ANSSI/BSI
Common situational picture

Vol. 1 – July 2018

Bundesamt
für Sicherheit in der
Informationstechnik

1 Forewords

BSI is a long-standing key strategic partner for ANSSI thanks to a high level of confidence built along years of regular exchanges, and its highest level of expertise.

Nevertheless, although this allows for highly valuable exchanges regarding important technical challenges, such as certification, operational cooperation and technical guidelines elaboration, the emergence and diversification of threats in the cyberspace call out for a continuous deepening of this partnership.

The sole improvement of national cyber security capacities, in France as in Germany, is indeed not sufficient to counterbalance the threat level we face, which, from this point of view, requires to merge even more our efforts.

I would like to stress the years of fruitful cooperation and great potential both countries have in this field. This first joint report materializes the intensification of the German-French partnership which will be expanded as a driver of cyber security policy within the European area.

55 years after the Elysee-Treaty, the renewal of the treaty in 2018 will strengthen French and German friendship and cooperation in Europe in all fields of politics, economics and society.

The cooperation of ANSSI and BSI represents an important pillar of practical, trustworthy and powerful French-German relationship. Our cooperation comprises all relevant fields for a secure digital future including cyber-security, cryptography, security-research, certification and standardization.

This paper is a result of the common work on appropriate analyses of the long-term risks in IT-security. The analysis is fundamental for the assessment and further decisions of strategies facing growing challenges, which occur consequently in a more digitalized world.

Furthermore, this paper expresses the high appreciation of the joint work between ANSSI and BSI, which opens up new perspectives and which represents an enrichment for both sides.

At this point, I would like to underline my gratitude for the mutual contributions based on respect and kindness.

2 General threat situation

Both France and Germany are facing growing challenges, which occur consequently in a more digitalized, connected world. Technical progress enables new facilities with all advantages and disadvantages.

High performance and secure information technologies are essentials to economic progress and open new opportunities to the 21th century's society. Technologies are conditioning the developments in the fields of communication, trading and transport. The working environment faces questions of industry 4.0, which also concerns the establishment of secure digital critical infrastructures.

Progress enables certainly new possibilities for crime, sabotage and espionage too. Since at least the rising of the ransomware threat in 2016, the overall threat situation remains on a distressing level, elsewise even raised in scale and mode of diffusion in 2017. In the national context, ANSSI and BSI reacted reasonably to incidents ensuring the IT-security of the national critical infrastructures. They developed operational and strategic responses tailored to those threatened or affected by attacks.

While some of the events observed are associated with an unprecedented growth in number, intensity or with the use of new operating methods, others cry out by their resonance in the global political, economic and strategic spheres. Attempts to destabilize democratic processes and economic order fall into the latter category and in some cases, only few resources are necessary for the resonance. The early and continuous collection of reliable information about happened or current incidents allows the assessment of the actual threat situation. The following analysis and qualified evaluation contributes to adequate reactions and the development of advisories for the user's countermeasures. The panorama of the cyber threats highlights three major phenomena in 2017.

1.1 Crime: Proliferation of sophisticated attack tools

The publication of sophisticated attack tools facilitates their proliferation, sometimes leading to real campaigns of attacks, whose consequences can be disastrous. Indeed, these tools can infinitely be copied and modified. Tools, which are disclosed on the internet, are thus recovered by other groups with criminal intent and join the ranks of their informatics arsenal. An increasing offering of attack tools was monitored. The most probable way of infection are malicious mails, that contain an attached macro-Word-file, js-file or link to their download. Thus, at least 86% of the mail traffic is

unrequested and potentially malicious. These mails are spread by huge botnets, such as Necurs and Mirai. The diversity of tools, operating modes and actors makes it more difficult, seemingly impossible, to identify the epicenter of the attack.

1.2 Sabotage: Resurgence of destructive attacks

ANSSI has noted an upsurge of attacks with destructive effects, made for profit or sabotage purposes. Among them, the agency observes since 2014 a constant rise in attacks by ransomware, variable virulence. This type of malicious code sequesters data from infected computer equipment until the victim pays the ransom, usually with a cryptocurrency such as Bitcoin.

BSI confirms this raise of the ransomware threat. It is definitely possible, that the intent of sabotage underlies some ransomware attacks in 2017. This indicates the implemented lateral movement, which limits the impact of an attack to the connected clients. In practice, NotPetya infected a Ukrainian financial software and caused incidents concerning critical infrastructures in the Ukraine, such as electricity networks, airports and railroad systems.

1.3 Espionage: Compromising publishers or IT service providers

On a worldwide scale, ANSSI notes a proliferation of computer espionage operations. These operations, carried out by organized groups, consist of collecting confidential information on know-how, individuals, competitors, a specific business sector or governmental and non-governmental organizations. The aim of these offensive actions is to gain a strategic advantage without alerting the targeted entity by using tools and modus operandi adapted to the target information security level. In 2017, those operations have been especially conducted without directly targeting the company but its supply chain.

Though, not only the high number and intensity of attacks is alarming. Vulnerabilities, which exist by conception, hold for risks. The disclosure of Meltdown/Spectre was much recognized in the media. Thereby it was published, that processors of Intel, ARM and AMD enabled bypass channel attacks on storage, which includes the capability of important passwords. Another critical vulnerability, which became public in October 2017, questions the security of WLAN-traffic. KRACK is the abbreviation of Key Reinstallation AttaCK and concerns session keys, which are necessary for the conduct of WPA- and WPA2-protected WLANs. Consequently, confidential data packets can be decrypted and the confidentiality of data transferred during communication is lost.

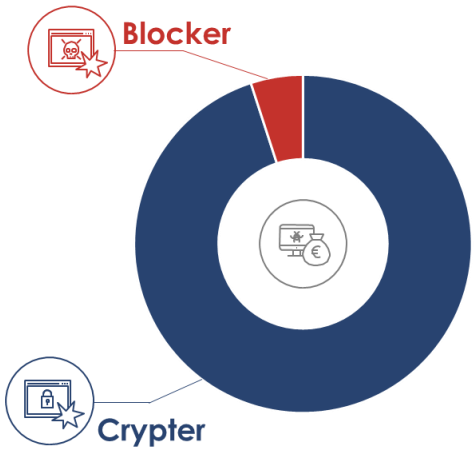
Thus, effective strategies for protection are necessary and several countermeasures ensure a solid ground for it.

- Strong patch-management: Regular and frequent updating process
- High awareness of malicious mails
- Regular and frequent back-up process, minimizing data losses, for instance by ransomware
    - Testing of the consistent and complete data handling, testing the back-up's running
    - Decryption tools for ransomware
- Actual antivirus-software and personal firewall settings
- User-account with limited rights for internet access
- Unique, strong and regularly changed passwords
- In case of the detection of an infection: Immediate adequate reaction, e.g. suppressing the connection to further devices to limit the impact and contacting the responsible authorities.

3 Ransomware

Definition: Ransomware is a malicious software, which limits or disenables the accessibility of data and demands for a ransom for recovery. Ransomware attacks are a form of digital extortion.

3.1 Categories



Two categories of ransomware can be distinguished. First: Ransomware, that blocks the access to a system, infects the operational system and is loaded after restart. It overlays the desktop with a picture or a website and demands for the payment. In 2015, a trojan was widely spread, which abused the name of security authorities and pretended an official claim for a fine. In the course of 2016, blocking ransomware barely appeared.

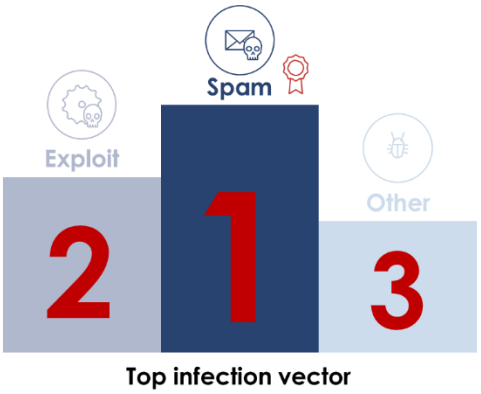
Second: 95% of known ransomware attacks were encrypting tools in 2016, using a combination of symmetric and asymmetric encryption like AES and RSA/ECC. The attacker puts in promise to provide a decryption tool in case of the victim's payment. The ransomware compares the data found on local devices, such as hard drives and USB-devices, as well as on network drives with a given list of data formats. This ensures that functions, which are necessary for the operational systems, keep running and the transaction of the ransom is possible.

.123 .3dm .3ds .3g2 .3gp .602 .7z .aes .arc .asc .asf .asm .asp .avi .bak .bat .bmp .brd .cgm .class .cmd .cpp .crt .cs .csr .csv .db .dbf .dch .dif .dip .djv .djvu .doc .docb .docm docx .dot .dotm .dotx .fla .flv .frm .gif .gpg .gz .hwp .ibd .jar .java .jpeg .jpg .js .key .lay .lay6 .ldf .m3u .m4u .max .mdb .mdf .mid .mkv .mml .mov .mp3 .mp4 .mpeg .mpg .ms11 .myd .myi .nef .odb .odg .odp .ods .odt .otg .otp .ots .ott .p12 .paq .pas .pdf .pem .php .pl .png .pot .potm .potx .ppam .pps .ppsm .ppsx .ppt .pptm .pptx .psd .qcow2 .rar .raw .rb .RTF .sch .sh .sldm .sldx .slk .sql .sqlite3 .Liedtitel .stc .std .sti .stw .svg .swf .sxc .sxd .sxi .sxm .sxw .tar .tar.bz2 .tbk .tgz .tif .tiff .txt .uop .uot .vb .vbs .vdi .vmdk .vmx .vob .wav .wb2 .wk1 .wks .wma .wmv .xlc .xlm .xls .xlsb .xlsm .xlsx .xlt .xltm .xltx .xlw .xml .zip

List of data formats, which are encrypted by the ransomware *Locky*

3.2 Attack Vector

- Spam: Mostly ransomware attacks are mass spam mail campaigns. The mail contains pretended bills, order confirmations, delivering mails, applications, scanned documents, fax mails or photos. These are social engineering techniques to enhance the click rate on the attachment. This is typically a Word document with macro execution, archive file, script file, program file or a combination that executes a PowerShell-script. Mostly the attachment has the function of a dropper, which reloads the actual ransomware.



Top infection vector

- Exploit Kits: An exploit kit uses different drive-by-exploits to find a vulnerability on a client's system, while the user is redirected.
- Other: Vulnerabilities of server software are abused to infect client using their services. In a few cases brute-force attacks targeted a special access to administration rights.

The following attack strategies enlarge the rate of the attacker's success:

- The height of the ransom is moderate, so a number of victims is able and willing to pay.
- Specification of a payment-deadline, up to that the recovery is possible. This can be pursued by the threat of raising the ransom, if it is not paid in time.

The victim can be threatened by deleting data the longer it takes for the payment.

3.3 Countermeasures

Recording the main attack vector for ransomware are spam mails, adequate protection against malicious mails will minimize the risk of a ransomware attack:

- Denial of the execution of script files, such as JavaScript, VisualBasic and PowerShell
- Changing the standard settings for the execution of script files to a text editor
- Denial of the execution of macros in Office documents
- Secure identification of the data format
- Raising the user's awareness of malicious mails

Regular and frequent patching of applications is one of the basic IT-security measures. So vulnerabilities can be closed, which are used by exploit kits for a ransomware infection. In special, web browser, plug-ins, e-mail software, pdf-application and Office programs are vulnerable and need to be patched. In general, the usage of

browser plug-ins should be limited as much as possible and a browser with sandbox technology is recommendable, just as well as actual antivirus software. In October 2017, Microsoft reacted to the raise of ransomware incidents by adding a controlled folder access to Windows 10 to prevent malicious alliteration of important files. Thus, protection measurements become more sophisticated.

The most important internal factor is the awareness of the threat of malicious mails and compromised websites. Checking the authenticity of the sender and the plausibility of the mail's subject should be a matter of course. Users should not obtain rights and permissions, which are not absolutely necessary for their duty, because this provides unnecessary risk in case of infection. The remote accesses to a system should be established via VPN and a 2 factor authentication. Testing the exposure of systems, which are externally accessible, is conducted by penetration testing.

Altogether, a regular and frequent back-up process minimizes the risk of data losses.

Nevertheless, if a ransomware infection was successful, the payment is not reasonable, since the recovery of data is not guaranteed and the payment conducts further development of attack tools. In case of a ransomware infection, a criminal complaint has to be made.

Not in every case, the encrypted data is lost. It is known that the main algorithms for encryption are RSA (key length 1024-4096 Bit), ECDH (key length 192 Bit), AES (key length 128-256 Bit), RC4 and Salsa20. Thus, numerous decryption tools are available open source. Some of them are provided by attackers with the intent of switching off competition in the field of ransomware.

Harasom	18.08.2013	https://decrypter.emsisoft.com/harasom
CryptoDefense	02.04.2014	https://decrypter.emsisoft.com/cryptodefense
TorLocker / Scraper	08.04.2015	https://securelist.com/blog/research/69481/a-flawed-ransomware-encryptor/
PCLock	29.04.2015	https://decrypter.emsisoft.com/pclock
TeslaCrypt 1.0 / AlphaCrypt	13.05.2015	http://www.bleepingcomputer.com/virus-removal/teslacrypt-alphacrypt-ransomware-information#decrypt
CoinVault / Bitcryptor	28.10.2015	https://noransom.kaspersky.com/
Linux Encoder	10.11.2015	https://labs.bitdefender.com/2015/11/linux-ransomware-debut-fails-on-predictable-encryption-key/
CryptInfinite	22.11.2015	https://decrypter.emsisoft.com/cryptinfinite
Rakhni	11.12.2015	http://support.kaspersky.com/de/viruses/disinfection/10556
Radamant	02.01.2016	https://decrypter.emsisoft.com/radamant
TeslaCrypt 2.0	20.01.2016	https://up2sha.re/GGTSPU-fw1.bsi.bund.de-32760-6546225-xMh9MxnlcLkeofgD-DAT/file?l=C5ag0MrQNqAb.pdf
KeyBTC	24.01.2016	https://decrypter.emsisoft.com/keybtc
LeChiffre	25.01.2016	https://decrypter.emsisoft.com/lechiffre
Gomasom	25.01.2016	https://decrypter.emsisoft.com/gomasom
CrypBoss	30.01.2016	https://decrypter.emsisoft.com/crypboss
DMALocker	06.02.2016	https://decrypter.emsisoft.com/dmalocker
HydraCrypt	12.02.2016	https://decrypter.emsisoft.com/hydracrypt
DMALocker2	18.02.2016	https://decrypter.emsisoft.com/dmalocker2
Nemucod	22.03.2016	https://decrypter.emsisoft.com/nemucod
Petya	09.04.2016	https://github.com/leo-stone/hack-petya/blob/master/README.md
Jigsaw/CryptoHitman	11.04.2016 11.05.2016	http://www.bleepingcomputer.com/news/security/jigsaw-ransomware-decrypted-will-delete-your-files-until-you-pay-the-ransom/ http://www.bleepingcomputer.com/news/security/jigsaw-ransomware-becomes-cryptohitman-with-porno-extension/
AutoLocky (nicht die in DE verbreitete Familie Locky)	16.04.2016	https://decrypter.emsisoft.com/autolocky

Example for available decryption tools in May 2016

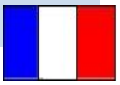
3.4 Development of ransomware incidents

An actual Sophos survey of 2.700 organizations points out, that 54% were hit by ransomware with a medium impact of 133 USD and 74 % of those hit were running updated antivirus software. Thus, ransomware is still a notable threat.

2015

February 2015 – CTB-Locker campaign

Identification of a campaign affecting French citizens, SMEs and local authorities. Techniques observed during this campaign is an email reproducing a fax reception with a ZIP archive joint which included a malware named CTB-Locker. This ransomware was among the most advanced one especially regarding crypto level and communication through Tor.



- Worldwide 150.000 WordPress websites point to CyptoWall-download.

February 2016 - Lukaskrankenhaus

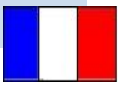
10.02. at 9 am: the IT-department of *Lukaskrankenhaus* in Neuss registers unusual alarm messages. The reason was a ransomware similar to TeslaCrypt 2.0, attached to a malicious mail and encrypting all data accessible in the internal network, including systems necessary for patient care. Nevertheless, the ransom was not paid, but a reloaded backup limited the data loss to 24 h. The actual impact was the new development of a secure IT-infrastructure as well as measurements to raise the awareness of the staff members.

2016

- Ransomware was the most frequent attack on companies' IT-infrastructure in spring. A BSI survey points out that 33% of all questioned companies were infected by ransomware, in 75% of this cases the attack vector was a malicious e-mail attachment. In 70% of the infections, just unique computers were affected, but in 22% relevant IT-infrastructure was omitted.
- Well-known ransomware families:
- Locky, TeslaCrypt, Nemucod, CTB-Locker, Petya, WannaCry, NotPetya, matsun, nymaim and Cerber
- Exploit-kits are offered open source and commercial: Angler, Neutrino, Magnitude …
- Spreading through botnets is rising. The former dridex-network, which distributed an online-banking trojan, is also used for spreading ransomware.
- SamSam is an extraordinary example for a targeted infection by using backdoors. The initial access was possible because of a flaw in the JBoss-application-server, in consequence the credentials for connected Windows systems were hooked. SamSam encrypted user files and deleted systematically Backup-files.

September 2016 – ANSSI recommendations for ransomware

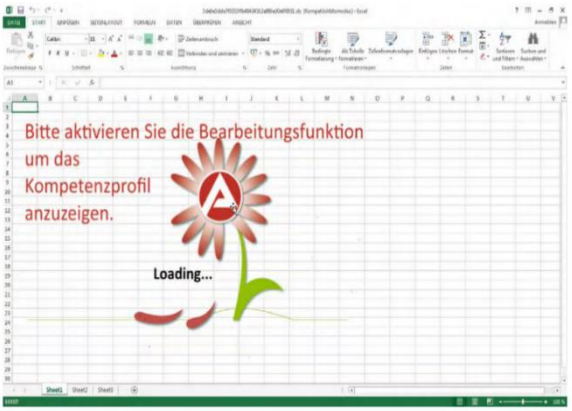
Facing the emergence of ransomware attacks, ANSSI released a list of best practices and reflexes to be adopted in case of emergency.



2017

December 2016 – application mail campaign

The malicious mails were sent to German recruiters and demanded for a macro execution of a tabular data file, the VBScript then started exe-files, encrypted data and denied a restart of the system. The malware was frequently modified to handicap the detection.



- Blocking ransomware occurs adapted for mobile phones and gains proliferation.
- Well-known ransom-families:
- Locky, Cerber, CryptXXX, Crysis, WannaCry, NotPetya, matsun, nymaim and Petya/GoldenEye
- Jaff was distributed via spam-mails of the Necurs-botnet. They had a Word document with macro attached. Already one month later a decryption tool was available.
- NotPetya/ExPetr first occurred in the Ukrainian financial software MEDoc. The provider's website was compromised and the automatic update process lead to the infection. It spied user credentials and used the known Microsoft Windows SMB-flaw to spread on a local platform.
- Bad Rabbit was a drive-by-ransomware mass attack, which had mostly Russian and Ukrainian victims.[9]
- Different offers for ransomware as a service (RaaS) are available, the prices mount from 35 USD.

May 2017 – Wannacry declaration of ANSSI Director

Several companies have been impacted, to some extent, sometimes at a minimal level, sometimes with a wide spreading of the malware. For major companies, there was a small number of cases, no numbers are available regarding the impact on SMEs and individuals.

The intervention of a British researcher helped to slow down the attack but the risk of an evolving of the malware was still present and other attack groups may have taken inspiration from the idea and acted on their own.

May/June 2017 – NotPetya and WannaCry

NotPetya affected the systems of a consumer goods group by a manipulated patch and spread via lateral movement causing a 4,5 days production stop in 17 factories and the shut-down of the whole telecommunication system. The head of management named the loss as low in proportion.

The WannaCry infection of mobility service company's system was strongly noticed. Display panels for departure and arrivals were overlaid by the red box of the ransomware demand. Monitoring cameras at train stations and some ticket vending machines were out of order, but train operations were still possible.

3.5 Further impacts

Until the media concentrated strongly on the WannaCry incident, a similar attack occurred, which was larger in scale and was actually predated. The cryptocurrency miner Adylkuzz was distributed in the same manner using the EternalBlue exploit und abusing the SMB-vulnerability on TCP port 445. Afterwards the backdoor DoublePulsar, which also had disclosed with the Shadow Broker leak, installed the mining software. Adylkuzz additionally shut down the SMB networking to prevent the systems from further attacks that could disturb the mining process, which might limited the spread of WannaCry. Thus, there was a strong connection between these incidents, but it might have been competition.

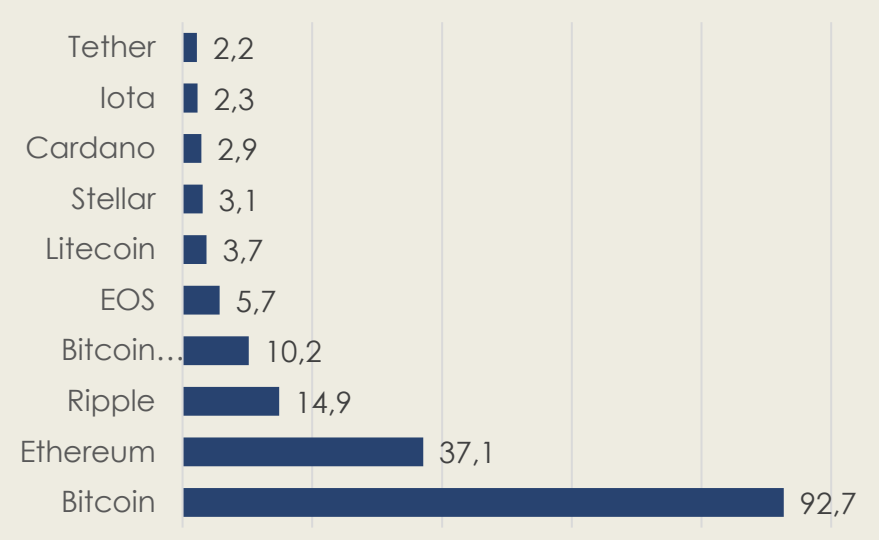
Another example for using the same distribution channels by cryptocurrency malware is the current campaign RedisWannaMine in March 2018. Already the name suggests the closeness to WannaCry. RedisWannaMine uses the EternalBlue exploit to abuse the Windows SMB-vulnerability and downloads subsequently the coinminer.

The Quant trojan was a former distributor of the ransomware Locky and malware of the Pony family, but was observed to be modified and to target cryptocurrency wallets. Quant was available for purchase on Russian underground forums for an amount of 275 USD. The malware scans the victim's application data directory of supported currencies like Bitcoin, Terracoin, Peercoin and Primecoin. Another function is the stealing of credentials for applications and the operating system.

There are multiple reports, which point out that men of action behind Lazarus and the ransomware VenusLocker changed their field of activity from ransomware to cryptocurrency crime and that they are no isolated cases.

This implicates the conclusion that ransomware steps aside for the threat of cryptocurrency crime. So, in the following section the backgrounds of this trending theme are explained.

4 Cryptocurrency Crime



The ten cryptocurrencies with the highest market capitalization (in billions euros)

Cryptocurrency Crime covers all actions with the intent of looting cryptocurrencies. This includes the thievery of cryptocurrency properties and illegal cryptomining, also known as cryptojacking, which is the use of a compromised machine to make it "mine" cryptocurrency and get the reward. Bitcoin is the first cryptocurrency, which was created in 2009. Nowadays, there are more than 1800 cryptocurrencies, but only a few of them (~30) have serious technologic and economic projects.

4.1 Blockchain and cryptocurrency

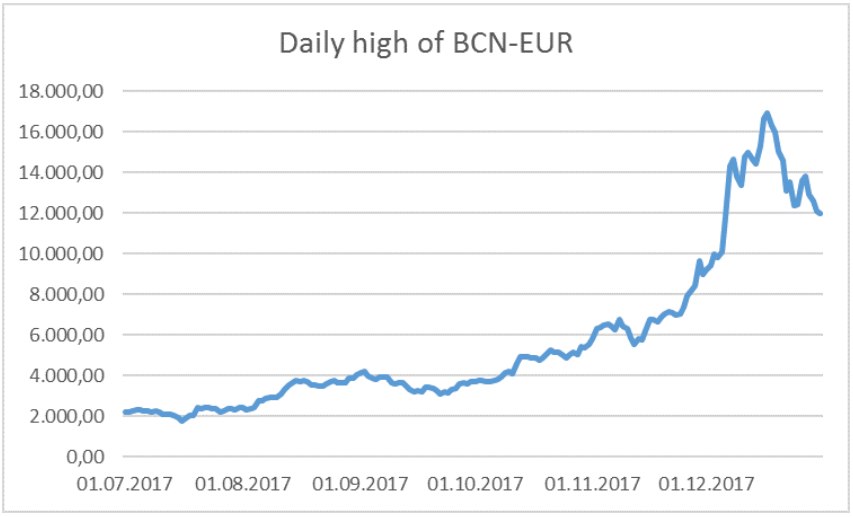
A cryptocurrency is a digital asset that uses cryptography to secure transactions, to control additional units and verify the transfers of assets. Cryptocurrencies work as a decentralized system in opposition to centralized electronic money or central banking. This system works through a blockchain, a decentralized database containing information, which are checked at regular time interval, grouped in "blocks". That Distributed Ledger Technology (DLT) does not divide users by different rights of reading, writing and saving. Each entry to the database has to pass a validation process and is added subsequently to each copy of each participant of the database.

4.2 Money creation process

For most cryptocurrencies, the blockchain process needs to validate every block by computing complex operations. Those operations require a decentralized computing power brought by users of the network. In order to encourage users to allocate a part of their computer calculation power, the cryptocurrency blockchain compensates participants by offering an amount of new created cryptocurrency. This recompense is proportional to the computer power allocated.

4.3 Cryptocurrency stock prices and cybercrime interest

Cryptocurrency crime was an upcoming theme in 2017 due to the enormous rise in stock prices of the highly volatile Bitcoin, which is the cryptocurrency with the highest market capitalization. From January 2017 to January 2018, Bitcoin value rose from 900 to 13 000 euros (+1440%). Other cryptocurrency rose tremendously as well (*Monero*, +2300%; *Ethereum*, +1980%; *Ripple*, +738%).



Development of the exchange rate for Bitcoin-Euro 01.07.-31.12.2017

4.4 What is cryptojacking, the cybercrime new trend?

Cryptocurrency crime is a new trend in cybercrime. Criminals focus on this news potential income for two reasons: The currencies' raising values and the relative anonymity of the stolen fund transfers.

Since cryptomining needs equipment with a high computing power and energy cost, cybercriminals now try to compromise those kinds of resources to get them mine for them. Attackers use different cryptojacking strategies:

- Botnet cryptojacking: Creating or using an existing botnet to mine cryptocurrency with a part of the computing power of each "zombie" machine.

Ex.: PyCryptoMiner botnet, identified by F5 Network Labs. The botnet exploits vulnerability CVE-2017-12149 and SSH protocol to spread

- Web cryptojacking: Web cryptojacking is a technic, which targets legitimate and popular websites. The attackers use a JavaScript insertion to include malicious tools

that force the visitors' Internet browser to mine cryptocurrencies.

Ex.: In January 2017, the Blackberry mobile website was compromised and contained Coinhive mining software making all visitors mine Monero cryptocurrency (XMR).

- Direct cryptojacking: The attacker targets a specific victim, chosen for the high computing capacity of its equipment, often companies or academic facilities. Once the server / machines are compromised, the attacker installs cryptomining software and gets the mined coins.

Ex.: According to SANS Institute, Oracle servers from DIGITAL OCEAN, GODADDY, VERIZON BUSINESS SERVICE et ATHENIX companies have been concerned by this direct cryptojacking. The global operation may have paid about 190 000 euros to the attacker.

- Smartphone cryptojacking: Distribution of compromised mobile applications. However, the computing power of smartphones is usually lower than personal computer's.

4.5 Development of cryptomining incidents

Cryptojacking itself is not a new phenomenon. Numerous incidents have been monitored since 2011. The State of IT Security in Germany first mentioned mining in 2016, due to the fact that 15 % of botnet infrastructures were used for illegal cryptomining. Though in 2017, the number and extent of incidents emerged.

2017:

- Multiple types of mining malware use known Windows OS vulnerabilities to infect unpatched systems, amongst others the mining malware Zealot uses the EternalBlue exploit, which is not the only case, whereas the former distribution channels for ransomware are conversed. Kaspersky Lab detected a mining malware, that gained cryptocurrencies in an amount of 5,5 Mio. Euro within six months.
- The trojan Loapi infected more than 1 million mobile phones. The malware spread with downloads in unofficial App-stores and via advertisements for porn and antivirus software. Loapi is the first cryptotrojan, that causes a physical damage of the system and is an example for enlarging the threat of cryptomining to mobile phones.
- In December, the new attack vector via social media was observed. The crypto malware Digmine infiltrates the registry of Windows clients and adds a browser extension to Chrome. It spies for credentials of automatic facebook log-ins and sends the malware to the victim's facebook friends

2018:

- Attacker compromised an unpatched Oracle server in order to mine 190.000 EUR worth of Monero.
- RubyMiner seeks to compromise web servers vulnerable to several known vulnerabilities in order to mine Monero. This attack campaign would have allowed the compromising of 700 servers in the United States, Germany, United Kingdom,

Norway and Sweden.

- The Monero-miner JenkinsMiner used vulnerability in Jenkins server and earned nearly 2,5M Euro worth of Monero.

4.6 Development of cryptocurrency thievery incidents

Let the incidents in 2017 with the highest damages be exemplarily illustrated.

- In the time of 18.-20.07.2017, cryptocurrencies in an amount of 85 Mio. Euro were stolen. The attacker targeted conventional banks and trading platforms for cryptocurrencies. Thereby two strategies can be distinguished: Replacement of legitimate wallet addresses, which were published on web sites, and exploitation of wallet vulnerabilities for sending the complete amount to the attacker's address.
- On 07.12.2017, a vulnerability of the wallet software Nicehash was used to loot 50 Mio. Euro. On 19.11.2017, the same happened to the trading platform Tether. The damage was 25 Mio. Euro.
- After weeks of non-activity, the Satori-botnet started to deploy code dedicated to the theft of Ethereum. It overwrites the code of the Claymore mining software to change the public address of the legitimate miner in order to recover the profits.

4.7 Conclusions

The threat of cryptomining has emerged within the second term of 2017. A reason for this is the raise of financial attractiveness to gain cryptocurrencies. Furthermore, an installed miner guarantees regular income and is rather low-profile, because the CPU's computing capacity is not fully used. The main incidents of illegal cryptomining concentrate on Monero mining, which is less computational intensive than Bitcoin mining and which ensures the non-traceability of the network member's identities. Monero mining was observed to be adapted for mobile phones to an increasing degree and to be distributed via social media for the first time. All those advantages may bring the cybercriminals to operate more cryptojacking attack than ransomware attack with a cryptocurrency ransom.

Concerning the thievery of cryptocurrencies mainly Bitcoin and Ethereum are of interest respectively their high proliferation. The strategies are the compromise of web sites, exploitation of wallet vulnerabilities and espionage for wallet credentials.

References:

[1] „Cybercrime | Bundeslagebild 2016“ – Bundeskriminalamt; Wiesbaden 2016
[2] „Lagedossier Ransomware“ – Bundesamt für Sicherheit in der Informationstechnik; Bonn 2016
[3] https://threatpost.com/crooks-switch-from-ransomware-to-cryptocurrency-mining/129229/; Consulted at 23.03.2018
[4] “How to stay proteccted against ransomware” – Sophos Ltd.; February 2018
[5] „Die Lage der IT-Sicherheit in Deutschland 2015“ – Bundesamt für Sicherheit in der Informationstechnik; Bonn 2015
[6] https://www.heise.de/newsticker/meldung/Trojaner-im-OP-wie-ein-Krankenhaus-mit-den-Folgen-lebt-3617880.html; Consulted at 28.03.2018
[7] „Die Lage der IT-Sicherheit in Deutschland 2016“ – Bundesamt für Sicherheit in der Informationstechnik; Bonn 2016
[8] „Die Lage der IT-Sicherheit in Deutschland 2017“ – Bundesamt für Sicherheit in der Informationstechnik; Bonn 2017
[9] https://securelist.com/bad-rabbit-ransomware/82851/; Consulted at 23.03.2018
[10] https://www.cnbc.com/2017/05/17/wannacry-cyberattack-worldwide-sophos.html; Consulted at 22.03.2017
[11] […]; Consulted at 28.03.2018
[12] https://www.proofpoint.com/us/threat-insight/post/adylkuzz-cryptocurrency-mining-malware-spreading-for-weeks-via-eternalblue-doublepulsar; Consulted at 23.03.2018
[13] http://securityaffairs.co/wordpress/70117/malware/cryptocurrency-mining-operations.html; Consulted at 23.03.2018
[14] http://www.zdnet.com/article/quant-trojan-upgrade-targets-cryptocurrency-user-wallets/#ftag=RSSbaffb68; Consulted at 23.03.2018
[15] https://www.zdnet.de/88321291/lazarus-gruppe-angeblich-fuer-bitcoin-stehlenden-trojaner-verantwortlich/?utm_source=rss&utm_medium=rss&utm_campaign=rss; Consulted at 23.03.2018
[16] https://threatpost.com/crooks-switch-from-ransomware-to-cryptocurrency-mining/129229/; Consulted at 23.03.2018
[17] https://securelist.com/mining-is-the-new-black/84232/; Consulted at 23.03.2018
[18] Source of data: SIX Financial Information via https://www.finanzen.net, Consulted at 10.07.2018
[19] „Distributed-Ledger-Technologien im Zahlungsverkehr und in der Wertpapierabwicklung: Potenziale und Risiken“ - Deutsche Bundesbank, Monatsbericht September 2017, S. 36-38
[20] https://securelist.com/mining-is-the-new-black/84232/ ; Consulted at 08.03.2018
[21] https://www.bleepingcomputer.com/news/security/android-malware-will-destroy-your-phone-no-ifs-and-buts-about-it/ ; Consulted at 07.03.2018
[22] http://www.silicon.co.uk/workspace/malware-spreads-cryptocurrency-miner-facebook-messenger-226463 ; Consulted at 16.03.2018
[23] https://www.heise.de/security/meldung/Angreifer-attackieren-ungepatchte-Server-Apps-von-Oracle-3938626.html; Consulted at 10/04/2018
[24] https://research.checkpoint.com/rubyminer-cryptominer-affects-30-ww-networks/; Consulted at 10/04/2018
[25] http://newsroom.trendmicro.com/blog/security-intelligence/cryptocurrency-mining-malware-2018s-new-menace; Consulted at 08.03.2018
[26] https://www.darkreading.com/vulnerabilities---threats/uptick-in-malware-targets-the-banking-community/a/d-id/1329541 ; Consulted at 08.03.2018

[27]https://www.theregister.co.uk/2017/12/06/nicehash_diced_up_by_hackers_thousands_of_bitcoin_pilfered/ ; Consulted at 08.03.2018
[28] https://thehackernews.com/2017/11/tether-bitcoin-hacked.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Security+Blog%29 ; Consulted at 08.03.2018
[29] https://www.helpnetsecurity.com/2018/01/17/satori-eth-mining-malware/; Consulted at 10/04/2018