Bundeskriminalamt

BKA

Cybercrime

National Situation Report 2019

Table of Contents

1 Preliminary Remarks

The Police Crime Statistics (PCS) cover known offences for which the police investigations have been concluded. These statistics thus reflect police recorded crime.

It must be assumed that the number of unreported and unrecorded cybercrimes is far above average, as can be inferred from the following aspects, some of which are specific to this field of criminal activity:

- Since more and more technical security devices are installed, many criminal acts committed on the Internet do not go beyond the attempt phase and are not noticed by the victims.
- The persons affected do not realise that they fell victim to an act of cybercrime (for instance when the identity they use in an online shop is stolen) or that the technical devices they use were misused for the commission of cybercrimes (for instance by use of infected PCs or routers as part of a botnet for the commission of DDoS[1] attacks or infection with cryptomining malware).
- Victims fail to report offences, particularly when no financial loss has been incurred (such as the mere detection of a virus on the PC) or the loss is adjusted by a third party (insurance company or the like).
- Victims, particularly companies, abstain from reporting identified offences in order to ensure, for instance, that they do not lose their reputation as a "safe and reliable partner" among their clients.
- Cases of extortion, for instance, are frequently only reported if offenders fail to decrypt systems they encrypted before although a ransom has been paid.

In order to describe the area of cybercrime as close to reality as possible despite the aforementioned factors, information provided by different institutions outside the police and the authorities (such as research facilities and IT security service providers) was also included in the report for the year under review, as had been laid down in the police strategy aimed at the suppression of cybercrime. In addition, the co-operation partner of the Bundeskriminalamt (BKA), the "German Competence Centre against Cyber Crime e.V." association (G4C)[2] including its affiliated companies, was involved in the drafting of this situation report.
The quantitative analysis of the cybercrime situation produced on the basis of the PCS is preceded by the qualitative analysis produced on the aforementioned basis in the current situation report.

[1] Denial of Service (DoS) attacks target the availability of services, websites, individual systems or entire networks. If such an attack is launched simultaneously by several systems, it is called a distributed DoS or a DDoS attack (DDoS = Distributed Denial of Service). DDoS attacks are frequently mounted by a very high number of computers or servers forming a botnet.
[2] G4C members: Commerzbank, ING-DiBa, HypoVereinsbank, Kreditanstalt für Wiederaufbau (Development Loan Corporation), Schufa (leading credit reference agency), Bank-Verlag (bank consulting firm and publishing house), R+V (insurance company), Broadcom, Diebold Nixdorf, Link11, G-Data; G4C co-operation partners: BKA and Federal Office for Information Security (BSI).

2 Distinctive Cyberattacks in 2019

Jan.

- A subsidiary of the Deutsche Kreditbank (DKB) is hit by a DDoS attack; its online services are temporarily unavailable.

Feb.

- Customers of various banks become the victims of SIM swapping[3] and subsequent TAN interception.

March

- The ransomware *LockerGoga* attacks the international industrial concern NorskHydro.
GandCrab blackmails several companies in Germany.

April

- Different DAX companies are reportedly spied out by means of the malware *Winnti*.

May

- A wave of the *Emotet* malware hits, inter alia, various tax offices.

June

- The IT systems of the Eurofins international forensics service provider are encrypted by ransomware. Partners of Eurofins thereupon end the co-operation.

[3] SIM swapping: The offenders have a target's phone number transferred to a SIM card held by the attacker. In order to obtain a SIM card with the victim's phone number from the respective telecommunications provider, the offenders often collect the necessary data of the potential victim beforehand by using various methods. The SIM card with the victim's phone number then allows the offenders to assign new passwords for accounts the victims hold with various providers (e.g. on e-commerce platforms or banking apps).

July

- The *Sodinokibi* ransomware infects several facilities of the German Red Cross (Deutsches Rotes Kreuz).

August

- The *GermanWiper* ransomware spreads across Germany. Even after payment of the ransom, the encrypted data remain unusable.

September

- The systems of the Rheinmetall Automotive Group are infected with malware.

October

- The *Emotet* malware severely affects the work of the Berlin Higher Regional Court and ransomware encrypts the systems of Regensburg university.

November

- The Pilz GmbH is forced to temporarily suspend operations due to ransomware.

December

- At the end of the year, *Emotet* resurfaces in many places. The "Klinikum Fürth" hospital as well as the city of Frankfurt am Main and the city of Homburg are infected by the Trojan.
- In addition, the university of Gießen becomes the victim of a ransomware attack.

3 Cybercrime in Germany

The level of professionalism of cybercriminals continues to increase.

Cybercrime creates and is based on criminal value chains.

Ransomware remains the greatest threat to commercial enterprises.

The number and intensity of DDoS attacks are increasing rapidly.

The offenders are globally networked and operate internationally, on a division-of-tasks basis and in a highly organised way.

Cautious Internet users continue to be the most important protection mechanisms against cybercrime.

3.1 THEFT OF DIGITAL IDENTITIES / ID THEFT

Most cybercrime offences begin with the theft of a digital identity. Intercepted passwords of e-commerce accounts, e-mail or messenger services, the cloud or internal company resources can be used by cybercriminals in a fraudulent manner. The impacts of digital identity thefts are manifold and constitute the basis of the commercial value chains of cybercrime; they range from using fee-based streaming services to unlawfully concluding contracts and ordering goods to mobbing, stalking or making online transfers.

What is a digital identity?

The term "digital identity" refers to the sum of all possibilities and rights of the individual users as well as their personal data and activities within the overall structure of the Internet.
Specifically, this also includes all kinds of user accounts, i.e. access data in the following areas:

- *communication (e-mail and messenger services),*
- *e-commerce (online banking, online stock trading, all kinds of Internet-based sales portals),*
- *job-related information (e.g. for online access to a company's internal technical resources),*
- *e-government (e.g. electronic tax return) and*
- *cloud computing (use of storage space offered as a service, of software or computing performance).*

Cybercriminals use various methods to steal digital identities. The most common ones are:

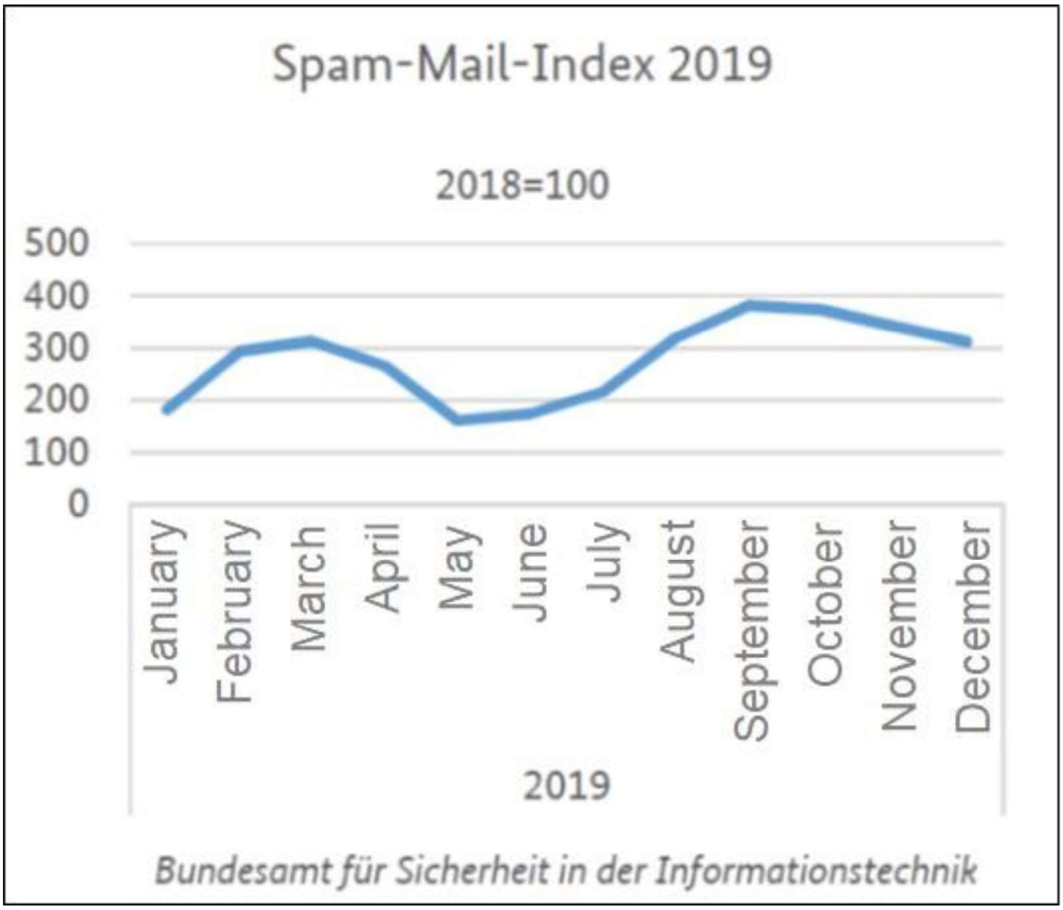
- phishing and spam mails,
- malware (e.g. keyloggers, which record keystrokes),
- analogue social engineering (e.g. via so-called tech support scam[4]),
- data leaks (the often unintentional outflow of data) or data breaches (active capture, interception or extraction of data by third parties).

[4] Criminals call targets and pretend to be an IT support team. Under the pretext that an error has occurred on the computer or that a false operating system licence has been used, the victim is asked to grant the criminals access to the computer via remote control or to disclose passwords.

Every stolen password, every leaked e-mail address, every obtained credit card number can be misused for criminal purposes or sold.

The spreading of spam mails is an attack vector most people have probably encountered already: Dubious e-mail senders send mails on very varied subjects apparently at random. The spam mail aims to prompt the user to download the attachment or follow a link. Both actions result in the IT systems being compromised: The e-mail attachment as well as the linked website may contain malicious code used to intercept data on the target system.

The Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik - BSI) keeps a so-called spam mail index, which measures to what extent the networks of the Federal Government are affected by the spam mails identified there. The index covers all unsolicited mails such as advertising, but also mal-spam.[5]



[5] Mal-spam is a spam mail carrying malware.

There is a clearly visible quantitative increase in the index in 2019 compared to the average of the previous year. At no time in 2019 is the spam mail index below the 2018 base value – the number of spam mails increased sharply in 2019, averaging 277.8, and is thus nearly 2.8 times as high as the 2018 annual average. In particular from August onwards, the index shows strong deviations from the average of the previous year.

Data breaches or unintentional data outflows caused by technical deficiencies can each involve millions of data records. Each data record lost can serve as a breeding ground for further criminal purposes and be sold. The criminal potential entailed by the loss of data records in the order of over 100 million affected customers is thus enormous: In early 2019, the National Cyber Defence Centre[6], for instance, reported a disclosed data dump involving approx. 773 million e-mail addresses and 21 million passwords in plain text. Even though most of the access data disclosed was probably no longer valid at that point in time, such disclosures pose a high risk of third parties illegitimately taking over digital identities.

A serious issue in this context: The individuals affected often do not know that their data were intercepted or lost. The reason for data losses is frequently the inadequately secured handling of data.

Case example: weleakinfo.com

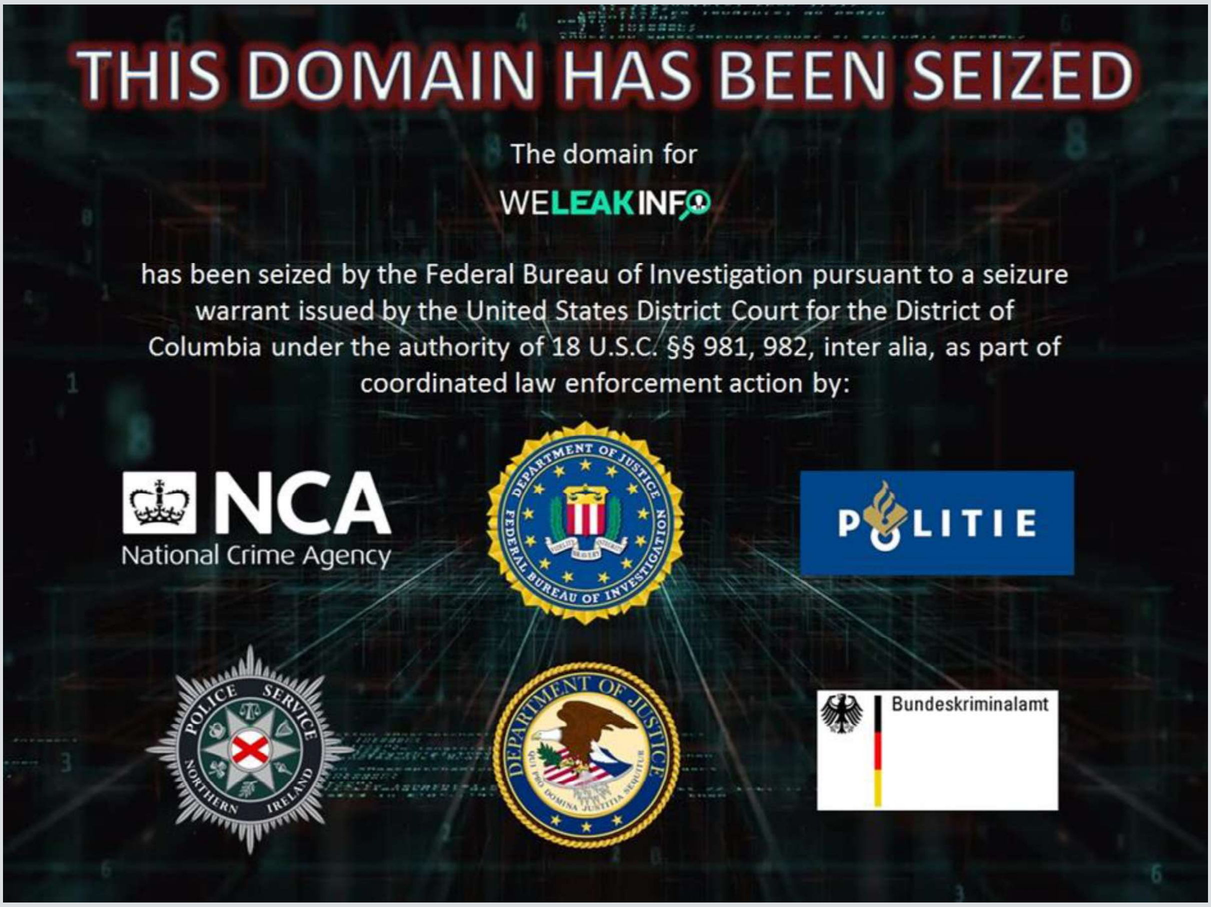
As of 04/01/2019, investigative proceedings were conducted at the BKA against a then 21-year-old German national, who published personal data and documents of politicians, journalists and public figures without authorisation via social media channels in the form of a so-called "Advent calendar". After having been provisionally arrested, the suspect stated that he had bought access data and passwords from the platform *weleakinfo.com* and used them for entering the accounts of his victims.

On 21/05/2019, Frankfurt/Main public prosecutor general's office (central office for combating Internet and computer crime - ZIT) initiated proceedings for suspected data espionage (section 202a of the German Penal Code) and handling stolen data (section 202d of the German Penal Code) against the operators of the platform *weleakinfo.com* and tasked the BKA with the investigations. Further investigative proceedings were conducted against the two administrators of the platform in the Netherlands, the United Kingdom and the USA.

The administrators of the a/m platform were arrested in the United Kingdom on 15/01/2020. In the course of further measures, several servers associated with the platform *weleakinfo.com* were seized in the Netherlands. The BKA conducted further measures to secure evidence from servers rented by the suspects in Germany. The domain *weleakinfo.com* was taken over by the FBI and given a seizure banner.

[6] The National Cyber Defence Centre is an inter-agency information, coordination and co-operation platform, where security-relevant cyber incidents are collected, analysed and assessed on a workday basis.

Case example: weleakinfo.com



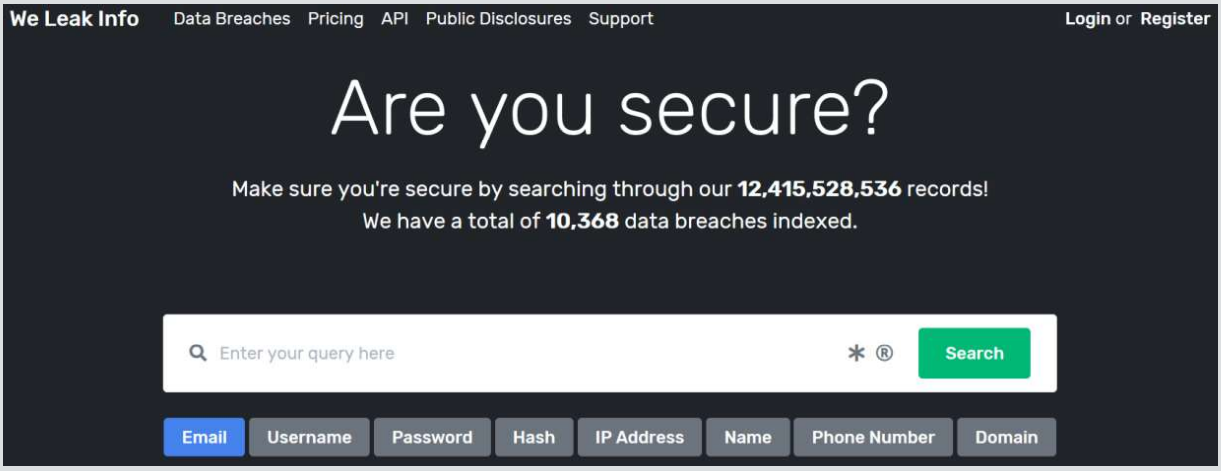
THIS DOMAIN HAS BEEN SEIZED

The domain for

WELEAKINFO

has been seized by the Federal Bureau of Investigation pursuant to a seizure warrant issued by the United States District Court for the District of Columbia under the authority of 18 U.S.C. §§ 981, 982, inter alia, as part of coordinated law enforcement action by:

In January 2020, *weleakinfo.com* offered for sale **12.4 billion data** records from over 10,000 past data leaks.

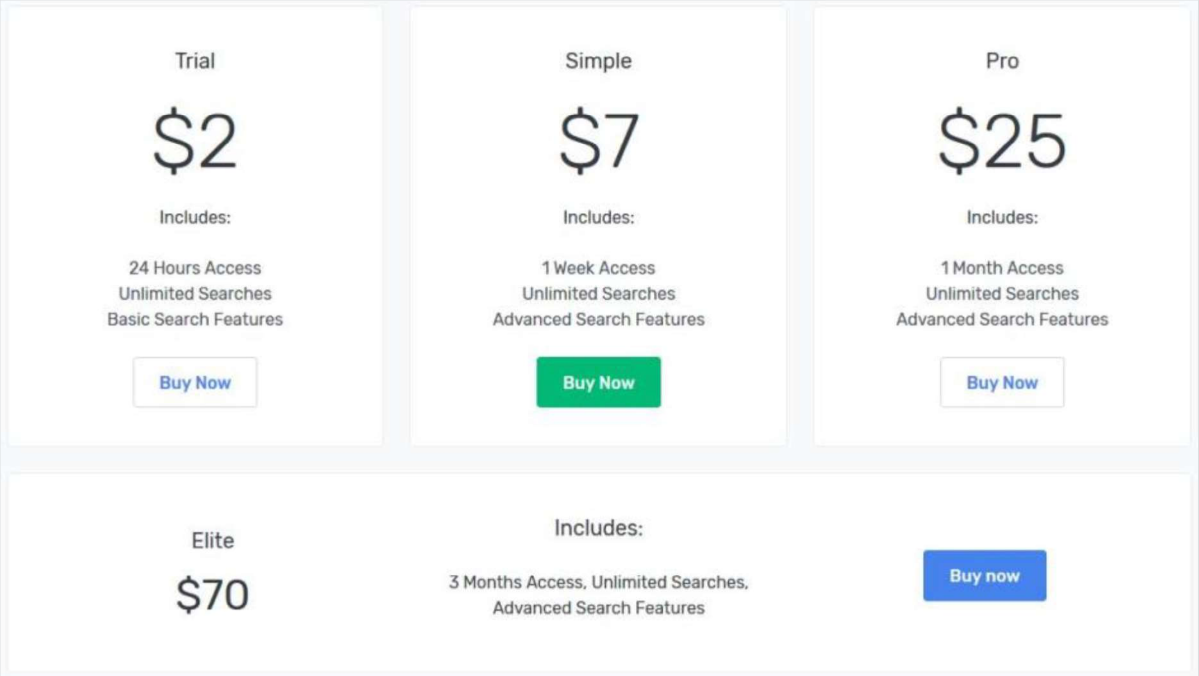


Are you secure?

Make sure you're secure by searching through our **12,415,528,536** records!
We have a total of **10,368** data breaches indexed.

The data came from data leaks spread on the Internet; they were compiled on *weleakinfo.com* by the platform operators and made available against payment to the registered buyers.

Case example: weleakinfo.com



Trial

$2

Includes:

24 Hours Access
Unlimited Searches
Basic Search Features

Buy Now

Simple

$7

Includes:

1 Week Access
Unlimited Searches
Advanced Search Features

Buy Now

Pro

$25

Includes:

1 Month Access
Unlimited Searches
Advanced Search Features

Buy Now

Elite

$70

Includes:

3 Months Access, Unlimited Searches,
Advanced Search Features

Buy now

In contrast to the standards of reputable sites such as the "Identity Leak Checker" of the Hasso Plattner Institute, the operators of the aforementioned platform failed to check whether the data requested were actually accessed by the rightful owner. It was thus possible for the paying customers, for instance, to query first and family names, usernames and e-mail addresses of third parties on *weleakinfo.com* to receive the associated passwords in case of a hit.

Brief assessment:
The investigations in the countries involved, which were conducted on a division-of-tasks basis and with different foci (GB/NL = person-related approach, Germany = infrastructure investigation, USA = securing of domains), resulted in an efficient and quick processing of the investigative complex. The close exchange of police information successfully ensured the international co-ordination of the different measures.

Each digital identity can serve criminals as a basis for committing numerous offences.

Every Internet user should be aware that his/her digital identity is similarly sensitive as, for example, his/her physical identity card, passport or credit card, and therefore needs to be protected. Even seemingly trivial measures, like using a safe password, contribute significantly to the security of one's data.

3.2 MALWARE

What is malware?

The term malware refers to all programmes which run malicious operations on an IT system. These malicious operations include, inter alia:

- *data espionage and forwarding of account data such as usernames and passwords,*
- *manipulation or destruction of data,*
- *illegitimate use of computing power for cryptomining,*
- *data encryption,*
- *integration into a botnet – also to launch DDoS attacks,*
- *fraudulent remote control of a third-party IT system.*

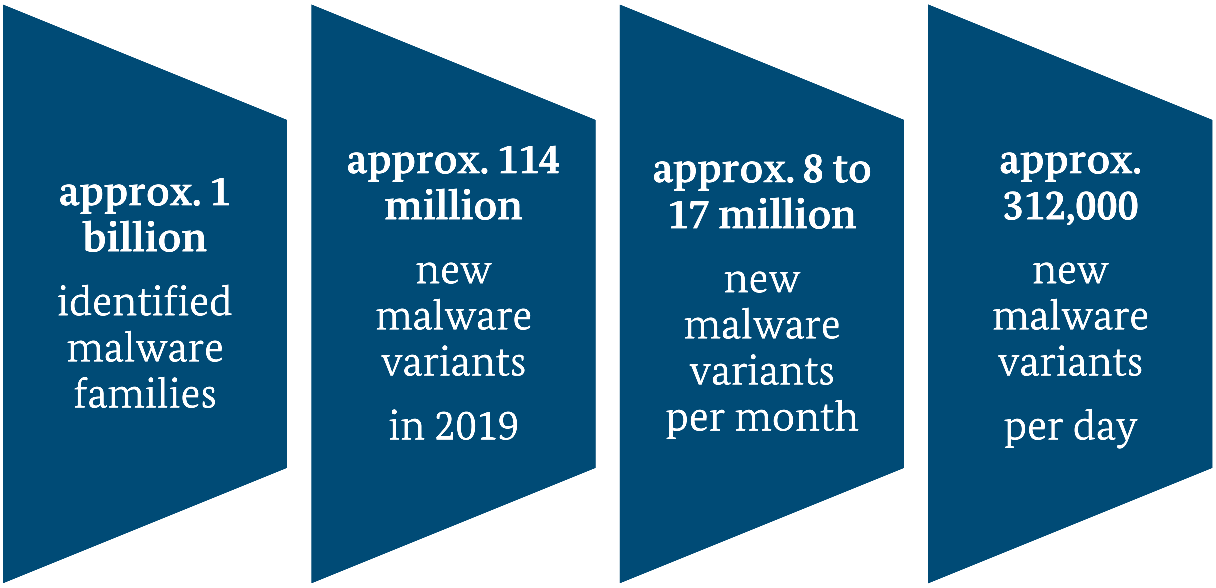
The majority of cybercrimes is committed by means of malware entering third-party systems where it can run a variety of malicious operations. Malware families can be spread in different ways.

The most commonly exploited entry vectors into a third-party IT system are infected attachments of spam mails. In these cases, the user is asked to download an attachment (often a Word or PDF document). After opening the attachment, the malware installs itself and spreads in the system. Just as often, spam mails contain links leading to malicious websites. Via such websites, malware is loaded onto the system of the parties concerned without them knowing (drive-by infection).

Over 1 billion malware families detected.

The number of malware families cannot be exactly determined. The reason for this lies in the hyperactive dynamics of cybercrime – dozens of new variants of already known malware families are identified every day.

The IT security service provider AV-Test estimates the extent of malware distribution in 2019 as follows[7]:



approx. 1 billion identified malware families

approx. 114 million new malware variants in 2019

approx. 8 to 17 million new malware variants per month

approx. 312,000 new malware variants per day

These numbers represent only a part of all malware variants identified. Owing to the significant quantity of unreported and unrecorded cybercrimes, the exact number is far higher. Cybercriminals constantly work on revising existing malware variants and equipping them with further malicious functions.

According to an analysis of G Data[8], the below-mentioned malware variants are among the ten most common malicious programmes worldwide and are also widespread in Germany:

- The *GandCrab* ransomware encrypting systems and demanding a ransom for decryption. In mid-2019, the group behind *GandCrab* announced they would cease their activities, but despite this, *GandCrab* is still in circulation and actively spread. It is assumed that the *Sodinokibi* ransomware, which was newly identified in 2019, is the successor of *GandCrab*.
- The loader *Emotet* – for information on the constant threat posed by *Emotet*, please see page 17.
- *AZORult* – an info stealer that intercepts different digital identities.
- *njRAT*, a remote access tool that records keystrokes (so-called keylogging) and gives third parties access to microphone and webcam.

[7] AV-Test – Malware, available at: https://www.av-test.org/en/statistics/malware/
[8] G DATA – Malware-Top-10 2019: Angriffe im Sekundentakt [attacks at second intervals], available at: https://www.gdata.de/news/2020/01/35714-malware-top-10-2019-angriffe-im-sekundentakt

High level of professionalisation in malware development.

The range of unlawful malware features is very high and one malware family often has several of these malicious functions.

A development that has become apparent in recent years is the growing professionalisation of malware programmers and of so-called malware crypting: Both the actual malicious code and its encryption / modification (crypting) constantly develop further and are becoming more complex. The cybercriminals' objective in this regard is to improve the malware's so-called obfuscation ability[9] in order to remain unnoticed by security systems as long as possible.

Before using their malware, developers also test whether it is detected by current antivirus (AV) software. Coding, crypting and testing with AV scanners are key elements of potentially successful cybercrime (see chapter 4.6). Even though this triad in malware development has already existed for many years, it continues to gain in importance.

The growing professionalisation is furthermore reflected in the modi operandi applied, particularly in the entry vectors chosen. Similar to state actors, cyber groups in the field of general crime increasingly operate in the context of so-called APT (Advanced Persistent Threat, see chapter 6): Before an attack on an IT system is actually launched, the target is spied out thoroughly. Company policy, monthly turnovers, personal details and websites are explored and the IT systems are analysed for possible weaknesses to determine the most suitable entry vector. Once the attackers have entered the target system, they take their time to covertly spy out the IT system and select specific data as a target.

In the phenomenon area of malware, it can increasingly be observed that malware specifically exploits operating system-specific vulnerabilities. Compromising the Remote Desktop Protocol[10] of Windows systems also forms a focal point. In addition to the compromising of accounts by misusing stolen digital identities, the use of exploits[11] and CVE[12] serves as a starting point for the installation of RATs[13] – if the cybercriminal then has access to the IT system, he/she can load further malware.

[9] Concealment against security mechanisms such as antivirus scanners.

[10] Remote Desktop Protocols are Microsoft network protocols for remote access to Windows computers.

[11] Exploits are programmes exploiting security flaws.

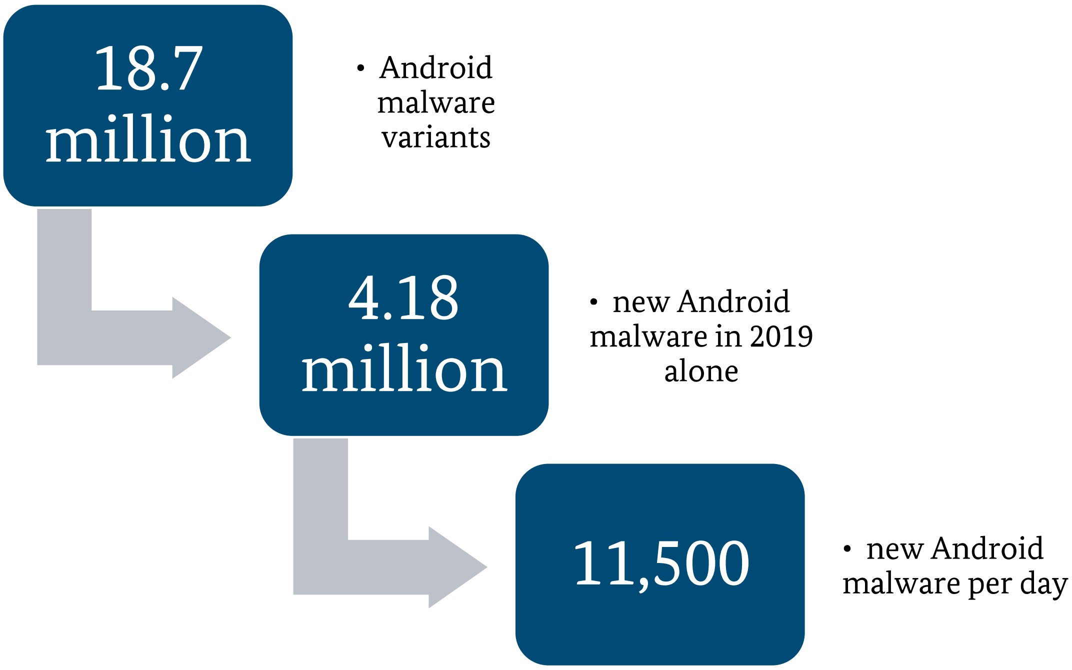
[12] Common Vulnerabilities and Exposures: Security flaws and vulnerabilities in IT systems and software.

[13] Remote Access Trojan – malware that provides administrative control over the computer attacked via a technical "back door".

Mobile malware

The G4C cooperation partner G DATA analysed[14] the distribution of mobile malware, i.e. malware specifically used against mobile terminal devices, for the period under review. In particular the Android operating system is a primary target of attacks in this context.

11,500 new mobile malware variants per day.



18.7 million
- Android malware variants

4.18 million
- new Android malware in 2019 alone

11,500
- new Android malware per day

Mobile malware can have different forms, ranging from info stealers, which phish passwords and account data, to ransomware, which encrypts the device. Two forms of mobile malware are particularly common: adware and spyware.

Adware is designed to flood the screen with unsolicited advertising. Although Internet users often consider this to be merely annoying, calling up advertisements which pop up can have serious consequences – the advertisement that has been clicked on may lead to a malicious website, where further and more aggressive malware may be transmitted.

Spyware spies out the infected system and forwards these data (such as up-to-date location data) to third parties. Similar to adware, spyware often disguises itself as legitimate software, e.g. in the form of an app. It is therefore recommended to download apps from official stores.

[14] G DATA – G DATA Mobile Malware Report 2019, available at: https://www.gdata.de/news/2020/05/36125-g-data-mobile-malware-report-2019-neuer-hoechststand-bei-schaedlichen-android-apps [new peak with regard to malicious Android apps]

The security vettings in official app stores (such as Google Play Store) have been further tightened in recent years[15].

Case example: *Emotet*

In 2019, the *Emotet* malware interfered with numerous authorities, businesses and companies in Germany, including the "Bundesanstalt für Immobilienaufgaben" (Institute for Federal Real Estate), a branch of the industrial concern Norsk Hydro, the Berlin Higher Regional Court and various local municipalities.

On 12/12/2019, for instance, the "Zentrale Ansprechstelle Cybercrime" (ZAC) [central point of contact for cybercrime] of the Bavarian Land Criminal Police Office received a call from the "Klinikum Fürth" hospital informing them that the hospital's IT systems had been compromised. A first analysis revealed that at least 53 clients had been infected with different malware such as *Emotet* and *Trickbot*. An e-mail carrying a malicious attachment was the entry vector. This e-mail was received at the hospital on 04/12/2019 and opened along with the attachment (document in .doc format) and macros contained therein. Analyses revealed that the macros embedded in the attachment referred to different URLs (website addresses). Via one of these URLs, indications of a downloaded malicious file related to *Emotet* were found.

The intervention of "Klinikum Fürth's" IT experts prevented extensive damage. The crisis committee established asked for urgent assistance by the police.

In the course of further analyses, further malicious code was identified on file share servers. They also revealed computers with outdated virus protection, which had not been in the focus so far.

The hospital’s operation itself was not affected by the cyberattack.

Digression / background:
Emotet is currently considered one of the most malicious programmes worldwide and has also infected the IT systems of numerous companies / institutions in Germany. *Emotet* is a loader / dropper whose primary function is to download further malware (such as ransomware). Depending on the location, further malware is downloaded; in Germany, particularly the malware variants *Trickbot* and *Ryuk*. The business model can be referred to as infection as a service.

The typical course of an infection by the *Emotet-TrickBot-Ryuk* malware combination starts with a malicious Word document spread via spam mails. By opening the document and allowing macros, a malicious code embedded in the document is executed and the actual *Emotet* Trojan is loaded onto the target system. From this point on, cybercriminals can spy out information on the target system, send this information to the offenders' command and control (C2) servers and carry out keylogging.

[15] See e.g. heise.de – Mehr Warnungen sollen Android-Nutzer schützen [More warnings are to protect Android users], available at: https://www.heise.de/security/meldung/Google-Play-Protect-Mehr-Warnungen-sollen-Android-Nutzer-schuetzen-4322166.html

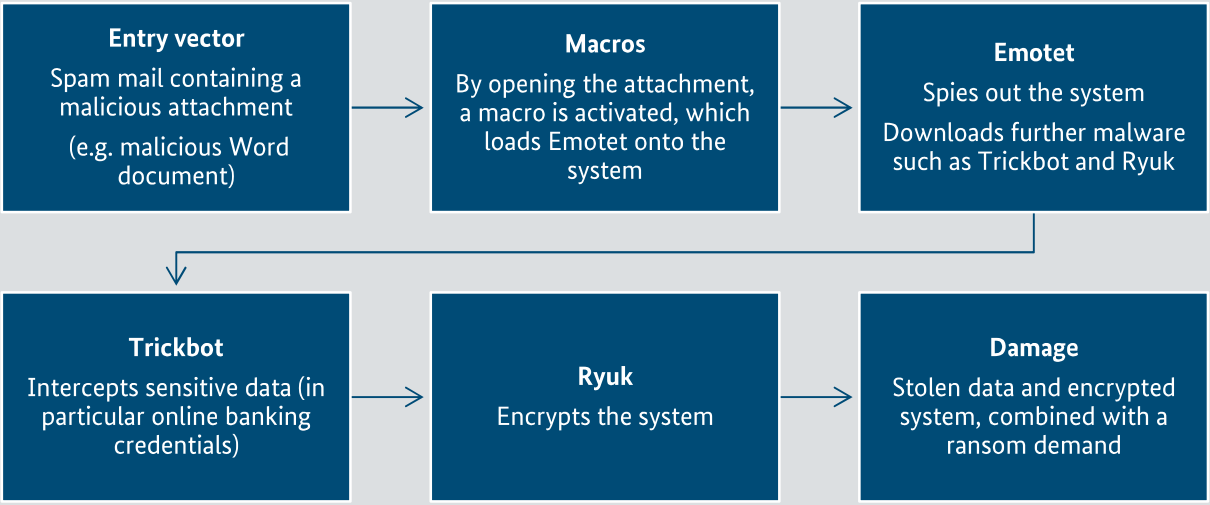
Case example: *Emotet*

Moreover, it was found that *Emotet* can download further modules, among them those used for:

- manipulating online banking,
- spying out passwords stored in web browsers and e-mail programmes,
- committing DDoS attacks and
- extracting information from e-mail address books (names and e-mail addresses).

After initial infection with *Emotet*, the Trojan *TrickBot* is often downloaded. *TrickBot* is a banking Trojan[16], which is mainly active in the USA and the UK. It intercepts further sensitive data in the target system and transfers them to a C2 server.

At the end of the infection chain, the ransomware *Ryuk* is downloaded, which encrypts the target system and demands a ransom for decryption.


Entry vector
Spam mail containing a malicious attachment
(e.g. malicious Word document)

Macros
By opening the attachment, a macro is activated, which loads Emotet onto the system

Emotet
Spies out the system
Downloads further malware such as Trickbot and Ryuk

Trickbot
Intercepts sensitive data (in particular online banking credentials)

Ryuk
Encrypts the system

Damage
Stolen data and encrypted system, combined with a ransom demand

Brief assessment:
Emotet poses a considerable threat. The malware is used to carry out targeted attacks on critical infrastructures, authorities and large companies. *Emotet's* primary ability is to download further malware. If an institution attacked does not react quickly and professionally enough, the entire IT network can be encrypted by further downloaded ransomware.

[16] Banking Trojans are malware that preferably steal (access)data for / in connection with the use of e-commerce and online banking.

Attacks on ATMs

Logical/digital attacks on automated teller machines (ATMs) are increasingly gaining importance although the number of cases is still comparatively low. This field of crime is primarily characterised by three modi operandi:

a) Jackpotting by means of malware (attacks on the PC of an ATM by means of malware)

b) Jackpotting by means of a black box carried along (a variant of the jackpotting attack on the payment module of the ATM by means of the perpetrators' hardware)

c) Network attack (malware attack on the card-issuing bank or the processing company to manipulate transaction processes; subsequently, a card-bound "cashout" or malware attack on the bank operating the ATM is carried out to gain direct access to the networked ATMs and to carry out a non-card-bound "cashout").

Following a significant rise in 2018, case numbers remained comparatively constant in 2019:

Year	Jackpotting by means of malware	Jackpotting by means of a black box	Network attacks
2017	11	3	3
2018	20	43	3
2019	21	47	1

The majority of jackpotting attacks carried out by means of a black box in Germany in 2019 were aimed at a specific type of ATM that was particularly vulnerable to such attacks. The perpetrators identified were mainly Russian and Ukrainian nationals.

19 of the 21 recorded jackpotting attacks by means of malware were committed in Berlin. These attacks can be attributed to a Romanian group of offenders.

The losses caused in 2018 and 2019 varied greatly, which is, inter alia, probably due to the fact that different security measures were in place for the ATMs.

Year	Jackpotting by means of malware	Jackpotting by means of a black box	Network attacks
2018	540,000 €	450,000 €	37,000 €
2019	125,000 €	940,000 €	10,000 €

Malware for ATMs is sold via the darknet to enable even technically less experienced perpetrators to manipulate ATMs and carry out a "cashout".

Since the perpetrators can expect potentially high profits, a continuing high threat posed by logical/digital attacks on ATMs has to be assumed.

Case example: Attacks on ATMs

Since November 2019, Osnabrück detective force had been conducting an investigation, on behalf of the local public prosecutor's office, into two Ukrainian nationals for suspected computer fraud on a repetitive and gainful basis.

The investigations led to the solving of a total of eleven cases of jackpotting committed by means of a black box in four Länder between 24/10/2019 and 10/11/2019. All in all, the suspects obtained EUR 214,970 in cash in this way, one third of which was seized. The investigations led to a perpetrator structure where so-called "runners" are responsible for carrying out the technical aspects of the offence at the ATM. These runners maintained contact to a perpetrator who acted as the "superior" of the runners and as a contact to the persons behind the scenes presumably staying abroad.

Remarkably, the suspects probably converted the cash amounts of EUR 29,640 and EUR 26,850 obtained from the offences into bitcoins at appropriate ATMs in two cases.

In July 2020, the two suspects were sentenced to four years' and three months' imprisonment for computer fraud on a repetitive and gainful basis.

Brief assessment:
The technical modus operandi is to be attributed to the field of cybercrime in the narrower sense[17] – which is also in line with the court assessment. The components of the offence – recruitment of runners, remote control of the black box from abroad and financial flows with bitcoin to Russian darknet marketplaces – suggest that there are internationally organised criminal structures.

[17] Cybercrime in the narrower sense refers to all offences that are targeted against the Internet[17], further data networks[17], IT systems[17] or their data. A list of the offences is given in chapter 8.4.

3.3 RANSOMWARE – DIGITAL EXTORTION

As in 2018, the trend towards targeted, highly professional ransomware attacks on companies continued. The intensity of such attacks continued to increase in 2019 – in particular, the effects resulting therefrom.

What is ransomware?

Ransomware encrypts the data of a digital system and, in many cases, even blocks other terminal devices accessible through a network (such as an enterprise network).

There are different types of ransomware:

a) Ransomware that actually does not encrypt the hard disk but only blocks user access to the system by manipulation. The most commonly known type is malware that misuses well-known names and logos of security agencies[18] in order to make the illicit demand for payment look "official".

b) Crypto-ransomware, which encrypts the data on the compromised terminal systems and, in recent cases, even on systems connected through networks (servers, file storages, etc.). This type has a very high destructive potential since, in a number of cases, it is not possible to decrypt and thus restore the data. Furthermore, in many cases paying the ransom demanded does not mean that the compromised system is decrypted afterwards.

c) A so-called "wiper" differs from "conventional" ransomware in one crucial aspect: There is no functionality to decrypt and restore data on a system – thus, the data are rendered unusable and are destroyed irreversibly. Even after the ransom was paid, the data cannot be restored.

From a criminal law perspective, the use of ransomware constitutes a combination of the criminal offences of computer sabotage and extortion, punishable under sections 303 b and 253, respectively, of the German Penal Code.

Ransomware attacks on companies have the potential to trigger existential threats. Although cybercriminals clearly focussed on companies and governmental institutions in 2019, private individuals can also become victims of ransomware. Here, a successful attack often results in the loss of many and very private data.

[18] Famous examples of such phishing mails are the "BKA Trojan" and the "GVU Trojan" (GVU = Gesellschaft zur Verfolgung von Urheberrechtsverletzungen e. V. [registered association for the prosecution of copyright infringements]).

Ransomware is and remains THE threat for companies and public institutions.

One of the first stages of a typical ransomware attack is the sending of a phishing mail. This mail contains a malicious document, which loads the malicious programme after being opened.[19] The general advice not to open e-mails from unknown persons frequently confronts companies with practical difficulties. In 2019, for example, alleged unsolicited applications were, in many cases, the starting point of ransomware attacks. Moreover, it was established that cybercriminals analyse e-mail correspondence obtained through previous cyberattacks in order to pretend that mails are sent from known sender addresses. In this way, e-mails received from allegedly known senders are filled with topics and conversational contents that appear realistic to the potential victim in order to make the victim open the malicious document or click on the link controlled by the perpetrator.

Increased destructive potential brought about by double extortion.

Since 2019, a further, very critical variation was added to this typical modus operandi – the so-called double extortion. Here, ransomware actors do not only encrypt the IT systems of their targets but extract sensitive data prior to the encryption and threaten to publish these data. In a modular procedure,

- personal contact and access data are spied out first,
- then, bank details, money transfers and other sensitive information are extracted and finally
- company secrets are extracted for the purpose of extortion (decryption against payment of the ransom and threat to sell or publish the data).

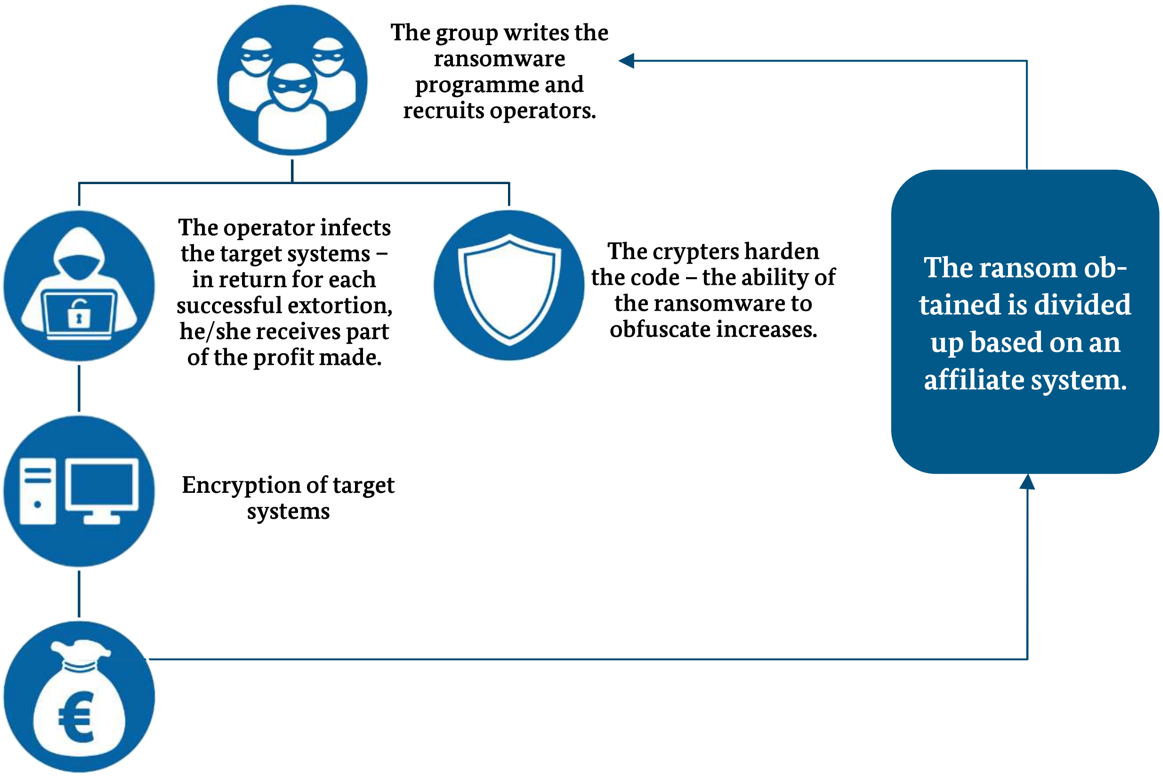
Thus, the victims are put under increased pressure to pay the ransom. In such cases, it is not only the availability of the encrypted data that is threatened but also their confidentiality and consequently the victim's reputation.

In 2019, the developers of the ransomware Maze began to implement this new modus operandi. They published the data of victims, who did not pay the ransom, on a "public shaming" website. Further actors, such as the groups behind the ransomware families Nemty and Sodinokibi, followed the example of Maze.

Since the business model is considered lucrative, it has to be assumed that further perpetrators will copy this modus operandi.

[19] Microsoft Office documents are used particularly often.

Ransomware actors – just like the rest of the cybercrime scene – operate in an organised way and based on a division of tasks so that the ransomware-as-a-service model has established itself within the underground economy (see chapter 4): One group of criminals writes a ransomware programme and recruits other so-called operators who load the programme on the target systems. Thanks to an affiliate system, all persons involved make a profit: In return for each successful extortion, the operators receive part of the extorted ransom – the remaining amount goes to the ransomware coders. One element of such procedures, which has meanwhile become standard, is the so-called malware crypting. Here, the code of the ransomware is optimised in order to hide it from the security mechanisms of the target systems.


The group writes the ransomware programme and recruits operators.
The operator infects the target systems – in return for each successful extortion, he/she receives part of the profit made.
The crypters harden the code – the ability of the ransomware to obfuscate increases.
Encryption of target systems
€
The ransom obtained is divided up based on an affiliate system.

Summary:
Among all phenomena described here, ransomware has, on the whole, the highest destructive potential for companies, public institutions, authorities and critical infrastructures. For any kind of company, an infection with ransomware and a related encryption of the system can result in massive and cost-intensive interruptions of business activities and functions.

In particular, victims who do not regularly make backups also have to expect long-term detrimental effects for their companies in case of an infection with ransomware. Regular backups alone, however, do not guarantee that the business activities can be resumed soon. Progressive ransomware variants are also able to access and encrypt backups. It is therefore recommendable to have offline backups that cannot be accessed at any time via the network or file shares and cannot be encrypted or overwritten.

In order to resume the infected company processes as soon as possible, many victims tend to pay the ransom. The BKA advises against doing so: This further strengthens the criminal business model "ransomware" and encourages further perpetrator groups to imitate such offences. Furthermore, it is not certain at all that encrypted data will actually be restored after the ransom is paid.

Victims should always contact the criminal investigation department in charge. Moreover, victims can help themselves by searching for open source decryption tools, for instance through "NoMoreRansom"[20], a project initiated by Europol and the Dutch police in co-operation with the private sector. The BKA supports this project and has been an official "Supporting Partner" of "NoMoreRansom" since 2017.

Case example: Hospitals "DRK-Kliniken" infected with Sodinokibi

On 13 July 2019, a ransomware attack was committed on the IT infrastructure of the "DRK Trägergesellschaft Süd-West" (German Red Cross Association South-West) seated in Mainz. The IT systems in twelve institutions of the society in Rhineland-Palatinate were encrypted on a large scale during the attack. As a result, the working procedures were significantly restricted.

The forensic analysis carried out as part of the investigations of Rhineland-Palatinate Land Criminal Police Office revealed that the ransomware Sodinokibi had been used. Sodinokibi (also known as Sodin and REvil) is ransomware that was first identified in May 2019 and has been used for criminal purposes throughout the world since then.

The ransomware was brought into the system via an externally accessible terminal server in order to obtain central user rights and to start the encryption of the internal system. Once Sodinokibi has entered the attacked system, it deactivates Windows' built-in automatic repair functions. Then, the user of the system concerned will see an extortion letter on the desktop – depending on the operating programme and the interface. Both the technical infrastructure of the ransomware and the effort made by the developers are highly professional.

In the TOR network, the criminals behind Sodinokibi operate their own website to document the extortion letters and the current amount of the demanded ransom in bitcoins. Moreover, a time slot is displayed indicating the time when this amount will be doubled.

Since 2020, Sodinokibi belongs to those ransomware families which extract data prior to the encryption of the system and threaten to publish the data.

Brief assessment:
Although patient care was always guaranteed, this case again shows that critical infrastructures in Germany are considerably jeopardised through cyberattacks: One single attack on a central server structure can be sufficient to trigger a chain reaction and to make several connected institutions incapable of acting.

[20] https://www.nomoreransom.org/

According to information provided by the company Coveware[21], a partner of the "NoMoreRansom" project, Sodinokibi is the most commonly used ransomware throughout the world – followed by Maze, Phobos and Ryuk.

Various sources suggest that Sodinokibi is the "unofficial" successor of GandCrab.

Since the further development of GandCrab was stopped, Sodinokibi has clearly been gaining in market significance; it is likely that further attacks using this ransomware will be committed.

[21] https://www.coveware.com/blog/q2-2020-ransomware-marketplace-report

3.4 DDOS ATTACKS

Cybercriminals use this method to overload websites, servers and networks of individuals or organisations, thus significantly restricting their functionality and/or causing a non-availability of services. The attack programmes are coordinated by a large number of computers and run simultaneously so that the target systems are overloaded by numerous IT processes.

Distributed Denial of Service (DDoS) attacks

By deliberately causing overload, cybercriminals attempt to disrupt the availability of an Internet service or a target system.

DDoS attacks are characterised by the fact that such attacks are usually caused by numerous individual queries and/or a large number of computers – often by means of large, remotely controlled botnets.

How are botnets created?

Botnets are created by installing malware on victim PCs, usually without their owners noticing.

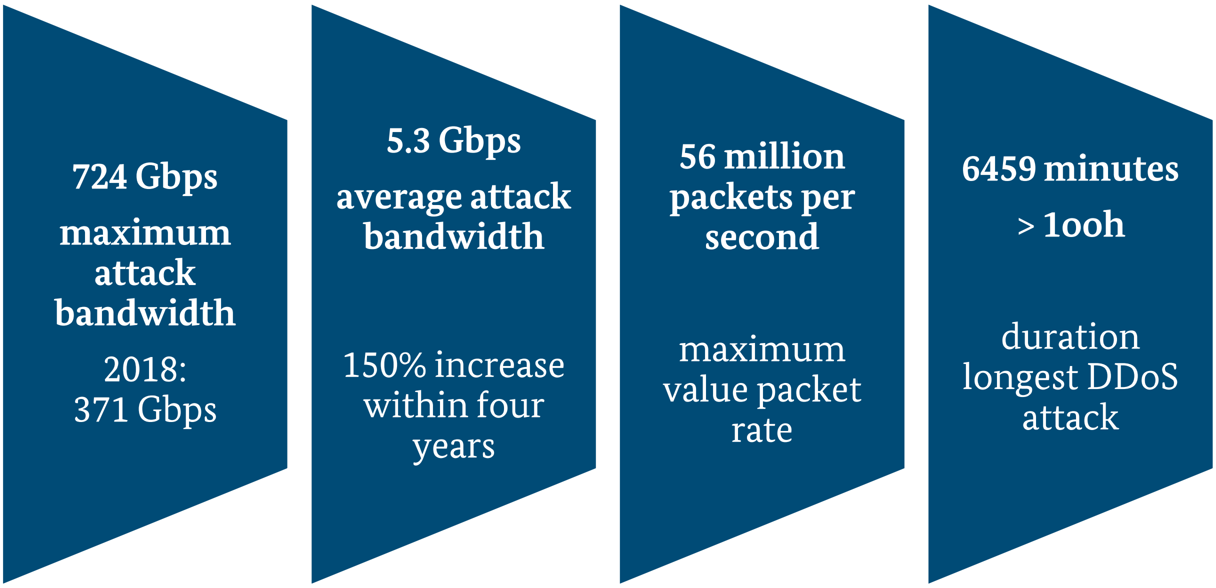
Once the malware has been installed, the perpetrator has almost full access to the compromised system. The numerous devices of the victims that were infected by malicious code are commanded and controlled through "command & control servers" without their owners knowing.
The "infected" PC is thus basically used as a resource for attacks – quite often for DDoS attacks.

The perpetrators often use botnets for the coordinate attack. They consist of a large number of previously infected computers, which are often located all over the world. A command and control server, which remotely controls these bot computers, determines the time and target of mass queries. Since basically all Internet-compatible devices could be integrated into such a botnet, the Internet of Things (IoT) with all its networked devices such as TV sets, cameras, routers, etc. plays an important and growing role in the field of cybercrime.

As regards situation reports on DDoS attacks, the BKA works closely with the G4C member Link11. The following explanations relate to information provided by this IT security service provider, which regularly analyses attacks registered in its network, as well as to additional information.

In the last few years, both the number and intensity (duration, bandwidth) of DDoS attacks have risen constantly.

According to the 2019 DDoS report of Link11[22], the analysis of the attacks that were registered in its network revealed the following threat situation for the year under review:



724 Gbps

maximum attack bandwidth

2018: 371 Gbps

5.3 Gbps

average attack bandwidth

150% increase within four years

56 million packets per second

maximum value packet rate

6459 minutes

> 1ooh

duration longest DDoS attack

Only one sixth of the companies within the EU use fast Internet connections of more than 100 Mbps[23]. The majority has a significantly slower Internet connection. Attacks of several 100 Gbps[24] are thus nearly always oversized for the particular target. Since the perpetrators attempt to achieve maximum impact with minimum use of resources, they adjust their attacks and can act with a significantly lower, target-adapted bandwidth of between 1 and 10 Gbps – this also explains the large discrepancy between the maximum and average attack bandwidth.

Attack vectors describe the path and means by which cybercriminals gain access to computers and servers in a network. If attackers misuse several protocols in an attack, it is called a complex or multi-vector attack. In the Link11 network, the portion of complex attacks, in which several attack vectors were used, was 67% in 2019. The changing vectors within an attack pose challenges for security service providers. Even though DDoS attacks always intend to overload the target system, a distinction has to be made between specific types of attacks:

Volumetric attacks
The perpetrators attempt to occupy the full bandwidth between the target and the Internet and to thus overload it. Massive data traffic and/or large amounts of data are used to impair the target system.

Protocol attacks
The perpetrators use vulnerabilities in different layers of the Internet protocol in order to make the target inaccessible and to thus disrupt the service offered by the attack target.

[22] https://www.link11.com/en/downloads/ddos-report-for-the-full-year-2019/
[23] Mbps: "Megabits per second"; unit of measurement for data transfer speeds.
[24] Gbps: "Gigabits per second".

Attacks on the application layer (application attacks)
Targeted attacks on the application layer[25] of a website and a resulting disruption of its services require only a low bandwidth and a limited number of "packets". Since malicious data traffic cannot be easily differentiated from legitimate data traffic, this type of attack is a problem for IT security service providers and poses a growing challenge.
Such so-called layer 7 attacks are becoming increasingly important.

IoT devices and cloud servers are used as amplifiers for DDoS attacks.

Numerous network protocols that are the basis for electronic data transfer can be misused by DDoS attackers as amplifiers for their attacks – so-called amplification vectors. At the end of 2019, Link11 observed more cases of the so-called "carpet bombings" strategy. It is defined as a flood of individual attacks that are directed not only against an individual Internet protocol of the target but simultaneously against the entire network. The manipulated data traffic thus spreads over a large number of attacks and Internet protocols within this network. The data volume of each attack, however, is so small that it is difficult to identify as manipulated data traffic and impossible to filter. The impact of such an attack, however, is similar to that of high-volume attacks.

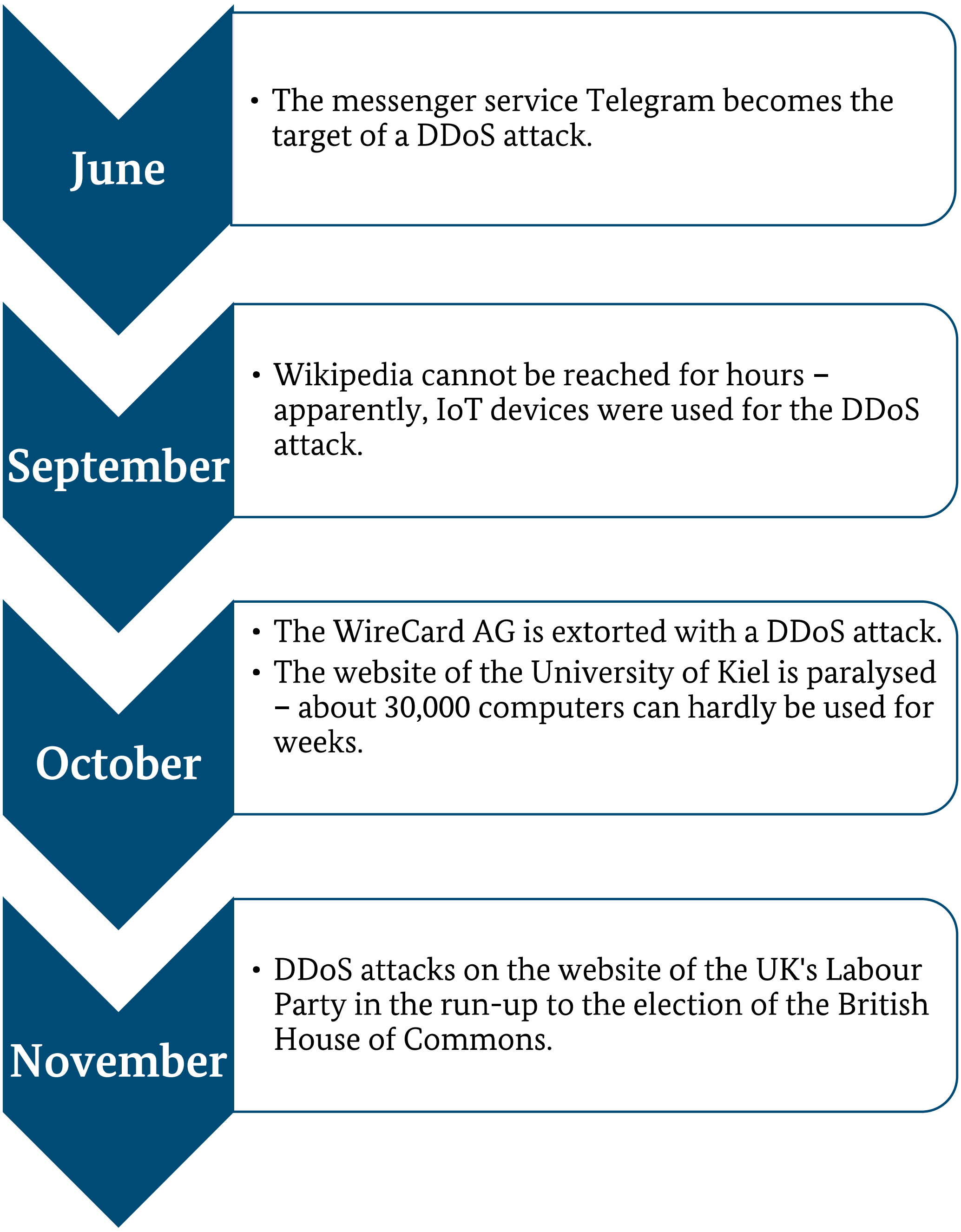
Cloud computing does not only offer numerous advantages for companies but also additional opportunities for cybercriminals. In the Link11 network, the portion of DDoS attacks that involved cloud servers was 45% in the reporting year 2019 – a trend that is on the rise.
Increasingly, DDoS attacks are coupled with extortion demands from perpetrators. Similar to ransomware attacks, payments in the form of bitcoins are demanded to cease the high-volume DDoS attacks.

DDoS attacks specifically cause damage to the individuals and organisations/companies attacked. The motives are manifold and range from damage to business competitors to mere political motivation. On the whole, monetary interests in the form of DDoS extortion play an increasing role.

Non-availability of websites results not only in failures of business processes and a drastic decrease in sales leading to significant financial losses, but also in damage to reputation and a loss of trust of business partners, customers and even voters. That is why DDoS attacks often cause businesses existential financial distress.

[25] The application layer is used, for example, for data entry and output and for generating websites on servers. Moreover, responses for visitors to these websites are provided there.

The following overview lists, by way of example, some of the DDoS attacks identified in 2019:



June

- The messenger service Telegram becomes the target of a DDoS attack.

September

- Wikipedia cannot be reached for hours – apparently, IoT devices were used for the DDoS attack.

October

- The WireCard AG is extorted with a DDoS attack.
- The website of the University of Kiel is paralysed – about 30,000 computers can hardly be used for weeks.

November

- DDoS attacks on the website of the UK's Labour Party in the run-up to the election of the British House of Commons.

4 Underground Economy

Illegal forums or marketplaces on the clearnet, deep web and darknet play an increasingly important role in cybercrime.

Definitions

***Clearnet** (also visible web, surface web, open web): It can be accessed by anybody with customary browser programmes, supported by simple handling with search engines. The clearnet, too, provides much illegal content, such as content related to politically motivated crime or platforms and forums of the so-called "underground economy" (criminal offences mostly committed in the area of cybercrime in the narrower sense).*

***Deep web** (also invisible web): Part of the Internet the contents of which cannot be found by search engines, for example, because websites were not indexed or linked to search engines or because they are access restricted. Deep web contents may be databases, Intranets or specialised websites and can be accessed by browsers, if and insofar as the URL is known and the user is authorised to access the site.*

***Darknet:** Darknet contents can only be viewed when using special anonymisation software. The darknet consists of forums, blogs/wikis, etc. with highly diverse – legal and illegal – contents. A significant part consists of so-called darknet marketplaces, where mostly incriminated merchandise is traded anonymously. There are also various demand-oriented Crime-as-a-Service offerings (offers to commit or support crimes on a contractual basis) or darknet sites containing child pornography. The structure and type of use of many darknet segments do not differ from the clearnet: In darknet forums, too, opinions are expressed and topics are discussed, and wikis provide explanations. On the darknet, however, these often refer to illegal activities and contents (e.g. narcotic drugs).*

Digital black markets on the darknet concern almost all fields of classical crime phenomena. In this context, it was established that the following goods and/or services are produced, procured and traded or exchanged:

- narcotic drugs and pharmaceuticals that are only available on prescription
- chemicals requiring a permit
- weapons, war weapons and explosives
- child and juvenile pornographic material
- counterfeit money, false instruments and other documents
- stolen property and counterfeit branded products
- handling access or credit card details that were spied out and stolen
- malware and vulnerabilities
- instructions for the commission of crimes
- information and services related to money laundering
- hosting and infrastructure services for criminal activities.

Now as before, the trafficking in narcotic drugs makes up the largest share of the illegal market on the darknet. The marketplaces are guided by the general market economy principles of supply and demand. On the other hand, various website operators draw up guidelines for self-regulation. In particular, child and juvenile pornographic material, firearms and fentanyl have disappeared from most marketplaces in response to intensive, internationally coordinated police law enforcement measures taken in the past years.

Tor network

The Tor network (The Onion Router), which is often used synonymously with the darknet in everyday language, is a parallel network, which is hosted on the Internet and consists of several thousand nodes. The network can be accessed through a specifically configured Tor browser; the data traffic is routed through several instances and thereby concealed. Web offers in the Tor network are therefore called hidden services.

Observations of the incriminated part of the darknet indicate that it is a loose network based on forum communication and significantly driven by the community idea. The essential elements of the incriminated darknet scene are described below.

4.1 MARKETPLACES

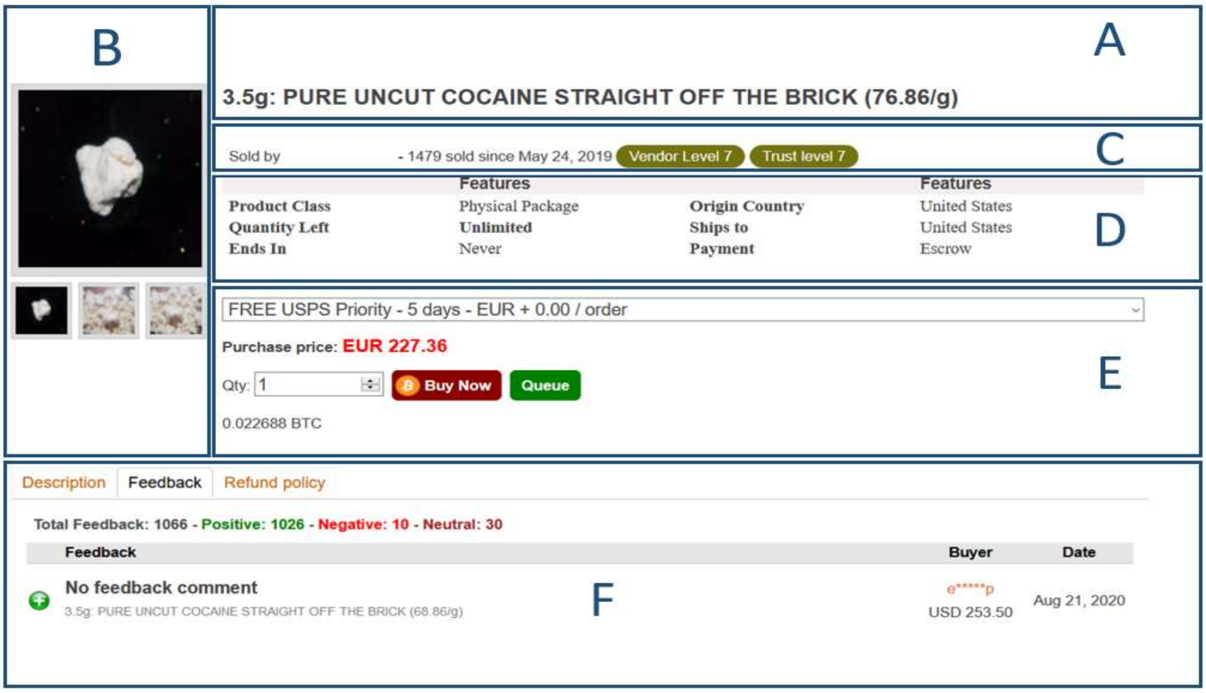
Marketplaces continue to make up a significant percentage of criminally relevant contents and of the criminal financial volume on the darknet. These websites, which are modelled on known e-commerce platforms, offer sellers the opportunity to trade conveniently and anonymously. Marketplaces are used to trade incriminated goods illegally, highly professionally and across national borders. The operators of these illegal platforms make profits by obtaining selling fees.

Bitcoin remains the most popular means of payment.

Due to their decentralised and partially anonymous characteristics, the money transfer is mainly made in crypto values. The cryptocurrency bitcoin is still by far the most frequently used payment method. To reduce the number of cases where goods were obtained by fraud or not supplied as agreed, the funds are held in trust by the platform operators for a certain period of time. This fact, in turn, offers website operators the opportunity to misappropriate the funds. This ploy, which is known as "exit scam", has been observed many times in the past years.

The communication on market-related topics is made either via forums operated by the marketplace administration or via separate forums. Some platforms also offer ticket-based support for their buyers and dealers.

Case example: Cocaine offered on a darknet marketplace



3.5g: PURE UNCUT COCAINE STRAIGHT OFF THE BRICK (76.86/g)

Sold by - 1479 sold since May 24, 2019 Vendor Level 7 Trust level 7

	Features		Features
Product Class	Physical Package	Origin Country	United States
Quantity Left	Unlimited	Ships to	United States
Ends In	Never	Payment	Escrow

FREE USPS Priority - 5 days - EUR + 0.00 / order

Purchase price: EUR 227.36

Qty: 1

0.022688 BTC

Description | Feedback | Refund policy

Total Feedback: 1066 - Positive: 1026 - Negative: 10 - Neutral: 30

Feedback	Buyer	Date
No feedback comment 3.5g: PURE UNCUT COCAINE STRAIGHT OFF THE BRICK (68.86/g)	e*****p USD 253.50	Aug 21, 2020

(A) Brief description or title.

(B) Photographs of the goods. The photographs sometimes contain aspects of so-called "proof pics" such as dealer names or the date.

(C) Information on the seller. In addition to the username, information on the number of sales as well as on the vendor level and trust level are displayed.

(D) Meta-information on the product. For example, available quantity, information on the time limit of the offer, product categories. In particular, details on the country of origin of the shipment are important to avoid customs checks. The payment in this case is processed by the platform operator by way of an escrow service. The payment will only be credited to the seller when the buyer reports that he received the goods or after a certain timeframe has elapsed.

(E) Quantity ordered, shipping options and resulting total price. The price is primarily displayed in conventional currencies and converted in the currency used – in this case, bitcoin.

(F) In the lower part is the "Feedback" tab that lists the feedback on and evaluation of the offer given by the buyers. Under the "Description" tab, a detailed description of the product can be entered. Under the "Refund policy" tab, the seller's refund policies may be viewed. The purchase price of products that are shipped by using a tracking function and do not arrive at their destination is often refunded.

4.2 FORUMS

In terms of their structure and functionalities, forums of the criminal darknet scene hardly differ from the clearnet's customary forums. To participate, a user account is required; personal information need not be provided. In some cases, access hurdles are created and specific sections are separately protected by means of invitation codes, restricted forum sections or "pay to join" criteria.

Police interventions and measures are closely monitored.

Forums provide a platform for discussions, testimonials, announcements and other communication among users. For instance, the quality and trustworthiness of marketplaces, traders and products are evaluated. Measures to conceal user identities play an important role in users' exchange on the darknet. Under the keyword OPSEC (Operations/ Operational Security), in sub-forums there is an active exchange of knowledge and experiences regarding methods, tools and behaviours which aim at protecting one's data against prosecution as effectively as possible. Apart from the use of encryptions and anonymous e-mail service providers, the presumed capabilities and investigative tools of the police and security authorities are frequently discussed. For this reason, marketplace operators, too, are increasingly urging their users to implement security and concealment measures.

Some forums offer additional separate trading areas which allow for the specific placement of offers and requests. The forums' contents and topics are rather diverse, and the individual forums differ widely with regard to their thematic priorities. The spectrum ranges from hacking and the production of narcotic drugs to legal contents. Moderation of the forums is generally limited to enforcing the rules set by the respective operator, which often merely provide for the prohibition of child and juvenile pornography and terrorist contents. In some cases, doxxing of users (i.e. collecting and leaking of personal data) is sanctioned.

In general, darknet forums play an essential role as information, networking and publication platforms for darknet users. With anonymity being ubiquitous, trust is built through mutual personal exchange.

4.3 TRUST ON THE DARKNET

In order to validate the authenticity of statements despite the lack of trust, users apply various technical methods. To ensure the authenticity of a message (a public post or confidential direct message, for instance), digital signatures are regularly used by employing public key encryption methods (particularly OpenPGP). These also allow for information to be encrypted, if need be. In general, on the darknet, a user's PGP key pair is a more important part of his/her online identity than his/her username.

The use of so-called "canary messages" is one way for platform operators to build trust. Here, a specific text message from a hidden service operator is digitally signed and published at regular intervals. The aim is to alert other users at an early stage if the platform has been seized by state authorities or the operator has been arrested. The term 'canary' takes its inspiration from the canaries' warning function in the coal mining industry. When the bird falls silent, there is something wrong.

4.4 LINK COLLECTIONS AND NEWS BLOGS

Link lists provide an overview of the available URLs of the different hidden services. Often they are also accessible from the clearnet. Owing to the lack of efficient search engines, they serve as portals where hidden services are made known.

Just like search engines on the clearnet, link collections are central points of contact on the darknet.

Since on the darknet URLs tend to get changed more often than on the clearnet, link lists also serve the purpose of distributing updated URLs. Some link list providers impose requirements in relation to security aspects (see 'canary' and 'OpenPGP'), which have to be met as a prerequisite for inclusion in the list. Link collections are thus essential for the orientation of users on the darknet.

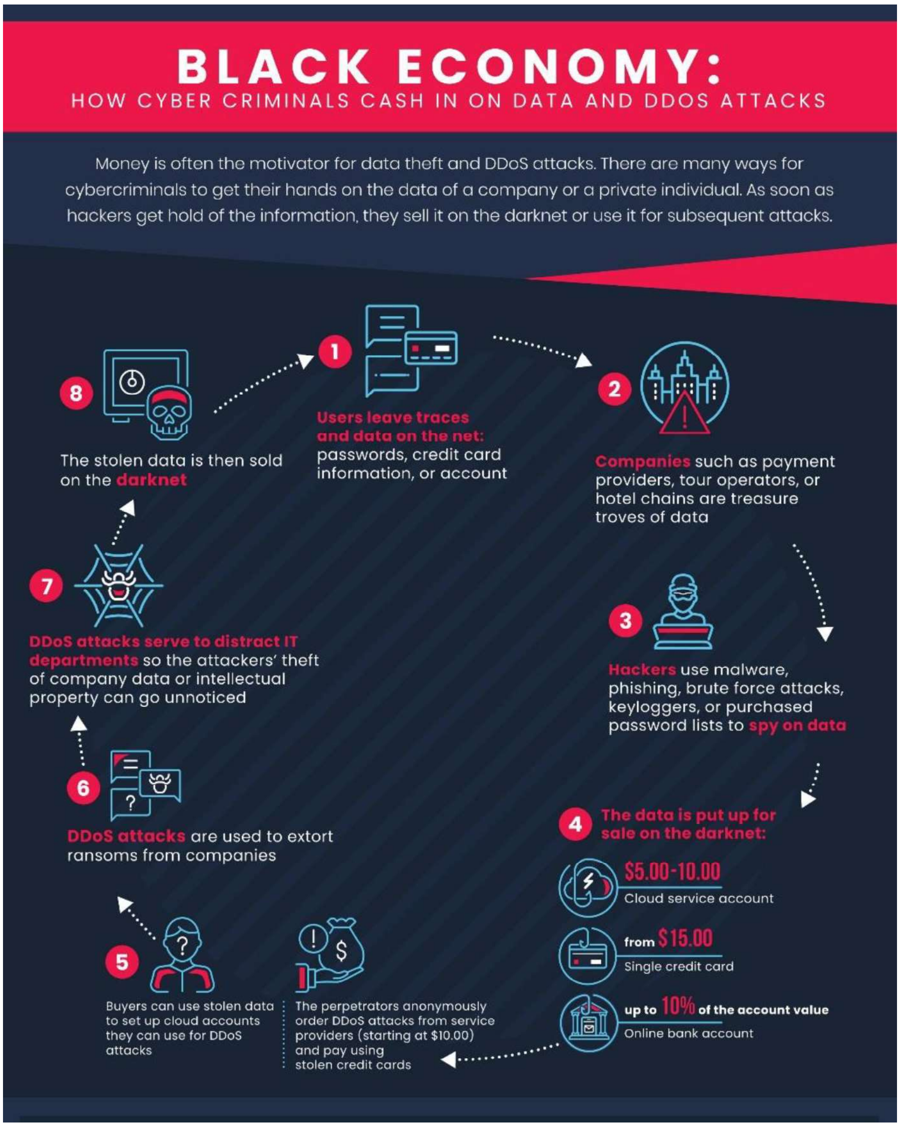
Scene-specific news blogs provide information on incidents concerning marketplaces and traders, e.g. arrests and police investigations. Blogs serve as an important source of information for the community, inter alia when it comes to adapting individual OPSEC measures to one's activities.

4.5 SERVICES

Digital services are another crucial part of the darknet infrastructure. Services such as e-mail accounts, server hosting or VPNs[26] are offered specifically to darknet customers. So-called bitcoin mixers or crypto exchangers have also gained great popularity on the darknet and play an important role in concealing money flows. With its large number of services, the darknet is independent of the clearnet and is meeting all the needs of its users, traders and platform operators.

Using the example of DDoS attacks, the following chart drawn up by Link11 illustrates the impact which digital identity theft and services offered on the darknet may have on the entire value chain in the field of cybercrime:

[26] VPN stands for "virtual private network". The use of such networks, which in principle are legal, allows for anonymous and encrypted Internet communication and data transfer. To this end, the user's IP address is replaced with the IP address of the VPN server.



BLACK ECONOMY:
HOW CYBER CRIMINALS CASH IN ON DATA AND DDOS ATTACKS

Money is often the motivator for data theft and DDoS attacks. There are many ways for cybercriminals to get their hands on the data of a company or a private individual. As soon as hackers get hold of the information, they sell it on the darknet or use it for subsequent attacks.

1 **Users leave traces and data on the net:** passwords, credit card information, or account

2 **Companies** such as payment providers, tour operators, or hotel chains are treasure troves of data

3 **Hackers** use malware, phishing, brute force attacks, keyloggers, or purchased password lists to **spy on data**

4 **The data is put up for sale on the darknet:**

$5.00-10.00 Cloud service account

from $15.00 Single credit card

up to 10% of the account value Online bank account

The perpetrators anonymously order DDoS attacks from service providers (starting at $10.00) and pay using stolen credit cards

5 Buyers can use stolen data to set up cloud accounts they can use for DDoS attacks

6 **DDoS attacks** are used to extort ransoms from companies

7 **DDoS attacks serve to distract IT departments** so the attackers' theft of company data or intellectual property can go unnoticed

8 The stolen data is then sold on the **darknet**

Copyright chart: Link11

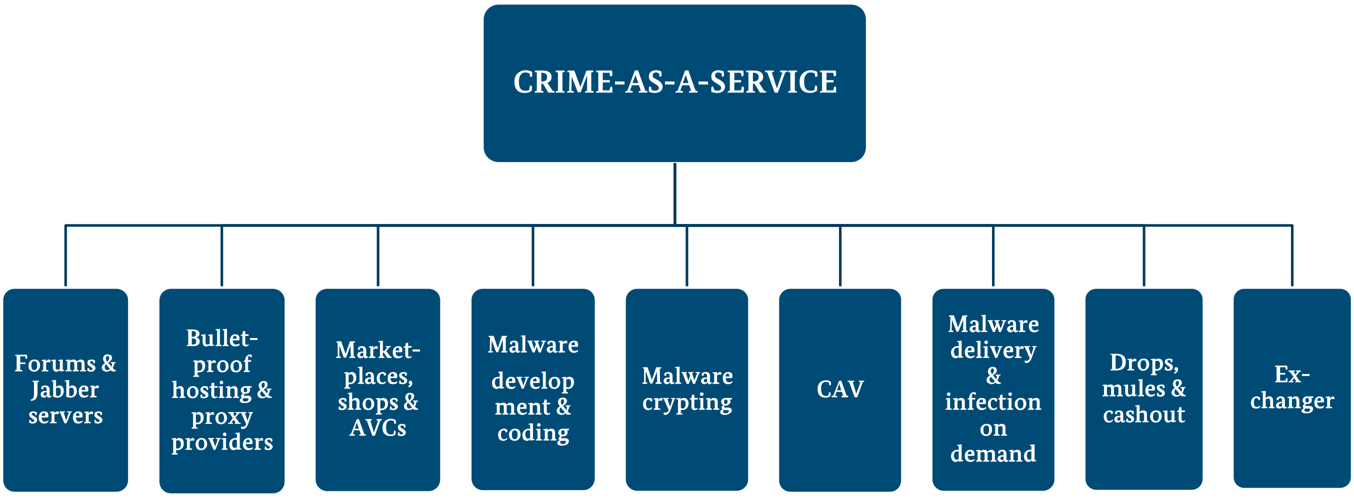
4.6 CYBERCRIME AS A SERVICE / THE NINE-PILLAR MODEL

Investigations conducted by the BKA in recent years have revealed that in the field of "Cybercrime-as-a-Service" (CCaaS) there is a high degree of division of tasks among the persons involved in an offence, and that individuals specialise in specific relevant contributions to the offence.

Cybercriminals increasingly focus on committing offences in an 'order-oriented' manner or facilitating them in a service-oriented way. It was found that active offenders outsource individual support services to outsiders and groups of perpetrators specialised in specific cybercrime services and/or purchase such services from them. The resulting fragmentation also allows less cyber-savvy offenders to commit technically more complex offences.

According to our information, this phenomenon or criminal ecosystem is based on nine pillars[27], which are described hereafter and several of which will be presented in more detail by way of case-specific facts from the reporting year 2019:

Pillar 1: Forums and Jabber servers


CRIME-AS-A-SERVICE
Forums & Jabber servers
Bullet-proof hosting & proxy providers
Market-places, shops & AVCs
Malware develop ment & coding
Malware crypting
CAV
Malware delivery & infection on demand
Drops, mules & cashout
Ex-changer

Forums[28] and Jabber[29] servers represent central communication hubs, they are "business directories" for providers of criminal services and individuals interested in such services. In these contact forums actors can share their requests and needs as well as their capabilities and products offered.

In addition, forums play a significant role in ensuring the "quality" of criminal services provided on the darknet: by means of rating systems customers can evaluate a product or service offered by a 'cybercrime provider', for instance by giving a star rating. The number and quality of positive ratings thus reflect a trader's reputation and/or standing within the community and are therefore important to the latter when it comes to obtaining further orders and imposing prices.

Case example: Police measures against forum administrators

Within the framework of an investigation conducted by the police in Rhineland-Palatinate and following extensive investigative measures, one of the main administrators of the largest German underground economy forums, Fraudsters, was arrested in Pinneberg in early July 2019.

This forum was, inter alia, used to commit currency counterfeiting, document forgery and narcotics offences and to exchange illegally obtained data. The forum had approximately 30,000 registered users. Within the framework of the proceedings, the suspect was sentenced to 6 years' and 8 months' imprisonment by Bad Kreuznach Regional Court.

[27]The following case examples exclusively deal with cases relevant to the year 2019/early 2020.
[28] An online forum is a virtual place where thoughts, opinions and experiences can be exchanged.
[29] Jabber is a provider-independent virtual instant messaging communication service.

Brief assessment:
In Germany, this was the first ever conviction for the formation of a criminal organisation pursuant to section 129 of the German Penal Code in connection with cybercrime offences. Since in similar proceedings it has not yet been possible to prove that the groups of perpetrators committed specific offences, which can only be carried out on the basis of an organisation, this judgement marks a milestone in the fight against cybercrime.

Pillar 2: Bullet-proof hosting and proxy providers

Since numerous modi operandi attributed to the field of cybercrime in the narrower sense require technological infrastructures which are resistant to intervention, criminal hosting service providers have specialised in providing safe server structures (IP addresses, domains) or proxy[30] and/or VPN providers. To this end, criminal hosting service providers often rent servers from commercial data centre operators and make them available to criminal customers against payment. The customers' aim is that the server structures operated remain online for as long as possible. Since complaints about the fraudulent use of a server are usually sent to the criminal host first, the latter is able to ignore them for long enough until the regular data centre operator will intervene and take the server offline, if need be. By then, the cybercriminals may already have completed the offence.

Case example: Bullet-proof hosting - "Cyberbunker"

Starting 2013, Rhineland-Palatinate Land Criminal Police Office conducted extensive investigations into the operators of a bullet-proof hosting data centre located in a former nuclear bunker which, in the scene, was also known as "Cyberbunker". Various sites were hosted there via which internationally operating criminals sold illicit goods such as narcotic drugs, forged documents and stolen data, disseminated child abuse material and carried out extensive cyberattacks.

The investigations substantiated the suspicion against a total of 13 suspects in connection with the formation of a criminal organisation (section 129 of the German Penal Code), and aiding and abetting serious drug offences, counterfeit currency deals and handling stolen data in hundreds of thousands of cases, as well as aiding and abetting the dissemination of child abuse material.

During concerted searches carried out in September 2019, various means of evidence were seized, inter alia 400 servers.

Brief assessment:
On 07/04/2020, the Land's central office for cybercrime (Landeszentralstelle, LZC) of Koblenz Public Prosecutor General's Office preferred charges against the suspects. According to the criminal assessment of the investigative complex made by the public prosecutor's office, this is a case of formation of and participation in a criminal organisation.

[30] A proxy is a communication interface in a network which, acting as an intermediary, receives requests on the one end and then, using its own address, establishes a connection to the other end.

Pillar 3: Marketplaces, shops and Automated Vending Carts (AVCs)

Criminal offenders require and/or use compromised access data for numerous cybercrime offences. Automated marketplaces/shops on the darknet offer such data.

Narcotic drugs are by far the most favoured products purchased and sold.

The external structure of such marketplaces often resembles those of regular online trading platforms found on the clearnet. The following products and services are typically offered on darknet marketplaces:

- Digital identities,
- Online access data (such as e-mail addresses, online banking accounts),
- Payment card data,
- Provision of servers,
- Narcotic drugs and
- Weapons.

Pillar 4: Malware development/coding
Malware is generally developed in accordance with the buyers' requirements; the latter will outline the basic functionalities of the malware required and look for suitable programmers in forums. At present, the following malware families are considered the most prevalent: Emotet, Dridex, Ryuk, Trickbot and Maze.

Pillar 5: Malware crypting
As a result of the significant improvements concerning both AV products and operating systems, offenders' requirements for malware, which is both effective and, above all, cannot be detected, have increased in recent years. For this reason, crypting service providers have been focussing on altering and/or encrypting malicious code in such a way that the malware cannot be detected by antivirus products.

Case example: Malware crypting

Within the framework of an investigation conducted since 2018, the BKA identified a Tunisian national living in Germany who is suspected of having released malware, which he had encrypted, for upload on a darknet forum using a virtual identity.

The investigations revealed that the suspect had been working as a crypter for a separately prosecuted user of the darknet forum, and that he had been acting as a crypting service provider in the cybercrime scene for many years.

The analysis of the communication revealed that the suspect had been advertising on numerous forums appealing to cybercriminals for years in order to win customers for crypting services. He is suspected of having encrypted malware on a large scale - particularly on behalf of the Russian cybercriminal scene - and thus having protected it from detection. Doing so, he is to have aided and abetted the commission of ensuing offences for which the malware was used.

Brief assessment:
This example clearly demonstrates that crypting constitutes both an essential part of malware development and a separate economic branch of the underground economy. In addition, it underlines the outstanding importance of international police cooperation with regard to successful cybercrime investigations.

Pillar 6: Counter Antivirus (CAV) services

Detection of the malware by AV products generally results in the infected victim system no longer being available for further criminal activities. In the underground economy, technically highly specialised counter antivirus service providers therefore offer to test malware samples regarding the rate at which they are detected by AV products. As the providers of such services work in a very agile manner, their customers will always receive an up-to-date evaluation of both the viability and functionality of their malware.

Pillar 7: Malware delivery / infection on demand

Malware can only release its criminal energy once it has infected victim systems and is spreading. In the CCaaS ecosystem there are so-called content delivery networks which have specialised in the distribution and installation of their customers' malware. These networks can often rely on a substantial number of computers already infected with different malware (botnets). The former can take advantage of their access to these computers in order to infect the latters' systems with the malware provided by their criminal customer. Criminal content delivery service providers are paid a success fee which is based on the number of successful malware installations on third-party systems ("Pay per Install").

Pillar 8: Drops, mules and Cashout

The main task of these service providers is to realise the monetary added value generated through criminal trade. From an offender's perspective, this activity poses the greatest risk as they will have to operate outside of the digital world. Illicit payments have to be transferred to accounts and withdrawn at ATMs. Fraudulently ordered shipments have to be collected at parcel stations or "dead" letterboxes. For this so-called "cashout", the persons behind a cyberattack quite often hire a separate criminal service provider, who, in turn, will task a subcontractor - so-called "runners" or "drops" - with actually collecting the goods or the monies. The monies and profits obtained in connection with the goods are usually transferred to the actual criminal party ordering the goods/services by means of cryptocurrencies.

Pillar 9: Exchanger

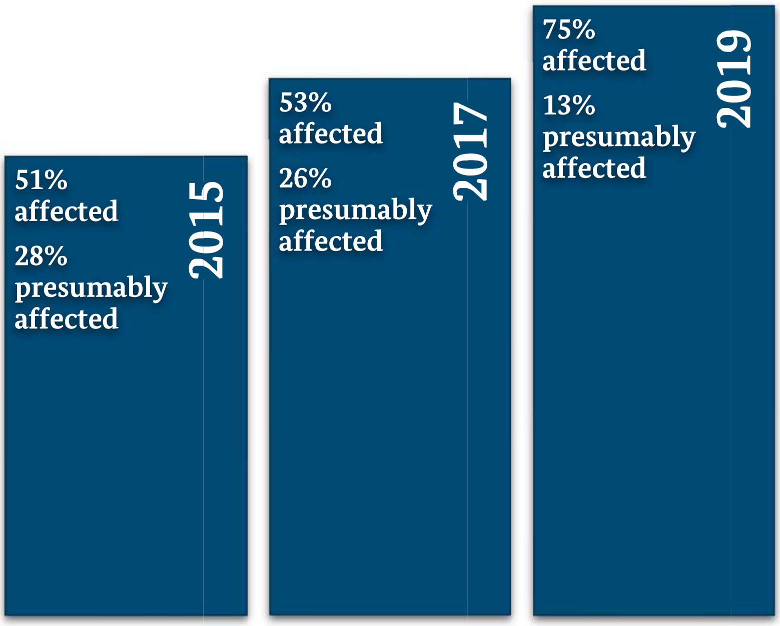
This pillar of CCaaS deals with money laundering in the digital space. The goal is to convert a digital currency into one or more other state or digital currencies in a cost-effective manner (so-called mixing services). In addition, illicit transactions are, at the same time, to be concealed to the greatest degree possible. Criminal "exchangers" have extensive knowledge of the technologies and business processes found in the field of cryptocurrencies as well as of the framework conditions in the financial sector.

Police experience concerning mixing services

- *The police have already shut down various mixing services and seized the corresponding transaction data.*
- *So-called "de-mixing" is possible; cryptocurrencies are not as anonymous as many offenders would like to think - cryptocurrencies, too, may provide promising investigative leads.*
- *The quality of the concealment often depends on the price demanded by the exchanger.*
- *The phenomenon of fraudulent mixing services: While they will accept a customer's cryptocurrency, they will not convert it or pay it back to the customer. A cybercriminal, who was duped, will rarely ever file a complaint.*

5 Attacks on the Economy and Critical Infrastructures

The German economy has been a popular target for cybercriminals - a BITKOM study[31] dated February 2020 found that the number of companies actually affected by a cyberattack significantly increased again in 2019.



[32]

In 2019, three out of four companies fell victim to cybercriminals - in 2017 it was but every other company.

Companies are subject to a broad range of cyberthreats - be it espionage or fraudulent modification of sensitive data, the disruption of server and website availability, manipulation of websites, malware infection, or encryption or even destruction of data. Owing to the increasing professionalism on the offenders' part, the situation further deteriorated significantly in the last year - modi operandi are becoming more complex, and both the way in which the latter interact and the type of attack vector used are becoming more sophisticated and diverse. It is not always the company itself which represents the entry vector of a cyberattack - cybercriminals often exploit the company's supply chain or the IT systems of its business partner(s) in order to compromise their actual target.

[31] Available at: https://www.bitkom.org/sites/default/files/2020-02/200211_bitkom_studie_wirtschaftsschutz_2020_final.pdf

[32] Number of respondents (n):
2015: n = 1074
2017: n = 1069
2019: n = 1070

In addition, in 2019 a modus operandi was identified according to which offenders actively scan the Internet for systems offering remote maintenance access. A so-called brute force attack is carried out on the passwords of such systems and, following successful login, malware and ransomware are installed.

Small companies and an increasing number of large private enterprises, but also more and more public institutions, are now in the focus of cybercriminals.

G4C and BITKOM have identified another development: While in 2018 attacks focused on business enterprises, particularly small and medium-sized enterprises (SMEs), in 2019 cybercriminals increasingly focused on so-called "big game hunting", i.e. targeted attacks on large companies and institutions.

Along with the modus operandi of double extortion mentioned in chapter 4.1, overall, there has been a qualitative increase with regard to both the intensity and the dimension of cyberattacks on the German economy.

In the year 2019, a loss amounting to approximately 102.9 billion euros was caused by cyberattacks on business enterprises.

According to BITKOM, the projected loss caused by cyberattacks in 2019 amounts to 102.9 billion euros - which is almost double the amount identified in 2017/2018, i.e. 55 billion euros.

The so-called critical infrastructures[33] - the institutional "central nervous system" of society and public order - are increasingly bracing themselves to counter and manage cyberthreats. Since failure of a critical infrastructure would result in the disruption of essential public processes, protection of the former is of utmost importance, also within the framework of police action aimed at warding off danger, and criminal prosecution.

Enterprises with critical infrastructures are obliged to report disruptions to the Federal Office for Information Security (BSI). In its 201934 situation report on IT security, the BSI states that 252 incidents were reported between 31/05/2018 and 01/06/2019. In contrast to the previous year, the majority of incidents reported related to the financial sector, closely followed by the IT and telecommunications sector. The percentage of incidents recorded by the BSI thus increased significantly, compared to previous year's report (145 incidents).

[33]Critical infrastructures include the sectors energy, water, food, information technology and telecommunications, finance and insurance, transport and traffic, health, media and culture as well as government and administration.

[34] "Die Lage der IT-Sicherheit in Deutschland 2019" (The State of IT Security in Germany 2019), available at: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2019.pdf

Given the developments outlined, it has to be assumed that the number of cyberattacks on critical infrastructures will further increase.

Case example: Ransomware attack caused a loss amounting to 2.4 million euros

Schleswig-Holstein Land Criminal Police Office advised that from early September 2019, a company seated in their jurisdiction was blackmailed by unidentified offenders (section 253 of the German Penal Code). The offenders had accessed the company's IT systems and encrypted all relevant data and systems using the ransomware iEncrypt.

As is usual with numerous ransomware variants, following the encryption an extortion message was displayed, demanding that a ransom be paid for the decryption of the data and referring to different e-mail addresses for further information. Once contact had been made via these e-mail addresses, which were linked to the iEncrypt ransomware, the company received the following reply from the offenders:

„Hello,
Attached is one decrypted file
We have an error with the second one "tablfertigung Berechtigung.xlsx", the file was modified in your environment AFTER the encryption process (we cannot help if you manipulate the files intentionally)
If you want to test it again, make sure the file itself and _readme are not corrupted in any way (do not rename or change the file name/format or its content)
The price is $2,600,000 (two million six hundred thousand)
The bitcon address for the payment: 3DCCbrz1FZRDqRLNRiJ63UzAVPqNUnDu8B
It takes around 40-80 minutes to get enough confirmations form the blockchain, in order to validate the payment
Upon receipt we send you the tool“

Brief assessment:
It has to be assumed that the offence was committed on a repetitive and gainful basis. In addition to the investigations conducted in Schleswig-Holstein, further similar cases, which were committed in the Federal Republic of Germany and which were clearly linked to the offence, came to notice. In each of the cases, the ransom demanded for decryption was at least in the six-digit range. This demonstrates the potential magnitude of a ransomware infection. Losses of this scale may threaten the existence of a company. For this reason it is indispensable, particularly for companies, to regularly make backups in order to not be at the mercy of an offender in case of a ransomware infection (please see chapter 9.4).

With regard to attacks on business enterprises, in the media as well as on channels of IT security service providers there is often mention of particularly complex cyberattacks, so-called APTs.

Characteristic of APT attacks is that they are used both for espionage, i.e. spying out data, and for sabotage, i.e. disturbing processes. APTs are often carried out by government-backed groups or groups similar to intelligence services.

Advanced Persistent Threats (APTs)

APTs are targeted cyberattacks on selected institutions and facilities where the attacker gains permanent access to a network and subsequently extends it to further systems. Such attacks are characterised by a very high deployment of resources and significant technology skills on the part of the attackers, and are usually difficult to detect.

In recent years, however, non-governmental groups, too, have increasingly been adopting this form of attack and, acting professionally, are thus gaining long-term, comprehensive access to third-party systems. Consequently, APT is no longer a distinguishing feature of government or government-related groups but a form of attack employed by a growing number of cybercrime actors.

APTs represent existential threats for companies.

With regard to government-controlled cyberattacks, the BKA has ascertained the following:

- Cyberattacks against Germany remain an important method for foreign intelligence services to collect information.
- Time and time again, dynamic server infrastructures and highly professional malware components, subject to permanent sophistication, are used for cyberespionage attacks throughout the world.
- Groups also adapt their attack narratives to current political and social situations and challenges, and take advantage of the population's fears and need for information.
- Most attacks are preceded by targeted "social engineering operations". The main attack vector is the sending of "spear phishing e-mails"[35], including both malicious links and malicious attachments, which are used to infect the victims' systems. Prior to launching cyberespionage attacks, criminals usually check the targeted persons in a professional manner. To this end, they do not only carry out specific checks on the Internet and in social media but also apply classical methods of espionage, such as gathering communications intelligence and using agents.

[35] "Spear Phishing" refers to more sophisticated phishing using a more targeted personal approach ("spear").

- Publications of numerous private IT security providers regularly point out that Germany is one of the targets of cyberespionage attacks. However, a concrete and reliable attribution of such intelligence service/government-controlled attacks is hardly possible.
- The percentage of unreported crimes is likely to be high as a result of undetected and/or unreported attacks.
- In its analysis[36] of various APT groups, the security company FireEye says that the former's operational bases are primarily found in China, Russia, North Korea, Vietnam and Iran.

Due to the comparatively high level of competitiveness and technological expertise of the companies located in Germany, the domestic business hub will remain an interesting target for cyberespionage and/or hackers committing offences of a general nature. Regardless of current economic developments, companies in Germany will very likely remain in the focus of cybercriminals. Due to the growing professionalism displayed by cybercriminals committing offences of a general nature, the latter increasingly employ APTs and, in consequence, will also become a critical threat for companies. This trend is being facilitated by the fact that profound IT knowledge is no longer indispensable and necessary components are available through the CCaaS ecosystem - as a consequence, there is an increased probability of highly-complex and serious attacks being launched by a wider spectrum of offenders.

Case example: SOFACY/APT 28

Since 2015, on behalf of the Federal Public Prosecutor General at the Federal Court of Justice, the BKA has been conducting investigations into unknown members of the Russian military intelligence service GRU[37], inter alia for electronic espionage concerning the German Bundestag (German Federal Parliament) in spring 2015. The investigative proceedings include numerous other offences linked to GRU and/or the cyberattack campaign SOFACY/APT28.
The case complexes which are the subject of the proceedings involve electronic attacks on internal IT networks, such as those of parties, political foundations and socio-political research institutions.

The examination and/or forensic analysis of the servers seized thus far have provided both comprehensive insights into the different forms of malware used by the SOFACY/APT28 group and information on the individuals involved. On 29 April 2020, the examining judge at the Federal Court of Justice issued an arrest warrant for one of the individuals concerning the electronic attack on the German Bundestag.

Brief assessment:
The case complexes are proof that the actors behind SOFACY/APT28 have a global IT infrastructure at their disposal and are utilising a complex network of servers to carry out cyberattacks. Within the framework of the investigations, numerous servers of Internet service providers based in Germany, who had offered anonymity and identity protection and accepted anonymous means of payment, were seized.

[36] https://www.fireeye.de/current-threats/apt-groups.html
[37] Glawnoje Raswedywatelnoje Uprawlenije, Translation: Main Intelligence Directorate

6 Police Crime Statistics

100,514 cases of cybercrime in the narrower sense (+15.4%)

294,665 cases where the Internet was used as an instrument of crime (+8.4%)

78,201 cases of computer fraud (+18.0%)

87.7 million EUR loss in the area of computer fraud (+44.4%)

9,926 cases of data espionage/interception of data (+13.3%)

FÄLSCHUNG

8,877 cases of forgery of evidentiary data/deception in legal relations (+5.1%)

3,183 cases of data manipulation/computer sabotage (+10.7%)

6.1 RECORDING MODALITIES

Cybercrime as a phenomenon distinguishes between cybercrime in the narrower sense and cybercrime in the broader sense[38].

The 2019 National Situation Report on Cybercrime provides information about the developments in the field of cybercrime in the narrower sense that came to police notice. It also includes information about cybercrime in the broader sense in view of the fact that the so-called underground economy is an essential part of cybercrime.

When looking at the statistical data gathered by the police, the specific recording and counting modalities in the Police Crime Statistics (PCS) must be taken into account. Furthermore, when interpreting the statistical data it must be kept in mind that some relevant phenomena, such as acts of extortion committed in connection with targeted DDoS attacks or ransomware, are, for instance, usually not recorded as cybercrime offences in the PCS but as more serious or specific offences - in this case as extortion.

Despite the limited informative value the PCS has with regard to the entirety of cybercrime offences committed in Germany, it provides a database which at least facilitates trend statements in this area of crime.

The police keep pointing out that victims should report any act of cybercrime: early reporting effectively counteracts the volatility of digital traces and increases the prospects of identifying the perpetrator(s). The common objectives are to identify the originators of cyberattacks, bring them to justice, deter potential perpetrators with a view to preventing reoffending and/or "copycat" offending. A comprehensive situation report also leads to new investigative approaches for more effective suppression (e.g. by analysing the attack vectors or detecting links between offences).

6.2 CYBERCRIME CASE FIGURES

The year 2019 witnessed another increase in the number of offences attributed to cybercrime in the narrower sense. The PCS showed a total of 100,514 cases. This represents a rise of 15.4% compared to the previous year (2018: 87,106 cases). The clear-up rate was 32.3%, which represents a decrease of 6.6% compared to the previous year.

More than three quarters of all offences were recorded as computer fraud cases. In 2019, there was an increase of 18.0% in this field of criminal activity. In most of these cases the Internet was merely used as the instrument of crime.[39] This means that they do not constitute cases of cybercrime in the narrower sense. This is one of the reasons why the PCS case numbers require differential consideration and evaluation.

The number of cases attributed to the misuse of telecommunications services pursuant to section 263a of the German Penal Code decreased by 49.2% to 327 cases (2018: 644 cases) in the reporting year. The main reason for this decline is the conclusion of a complex investigation conducted by

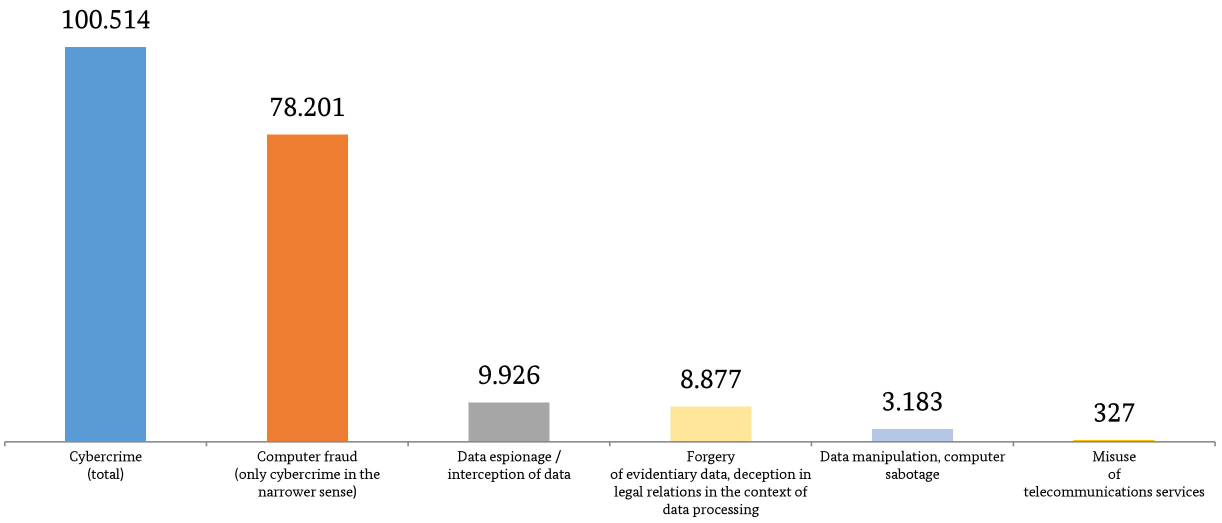
[38] Cybercrime in the broader sense includes all offences committed with the aid of the Internet as an instrument of crime.

[39] For instance obtaining goods or services by fraud through the following method: When attempting to acquire goods or services through the Internet, the fraudsters fail to pay the goods/services purchased.

Oldenburg public prosecutor's office and Osnabrück police station[40]. It involved numerous (cleared-up) individual cases and thus caused the high case numbers in 2018.

In the field of data manipulation/computer sabotage pursuant to sections 303a, 303b of the German Penal Code, there was an increase of 10.7%. 3,183 cases were recorded (2018: 2,875 cases).

Cases of Cybercrime in the Narrower Sense (2019)



The Police Crime Statistics provide only a limited basis for statistical statements on the overall financial loss arising from cybercrime since they solely indicate losses resulting from computer fraud and the misuse of telecommunications services. The total loss in these two fields of crime recorded for 2019 amounted to EUR 88.0 million (2018: EUR 61.4 million). This represents a 43.3% increase compared to the previous year. EUR 87.7 million were attributable to computer fraud (2018: EUR 60.7 million).

6.3 SUSPECTS

In 2019, a total of 22,574 individuals suspected of cybercrime were recorded. Compared to the previous year, this is an increase by 2.4% (2018: 22,051 suspects). 68.3% of all suspects were male, 31.7% were female.

What is striking is that female suspects are over-represented in the field of cybercrime in the narrower sense in relation to the total offences recorded in the PCS (share 25.0%). The criminal offence of computer fraud, primarily the obtaining of goods by fraud, is the decisive factor for this. This offence type has high case numbers and a high percentage of female suspects (computer fraud pursuant to section 263a of the German Penal Code – female suspects: 34.1%; obtaining goods by fraud pursuant to sections 263, 263a of the German Penal Code – female suspects: 33.9%).

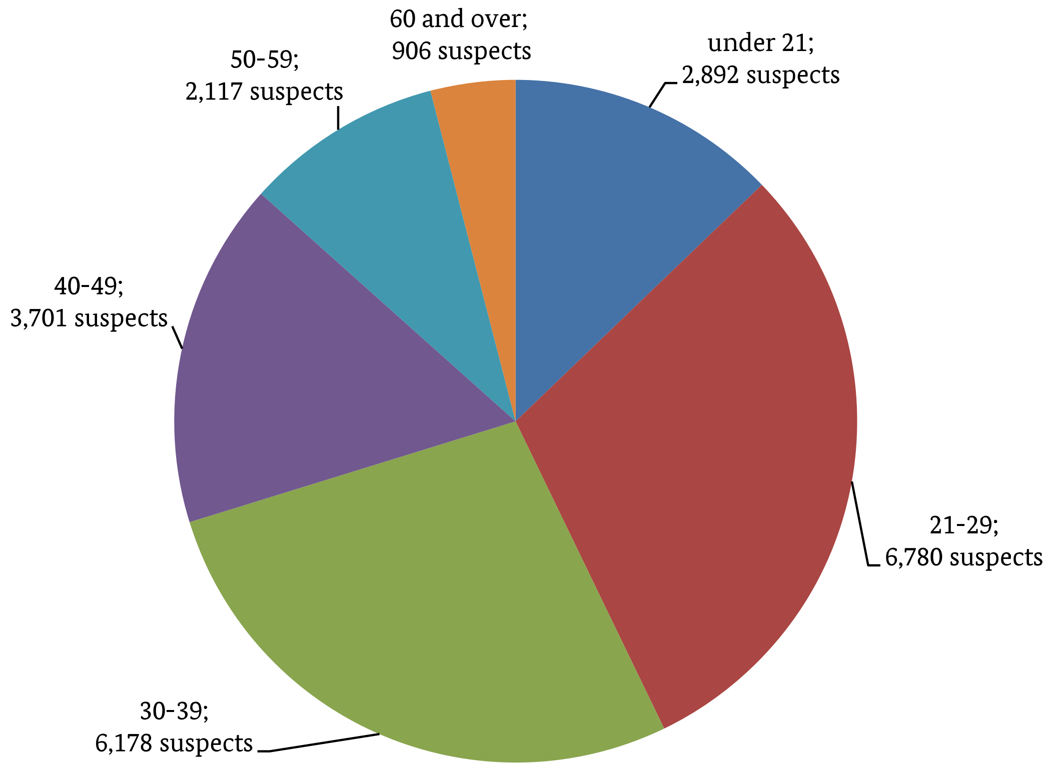
[40] In this investigative complex a suspect gained access to so-called FRITZ! Boxes through the Internet and programmed call forwarding to premium rate numbers. Subsequently, call forwarding was activated automatically so that chargeable connections were made from the router/subscriber's line that had been tampered with. Disguising his real identity, the suspect "rented" the previously programmed national and international premium rate numbers and obtained part of the telephone fees incurred.

With respect to cybercrime offences with lower case numbers, the percentage of female suspects is almost identical with their share in the total number of offences (e.g. data espionage, interception of data, handling stolen data pursuant to sections 202a-d of the German Penal Code: 25.2%), or even lower (e.g. data manipulation, computer sabotage pursuant to sections 303a, b of the German Penal Code: 22.4%).

In 2019, 17,015 identified suspects (75.4%) were German nationals. 5,559 suspects were non-German nationals; Turkish (13.2%), Romanian (9.2%) and Polish (6.1%) nationals came to notice most frequently. The high percentage of all three groups of nationals is attributable to the offence of obtaining goods by fraud.

More than half (57.4%) of the recorded offences assigned to the field of cybercrime in the narrower sense were committed by suspects aged between 21 and 39 years.

Age Structure of Suspects (2019)



The spectrum of perpetrators ranges from lone offenders to internationally organised crime groups. Jointly acting offenders rarely operate in hierarchical structures to commit cybercrimes. Frequently, they do not know each other personally and prefer the higher level of anonymity the Internet offers even when operating on a division-of-tasks basis.

Offenders respond quickly and flexibly to new technical developments and adapt their behaviour accordingly. Services they are unable to provide are purchased in the underground economy (see chapter 5).

6.4 ORGANISED CRIME

Organised crime (OC) groups also operate in the area of cybercrime. Ten of the altogether 579 OC investigations reported for 2019 were conducted for cybercrime offences (2018: 13 OC investigations).

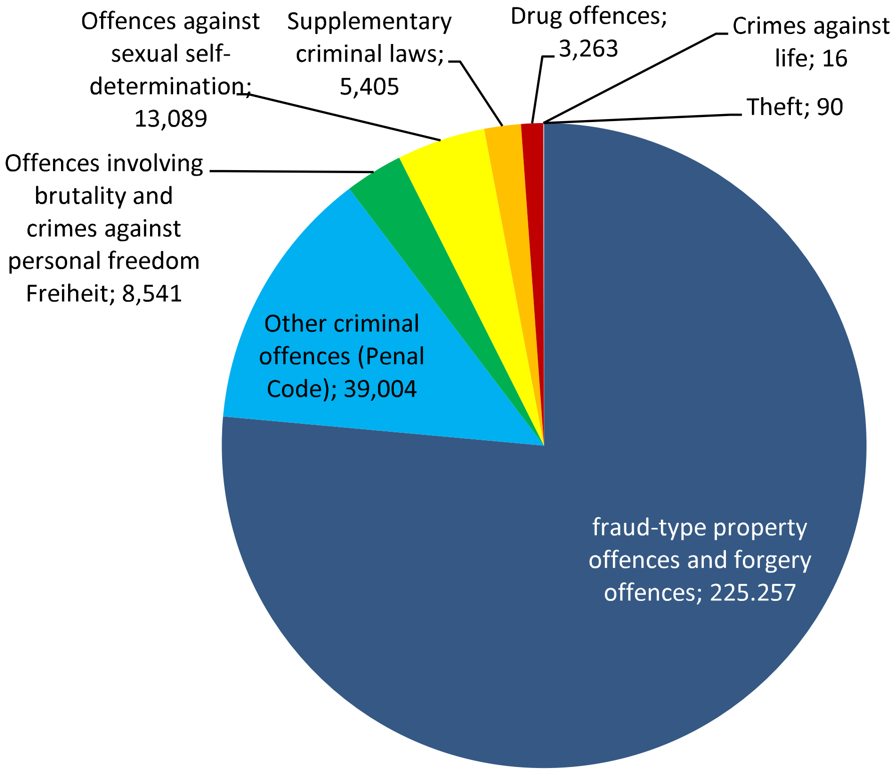
Organised structures committed the same cybercrime offences as individual perpetrators and loose networks. These were mainly computer fraud offences, attacks on online banking and the distribution of ransomware for digital extortion.

6.5 THE INTERNET AS AN INSTRUMENT OF CRIME

In 2019, a total of 294,665 cases were recorded in the PCS where the Internet had been used as an instrument of crime. This represents an increase of 8.4% compared to the previous year (2018: 271,864 cases).

The PCS special designation[41] "Internet as an instrument of crime" is assigned whenever the Internet plays an important role for the commission of offences, as in the case of extortions in connection with DDoS attacks or transactions with online mail order shops. The special designation, however, is not used if, for instance, there had only been casual contact between offenders and victims via the Internet prior to the actual offence.

The Internet as an Instrument of Crime - Distribution by Fields of Criminal Activity (2019)



[41] Special designations are characteristics which can optionally be selected in the PCS when recording a crime. Certain PCS-relevant forms of crime are marked with special designations.

In 2019, 74.1% (218,270 cases) of all offences where the Internet was used as an instrument of crime were fraud offences (2018: 75.7%; 205,735 cases). These included 156,966 offences (2018: 154,773 cases) designated "fraudulent failure to supply goods as agreed", where suspects offered goods for sale on the Internet but provided only inferior-quality items or none at all, or "obtaining goods by fraud", in which goods were ordered and not paid for.

7 Overall Assessment and Outlook

Cybercrime continues to gain in importance. This is evidenced by the police case figures as well as numerous studies and analyses of this phenomenon. The industry association BITKOM (German Association for Information Technology, Telecommunications and New Media) arrived at the conclusion that both quantity and quality of cyberattacks have increased and the data from the 2019 PCS support this conclusion. Furthermore, various other studies corroborate the assumption that the number of unreported and unrecorded cybercrimes is high and that police data alone do not give a realistic picture of this field of crime.

According to a survey conducted by the "eco-Verband" (Association of the Internet Industry)[42] in 2020, 91% of all companies interviewed assessed the overall threat to Internet security to be growing or even skyrocketing. None of the respondents stated that the danger posed by cybercrime had diminished. In a spring 2019 survey[43] by the "Forsa Institute for Social Research and Statistical Analyses" on "Cyberrisks in German Small and Medium-sized Businesses" (representative survey of 300 decision-makers at small and medium-sized businesses), 24% of respondents stated that they had already suffered economic losses caused by cyberattacks. The losses were mainly due to costs for clearing up the incident and data recovery and/or damage caused by interruptions of operations. However, indirect economic damage resulting from reputational harm or the theft of company secrets also plays a role for the companies affected after such attacks.

For the "Allianz Risk Barometer 2020"[44], more than 2,700 persons from different industrial and economic sectors in 102 countries were interviewed about the most significant business risks. For the first time in 2019, a share of 39% of respondents considered "cyber incidents", such as cybercrime, IT failures and data breaches, to be the greatest business risk. In 2013, this risk had ranked only at position 15 with a share of 6% of answers. Companies are increasingly exposed to data scandals and a growing number of other cyberattacks, such as extortions and spoofing.

According to the study „e-Crime in the German economy 2019“[45] undertaken by the KPMG audit company, 39 % of all companies in Germany had been affected by cybercrime in the past two years. A representative selection of 1,001 companies had been interviewed for the study. Identification of offenders is particularly difficult for the companies. 80 % of those affected are only able to recognise that unknown persons from outside their company are responsible for the attack. It is therefore highly likely that not only the perpetrators, but also the actual offences committed will remain unrecognised.

[42] Extract available at: https://www.eco.de/presse/eco-it-sicherheitsstudie-2020-unternehmen-ruesten-sich-fuer-den-ernstfall/

[43] Cyberrisiken im Mittelstand. Ergebnisse einer Forsa-Befragung. Frühjahr 2019 (Cyberrisks in Small and Medium-sized Businesses. Results of a spring 2019 Forsa survey), available at: https://www.gdv.de/resource/blob/48506/a1193bc12647d526f75da3376517ad06/cyberrisiken-im-mittelstand-2019-pdf-data.pdf, p. 5.

[44] Allianz Risk Barometer 2020 – Cyber incidents, available at: https://www.agcs.allianz.com/news-and-insights/expert-risk-articles/allianz-risk-barometer-2020-cyber-incidents.html, published on 14/01/2020

[45] e-Crime in the German economy 2019, available at: https://hub.kpmg.de/studie-e-crime-in-der-deutschen-wirtschaft-2019

The developments in the individual fields of cybercrime already identified in 2018 continued in 2019. Threats posed by cybercrime are at a high level and will continue to increase due to further technical developments and the ongoing spread of digital technology. It became clear again in the reporting year that the IoT was actively used for the reinforcement of DDoS attacks.

> ***The perpetrators run an organised and highly-professional industry, which is based on a division of seamlessly interacting tasks and grows through each successful attack.***

The characteristic feature of cyberattacks committed in 2019 is the linking of value chains: data are first stolen in a criminal manner and then used as a basis for further criminal activities. Illegal profits can be generated at various points of the chains by purchasing and selling these data and using them in different ways in cyberspace.

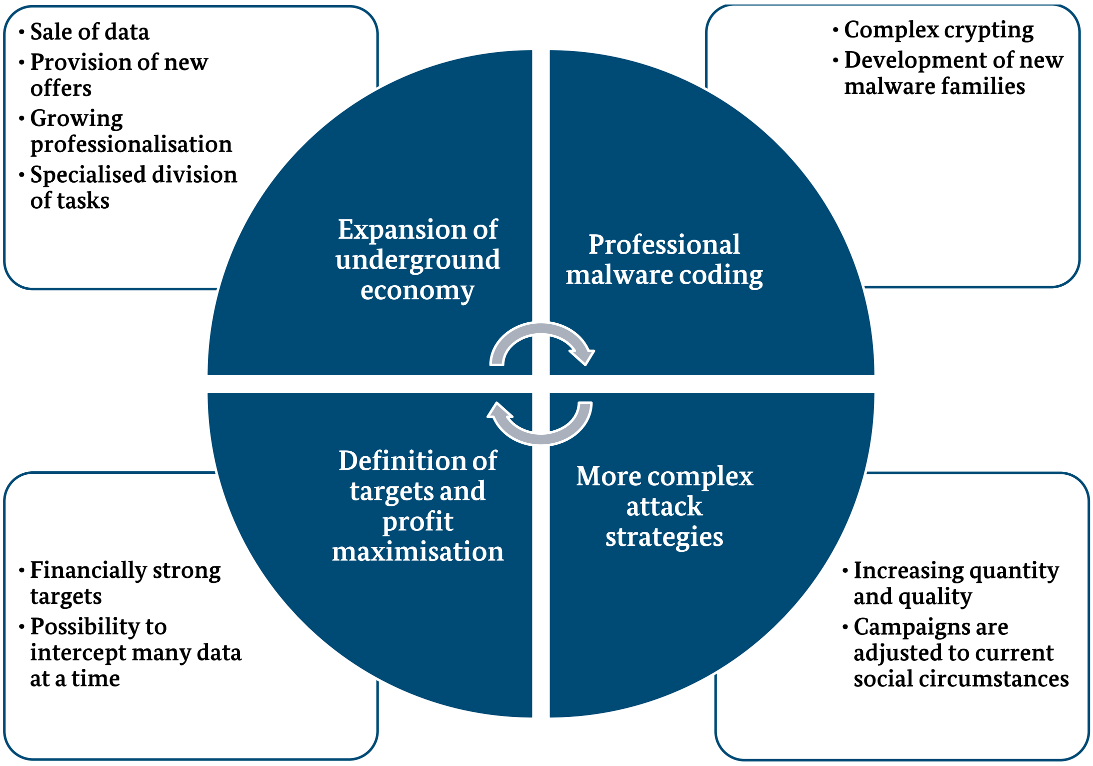
The present cybercrime situation report shows four key developments:

1. The perpetrators are becoming increasingly professional - not only with regard to malware coding but also when it comes to the specialising division of tasks in the underground economy. In this way, an organised, autonomous industry is establishing itself, which damages (fundamental) parts of society.

2. This professionalisation leads to an increase in quantity and quality of cyberattacks: While the malware families and attack campaigns employed are becoming more sophisticated and technically complex, skilful and proficient actors are establishing themselves perfecting the infrastructures of the underground economy thereby creating the basis for further, resource-consuming cyberattacks.

3. To generate maximum profit, cybercriminals direct their attacks on business enterprises and public institutions. Not only do cybercriminals attack apparently lucrative institutions - they also know that the failure of one of these elements can have far-reaching implications and can therefore be used to reinforce ransom demands. With this in mind, cybercriminals select their targets with a view to causing maximum harm to society.

4. Each successful attack serves as a breeding ground for the cybercrime scene. Through the acquisition of financial means the underground economy grows, new offers emerge, new data are sold and new actors step forward. This is where the value chain starts again - with increased intensity.


• Sale of data
• Provision of new offers
• Growing professionalisation
• Specialised division of tasks
• Complex crypting
• Development of new malware families
Expansion of underground economy
Professional malware coding
Definition of targets and profit maximisation
More complex attack strategies
• Financially strong targets
• Possibility to intercept many data at a time
• Increasing quantity and quality
• Campaigns are adjusted to current social circumstances

With regard to the private sector, operators of public facilities and critical infrastructures, these developments show: cybercriminals will continue to commit attacks for which they will use a high number and variety of attack vectors with a view to introducing malware variants into target systems to intercept, encrypt or destroy data there.

The level of threats posed by cyberattacks increased strongly in 2019 and will continue to rise in 2020.

Calls to action and advice about appropriate risk awareness in cyberspace, however, are also directed at citizens: They must be vigilant about their data on the Internet and suspicious when receiving e-mails from unknown senders. They should also make regular backups, abstain from paying any ransom money and inform the police instead.

For companies, an IT security concept is indispensable and the staff should be made aware of the dangers possibly arising from cybercrime. An e-mail with an attachment containing ransomware, for instance, can have fatal consequences for the entire company.

Cybercrime permeates the whole of society - enterprises, public institutions and critical infrastructures but also citizens' private lives are displayed in digital space due to the ongoing spread of digital technology. This means that virtually everybody can become a target of cybercriminals - in view of the increasing level of threat arising from cybercrime it must therefore be considered as a challenge for the whole of society.

This is particularly demonstrated by the cybercriminals' adaptability: Political developments, social movements, public discussions are immediately exploited as a narrative for spam and phishing mails.

Perpetrators take up current social developments in a highly flexible manner - this must also apply to the necessary awareness-raising and protective measures.

The BKA and other security authorities issue warnings when a new threat has been identified. These serve to quickly inform companies and citizens about new risks and enable them to act accordingly.

However, protecting a company from an attack always starts with the staff: staff members must be made aware of the need to delete e-mails from dubious senders or to react with scepticism when receiving seemingly unusual e-mails from (alleged) partners before opening attachments.

Successful suppression of cybercrime depends on national and international co-operation. Cybercrime is a phenomenon that knows no national boundaries and attacks both private individuals and companies as well as society as a whole. This area of crime can only be tackled effectively through the pronounced and trusting cooperation between law enforcement/prosecution authorities, industry, science, judicial authorities and political bodies. Expanding this cooperation is the focal point of the special cybercrime units at the security authorities of the Federation and the Länder.

Cybersecurity and IT proficiency must be seen as standard in today's society.

Progressive developments, such as the IoT, industry 4.0 or the engineering of intelligent software, lead to a steady expansion of the range of potential targets of cybercriminals. As much as technical progress may change people's lives for the better, it always entails the possibility of criminal use, for instance as "learning malware".

IT-specific subjects, particularly in the context of cybersecurity, are occasionally discussed in the abstract in public debate. This keeps part of the population from dealing with such subjects in the first place. Broad attention for these subjects may, however, strengthen the population's resilience to cybercriminals and their methods. This prevents offenders from being successful from the outset.

When considering the information held by security authorities and private industry in full, it must be assumed that the increase in the risk posed by cybercrime identified in 2019 will continue in 2020.

8 Appendix

8.1 KEY INFORMATION - COMPACT OVERVIEW

Theft of digital identities	• Merchandise of underground economy • Every stolen digital identity is a breeding ground for further criminal activities
Malware	• Emotet remains the biggest malware threat - particularly in combination with TrickBot and Ryuk • Number of malware families is steadily increasing • Professional crypting making malware invisible for AV scanners
Ransomware	• The primary, existential threat for companies • Systems are no longer only encrypted - perpetrators threaten to publish the encrypted data
DDoS	• Both quantity and quality are increasing • Increased use of IoT and clouds to reinforce DDoS attacks
Underground Economy	• Highly specialised industry with divided responsibilities • Based on nine pillars - each with its own area of specialisation • Each pillar ensures the smooth execution of criminal activities
Attacks on companies	• APT-like behaviour of criminal organisations • Damage caused by, for instance, a ransomware attack is at least in the 6-digit range

8.2 OFFENCES CLASSIFIED AS CYBERCRIME IN THE NARROWER SENSE

The relevant criminal offences attributed to cybercrime in the narrower sense are described below.

Computer fraud as cybercrime in the narrower sense (section 263a of the German Penal Code). Since 01/01/2016, the PCS has divided this offence into the following types of fraud:

- fraudulent obtaining of motor vehicles pursuant to section 263a of the German Penal Code,
- other types of credit fraud pursuant to section 263a of the German Penal Code,
- fraud using unlawfully obtained payment card data pursuant to section 263a of the German Penal Code,
- fraud using unlawfully obtained other non-cash means of payment pursuant to section 263a of the German Penal Code,
- obtaining services by deception pursuant to section 263a of the German Penal Code,
- accounting fraud in the healthcare sector pursuant to section 263a of the German Penal Code,
- transfer fraud pursuant to section 263a of the German Penal Code.

Other forms of computer fraud (pursuant to section 263a subsections 1 and 2 of the German Penal Code and preparatory acts pursuant to section 263a subsection 3 of the German Penal Code, unless included in the following types of fraud or the "misuse of telecommunications services").

Data espionage and interception of data including preparatory acts and handling stolen data (sections 202a, 202b, 202c, 202 d of the German Penal Code) comprises the theft and handling of stolen digital identities, credit card, e-commerce or account data (e.g. phishing). The stolen data are usually offered for sale as merchandise on digital black markets and misused by offenders. Therefore, exploitation is a two-phase process: the sale of the data and the fraudulent use of purchased data. Significant profits are generated at both levels.

Handling stolen data (sections 202a, 202b, 202c, 202 d of the German Penal Code) comprises the theft and handling of stolen digital identities, credit card, e-commerce or account data (e.g. phishing). The stolen data are usually offered for sale as merchandise on digital black markets and misused by offenders. Therefore, exploitation is a two-phase process: the sale of the data and the fraudulent use of purchased data. Significant profits are generated at both levels.

Forgery of evidentiary data and/or deception in legal relations (sections 269, 270 of the German Penal Code) - these offences include the deception (of a person) by forgery of data. Data are forged and/or altered by their holder and used for deception in legal relations. This is done, for instance, by sending e-mails under the pretence of real identities or companies. A cover identity is used to persuade victims, for instance, to disclose their account details or credit card data or to make payments. It also includes the sending of malicious software camouflaged as invoices in e-mail attachments.

Data manipulation/computer sabotage (sections 303a, 303b of the German Penal Code) - this is a form of digital criminal damage. The punishable offence consists of the alteration of data in a data processing system and/or the alteration of the system by other persons than the data owner. Sections 303a, 303b of the German Penal Code typically include Denial of Service attacks (DoS/DDoS attacks) as well as the distribution and use of various kinds of malware (Trojans, viruses, worms, etc.).

Misuse of telecommunications services (section 263a of the German Penal Code) - this is a special and separately recorded form of computer fraud. Offenders exploit vulnerabilities or weak access security features of companies and private homes, e.g. to access routers without authorisation, call expensive international telephone numbers or systematically use premium or value added services.

8.3 HOW CITIZENS CAN PROTECT THEMSELVES

Be sceptical about e-mails from unknown senders!

Always keep your security programmes and other software up to date!

Choose complex passwords - "Password1234" is not a secure password!

Only trust official websites and app stores!

Make regular backups of your system!

8.4 HOW COMPANIES CAN PROTECT THEMSELVES

Develop an appropriate IT security concept for your company.

- Draw up procedures and instructions specifying how your staff should react in the event of a cyberattack.
- Regularly update your security concept.
- Train your staff about cybersecurity.
- Create backups of your system (which are not connected to the system).

How you can help

- Be reluctant to pass on confidential and personal information.
- Have a healthy distrust if you come across anything unusual.
- Check e-mails for correct senders' addresses.
- Do not open suspicious e-mails.
- Be suspicious when receiving links or attachments in e-mails from unknown senders.

Measures to be taken after an infection with ransomware

- Immediately disconnect the infected computers from the network and turn off affected devices.
- Isolate backups to prevent them from being encrypted as well.
- Save relevant files which could shed light on the infection process. These include, for instance, log files or e-mails.
- Change all user and network passwords if these may have been compromised by the incident.
- File a criminal complaint with the Central Point of Contact for Cybercrime without delay.

Inform the police!

- In any case, file a criminal complaint.
- Obtain information via the Central Points of Contact for Cybercrime: https://www.polizei.de/Polizei/DE/Einrichtungen/ZAC/zac_node.html
- We urge you to immediately file a criminal complaint for any kind of cyberattack - successful cybercriminals will repeat their attacks!

Editorial information

Published by
Bundeskriminalamt, 65173 Wiesbaden

Last updated
September 2020

Designed by
Bundeskriminalamt, 65173 Wiesbaden

Picture credits
Bundeskriminalamt

Please visit our website if you wish to download further publications of the Bundeskriminalamt:
www.bka.de/Lagebilder

This report is published by the Bundeskriminalamt as part of its public relations work.
It is made available free of charge and is not destined for sale.