were recovered thanks to safe and undamaged backups. While the wages of municipal employees were paid in time, some social benefits were disbursed with some delay.

It was established, through the forensic investigations, that the perpetrators of this attack used a compromised account of one of the city's suppliers to breach the urban community's network. The methodology and offensive tools used showed no major innovation and correspond to what is traditionally observed in this type of attack. ANSSI followed through its assistance by providing regular audits of the municipality's Active Directory and counselling on ways to further secure it.

Grief ransomware attack against German county

On 6 July 2021, the German county Anhalt-Bitterfeld became victim of a ransomware attack. The attack resulted in the outage of numerous services provided by the affected public administration. Emergency services were not impacted.[30]

[28] https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2020/UKDuesseldorf_170920.html

[29] https://www.landtag.nrw.de/portal/WWW/dokumentenarchiv/Dokument/MMV17-3855.pdf

Ransomware attacks against local administrations are relatively common. Compared to similar cases, however, this incident stands out, because it is the first time a county officially declared a disaster situation in order to deal with a cyber-attack. This is a formal act in Germany that allows the affected local administration more room to manoeuvre and access to more resources such as the support by other public authorities on the local and federal level.[31]

Following the ransomware attack, data presumably stolen during the attack was published on the dedicated leak site attributed to the ransomware Grief. Grief is believed to be the successor ransomware to DoppelPaymer. From time to time, some cybercriminals abandon their ransomware and return under a new name. Such rebranding methods impede investigations and hamper adequate first response countermeasures.

DarkSide ransomware attack against US pipeline company

Although it appeared in August 2020, DarkSide became a RaaS at the beginning of October 2020. The attackers behind the ransomware announced to be former affiliates of older RaaS and have pledged not to attack small businesses so as not to bankrupt them, nor to attack hospitals, schools, universities, government entities and non-profit organisations.

On 7 May 2021, one of DarkSide's affiliates compromised the information system of Colonial Pipeline, a company that manages the delivery by an oil pipeline of 45% of the East Coast's fuel, causing a massive shutdown of Colonial Pipeline's activities. As a consequence, the US Environmental Protection Agency issued an emergency fuel waiver to compensate for the shortage impacting 17 states and the District of Columbia, linked to the cessation of activity of around 8,800 kilometres of fuel pipeline. Moreover, the Federal Motor Carrier Safety Administration declared a regional emergency to provide oil supply through commercial motor vehicle operations.

After having paid the USD 5 million ransom asked by DarkSide operators, and helped by the Federal Government, Colonial Pipeline gradually restored its operations and resumed its normal activity one week after the cyber-attack.

This attack marked a turning point. As a reaction to it, US President Joe Biden stated that the United States planned to disrupt the hackers behind the cyber-attack.

The day after this announcement, DarkSide's operators declared that they had lost control over their web servers and that some of the cryptocurrency funds they had obtained from ransom payments had been withdrawn from their payment server and transferred to an unknown wallet. As such, the US Department of Justice stated that it had seized the major part of the ransom paid by Colonial Pipeline. Nonetheless, as there has not been an official confirmation of the US authorities' involvement regarding the loss of control over DarkSide infrastructure by its operators, this announcement could also have been an "exit scam", i.e. a way for the DarkSide operators to shut down their operations. A rebranding or the use of another ransomware by the same actors is therefore possible. In fact, in August 2021, Chainalysis confirmed that DarkSide has reappeared as BlackMatter.

As a consequence of the cyber-attack on Colonial Pipeline, some cybercrime forums within the cybercriminal ecosystem ("exploit", "XSS") decided to ban ransomware advertisements and some ransomware operators announced that they would stop advertising their RaaS and become private.

[30] http://www.anhalt-bitterfeld.de/de/meldung-detail/presseinformationen-zum-cyber-angriff-auf-die-kreisverwaltung.html
[31] http://www.anhalt-bitterfeld.de/de/meldung-detail/cyberangriff-auf-landkreisverwaltung.html

Sodinokibi ransomware attack against several service providers worldwide

On 2 July 2021 and the following days, a coordinated ransomware attack with Sodinokibi (also known as REvil) against several service providers and their respective customer bases occurred worldwide. In this incident, the criminals exploited multiple vulnerabilities in Kaseya's Virtual Systems Administrator (VSA). Service providers use this software to administrate systems and networks of their customers.[32]

The vulnerabilities enabled the attacker to distribute Sodinokibi through Kaseya VSA itself. Since the VSA client is installed on all administrated systems, the attacker was able to skip the lateral movement that would normally occur after the initial infection. Uncommon to other ransomware attacks with Sodinokibi, this ransomware attack was tailored to maximise operational speed. Otherwise, the recommendation of Kaseya to temporarily disable the exploited VSA servers would have probably limited the success of this ransomware campaign.

Following the encryption with Sodinokibi, the attacker tried to extort the affected service providers as well as their customers. Additionally they made a ransom demand to Kaseya for a general decryption tool that could be used on all encrypted systems.

On 13 July 2021 the infrastructure, including the dedicated leak site as well as payment servers behind Sodinokibi, went offline without prior notice. Any victim that had negotiations ongoing was hence unable to obtain a decryption tool by paying the ransom. On 22 July 2021, Kaseya announced they had gained access to a general decryption tool for this ransomware campaign through an undisclosed source. The decryption tool was subsequently checked by an IT security provider and distributed to customers of Kaseya.

Law enforcement actions

In 2021, several internationally coordinated law enforcement actions against well-known cybercriminal groups and their respective malware were successful. Two of those cases will be highlighted in the following sections.

[32] https://www.zdnet.com/article/updated-kaseya-ransomware-attack-faq-what-we-know-now/

[33] https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-003.pdf

Emotet

The malware Emotet was a downloader for the malware of several other cybercriminals. The cybercriminals behind Emotet therefore acted as an access broker. The infection chain consisting of Emotet, TrickBot and Ryuk was particularly active and resulted in multiple major cybersecurity incidents in Germany and France as well as worldwide.[33]

On 26 January 2021, the Attorney General's Office in Frankfurt am Main and the Federal Criminal Police Office (BKA) led an internationally coordinated law enforcement action against Emotet, its infrastructure and the responsible cybercriminals. The action resulted in a comprehensive takedown of Emotet and the extensive confiscation of evidence.[34]

In order to assess and inform all victims of their compromise, updated communication parameters were delivered to systems infected with Emotet. These changes revoked access to infected systems for the cybercriminals and made sure that infected systems only communicated with infrastructure specifically hosted for collecting evidence.

Egregor

In February 2021, shortly after the dismantling of Emotet, the ransomware Egregor was targeted by a joint police operation led by France and Ukraine. Egregor was allegedly operated by the same cybercriminals as the Maze ransomware and had been operating under the RaaS model since September 2020. Several attacks against large French companies warranted a law enforcement operation, with the help of private-public sector partnerships. Three members of the cybercriminal group operating Egregor were thus arrested, confirming the end of the ransomware activity.

[34] https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2021/Presse2021/210127_pmEmotet.html

National responses

a. How does ANSSI deal with/react to the ransomware threat?

Because of its large impact on its victims, ransomware is considered to be one of the most serious cybercriminal threats. Over the years, ANSSI has witnessed a steep increase in both the frequency and sophistication of such attacks. Indeed, the number of ransomware-related incidents grew by 255% between 2019 and 2020. Amongst them, the number of attacks paralysing the majority or entirety of the systems rose by 80%.

Because of the nature of the threat, the entire French ecosystem is mobilised. ANSSI works closely with the judiciary system, law-enforcement agencies, as well as with private service providers who intervene in cases of incident response.

In order to appropriately adapt to these new forms of cybercrime, ANSSI's strategy has been adjusted both in terms of prevention and response.

Since 2019, ANSSI has led a multi-pronged prevention effort by:

- Publishing generic or ransomware-specific best practices guides (cf. appendix).
- Raising the public's awareness of this threat.
- Ensuring that the services and products provided by the private sector match operational needs.
- Producing cyber threat intelligence (CTI) on cybercriminal groups and publishing technical analysis and TTPs in order to detect threat actors (cf. appendix).

In terms of cyber defence and response, ANSSI:

- Disseminates information on ransomware attacks via various channels, including the CERT-FR website, to reach as many people as possible through analysis of the functioning of the groups but also transmission of technical elements to detect them.
- Searches for French victims via different means and channels: CERT-FR may thus be led to alert an entity about a potential ongoing compromise of which the entity would not yet be aware.
- Actively scans for systems susceptible to the most used vulnerabilities and thus anticipate attacks.
- Assists victims who reach out for help. In some cases, ANSSI will send teams on premise to guide the victim on crisis management, forensic analysis and remediation. Agents can be mobilised for up to several weeks. While ANSSI cannot guarantee this type of mobilisation for each incident, it will at least provide first aid to the victims and reorient them towards private incident response service providers.

The agency is not in a position to intervene directly for the benefit of all, but it is developing relays to disseminate useful information and so that other actors are able to help entities suffering from this type of attack.

[35] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/Nationales-IT-Lagezentrum/Nationales-Cyber-Abwehrzentrum/nationales-cyber-abwehrzentrum.html

[36] E.g. https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/verbraucherinnen-und-verbraucher_node.html

[37] https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/Service-fuer-KRITIS-Betreiber/UP-KRITIS/up-kritis_node.html

b. How does BSI deal with/react to the ransomware threat?

Since 2016, BSI has assessed ransomware to be a considerable threat to the cybersecurity of governmental bodies, the economy and the public in general – even more so since ransomware attacks started to focus more on organisations. Nevertheless, even in the age of BGH there are still ransomware-campaigns targeted at individual citizens. Therefore, BSI employs a multitude of measures to combat ransomware, to raise situational awareness and to establish cybersecurity standards across different sectors of the economy.

Cooperation and exchange of information is integral in an ever-changing threat landscape. That is why BSI works closely together with national as well as international CERTs and CSIRTs. Furthermore, BSI is a core member of the National Cyber-Response-Centre.[35]

BSI advances a variety of prevention efforts by:

- Raising awareness of ransomware and cyber-threats in general through recurring publications (cf. appendix) and targeted public relations campaigns.[36]
- Establishing and fostering public-private cooperation between providers of critical infrastructures, their unions and responsible governmental agencies (UP-KRITIS).[37]
- Supporting the Alliance for Cyber Security[38] and establishing the Cyber-Security Network for voluntary cyber-security experts.[39]

In terms of cyber defence and response, BSI:

- Cooperates as CERT-Bund nationally with more than 45 CERTs from the economy, academia and government in the CERT-Verbund association.
- Cooperates as CERT-Bund together with CERT-FR internationally as a member of the European CSIRT-Network and various other groups such as the International Watch and Warning Network (IWWN) or the global Forum of Incident Response and Security Teams (FIRST).
- Shares and warns different target groups via a multitude of channels like CERT-Verbund, the Alliance for Cyber Security, UP-KRITIS, Internet service providers or, in case of a credible threat, directly, if possible.
- Gathers information about systems that are susceptible to known vulnerabilities in order to inform the operators of those systems via their internet service provider.
- Protects the network of the federal administration with various detection capabilities in order to prevent ransomware-attacks and other cyber-attacks as early as possible.
- Provides first-aid-documents to victims of ransomware. Additionally BSI can give remote advice on how to proceed. In certain cases, institutions like critical infrastructures, federal administration and highly prominent cases can receive direct support from the BSI on site with a mobile incidence response team and with forensic analyses.

BSI is dedicated to continuously adjusting and improving its preventive, detective and reactive measures and efforts in accordance with the ever-changing threat landscape. Cooperation on bilateral levels like between CERT-FR and CERT-Bund or in the form of associations are integral for BSI to stay on top of the threat landscape.

[38] https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Home/home_node.html

[39] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber-Sicherheitsnetzwerk/cyber-sicherheitsnetzwerk_node.html

Outlook and Conclusion

The revenue generated by ransomware attacks and the emergence of insurance and negotiation companies validating their business model suggests that the ransomware phenomenon will continue to grow in the coming years. Specifically, the increase in BGH campaigns is aided by cybercriminals' efforts to secure ransom payments. The increase in the number of ransomware attacks is also related to the increase in the number of attackers, facilitated by the RaaS model as well as a cybercriminal ecosystem providing support at any point in the infection chain.

Considering the publicly visible success some cybercriminals have had in recent years, other and new criminals will be attracted into this space time and time again. This way, even though some criminals cease their operation or are arrested for their crimes, new ones will take their place or they will return under a different name.

Ransomware is a relatively high risk – high reward activity compared to other cybercriminal threats. Since a ransomware attack is immediately observable by the victim and experiences rising levels of scrutiny by law enforcement, any cybercriminal with insufficient operational security will be caught eventually. However, those criminals that can persist are likely to grow in skill level and available resources.

A ransomware attack can have real-world consequences: for example, the loss of operations, sometimes permanently, experienced by many victims, or the exfiltration of sensitive or confidential data that can jeopardise reputations, merger and acquisition transactions, ongoing projects, or even national security, for example in the case of attacks targeting defence contractors. Ransomware attacks can therefore no longer be relegated to the level of simple profit-making attacks, as their sophistication, their interest in the victim's data and the loss of business continuity they cause bring them closer to espionage or sabotage attacks traditionally associated with state-level attackers.

Ransomware is also within the reach of state-level or hacktivist attackers, who may use it to monetise their intrusion as a secondary motivation, to erase their traces, or even for destabilising purposes. These attackers also have the possibility to hire the services of cybercriminals and to consult or buy the data they exfiltrate.

In order to keep ransomware in check, it is fundamental to cooperate nationally and internationally across jurisdictions. The takedowns of Emotet and Egregor are prime examples of what can be achieved. Just as important is the recognition of IT security as an integral part of any digital development. IT security is a continuous battle. Therefore, continuous awareness and investments by every participant in our modern interconnected society are vital.

Collection of further reports, guidelines and supporting documents

Listed below are links to different reports and publications by ANSSI and BSI concerning ransomware. Some of those publications are only available in the respective national language.

Ransomware in general

ANSSI, English, Ransomware attacks, all concerned. How to prevent them and respond to an incident:
https://www.ssi.gouv.fr/en/guide/ransomware-attacks-all-concerned/

ANSSI, French, État de la menace rançongiciel à l'encontre des entreprises et des institutions:
https://www.cert.ssi.gouv.fr/cti/CERTFR-2021-CTI-001/

ANSSI, English, The Egregor ransomware:
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-007.pdf

ANSSI, English, The Ryuk ransomware:
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-006.pdf

ANSSI, English, The Malware-as-a-Service Emotet:
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-003.pdf

ANSSI, French, Infrastructure d'attaque du groupe cybercriminel TA505:
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-002.pdf

ANSSI, English, Development of the activity of the TA505 cybercriminal group:
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-009.pdf

ANSSI, English, The malware Dridex: origins and use:
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-008.pdf

ANSSI, English, Attacks involving the Mespinoza/Pysa ransomware:
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-003.pdf

ANSSI, English, BitPaymer/IEncrypt ransomware:
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2019-CTI-006-EN.pdf

ANSSI, French, Informations concernant les rançongiciels Ryuk et Lockergoga:
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2019-CTI-001.pdf

BSI, German, Ransomware:
Managementabstract Fortschrittliche Angriffe – Neue Qualität aktueller Angriffe und Prognose:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware_Managementabstract-Angriffe.pdf

BSI, German, Ransomware:
Bedrohungslage, Prävention & Reaktion 2021:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware.pdf

In urgent cases

BSI, German, Ransomware:
Erste Hilfe bei einem schweren IT-Sicherheitsvorfall:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware_Erste-Hilfe-IT-Sicherheitsvorfall.pdf

BSI, German, Qualifizierte Dienstleister für DDoS-Mitigation und APT-Response:
https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Informationen-und-Empfehlungen/Informationen-und-weiterfuehrende-Angebote/Qualifizierte-Dienstleister/qualifizierte-dienstleister_node.html

BSI, German, Ich habe einen Vorfall – Checkliste Organisatorisches:
https://www.bsi.bund.de/DE/IT-Sicherheitsvorfall/Unternehmen/Ich-habe-einen-IT-Sicherheitsvorfall-Checkliste-Organisatorisches/ich-habe-einen-it-sicherheitsvorfall-checkliste-organisatorisches_node.html

BSI, German, Ich habe einen Vorfall – Checkliste Technik:
https://www.bsi.bund.de/DE/IT-Sicherheitsvorfall/Unternehmen/Ich-habe-einen-IT-Sicherheitsvorfall-Checkliste-Technik/ich-habe-einen-it-sicherheitsvorfall-checkliste-technik_node.html

Imprint

Published by: Bundesamt für Sicherheit in der Informationstechnik (BSI)
53175 Bonn, Germany

Source: Federal Office for Information Security (BSI)
Section WG24 – Cyber Security for Citizens; Public Relations
Godesberger Allee 185 – 189
53175 Bonn, Germany
Phone: +49 (0) 228 99 9582-0
e-mail: bsi@bsi.bund.de

Agence nationale de la sécurité des systèmes d'information
Secrétariat général de la défense et de la sécurité nationale
51, boulevard de La Tour-Maubourg
75700 Paris 07 SP, France
Phone: +33 (0)1 71 76 85 85
E-Mail: communication@ssi.gouv.fr

Last updated: November 2021

Item number: BSI-LaB21/002

Image credits: S. 1, Rückseite: AdobeStock© Pixels Hunter; S. 2: AdobeStock© Suttipun;
S. 7: AdobeStock© beebright; S. 16: AdobeStock© ponsulak;
S. 17: AdobeStock© Gorodenkoff; S. 22: AdobeStock© kamiphotos