INFINITY

IMMERSE. INTERACT. INVESTIGATE.

Policy Brief

Cybercrime: threats and developments (June 2020 – May 2021)

DISSEMINATION LEVEL PUBLIC

PARTNER

EUROPOL

AUTHORS

EUROPOL

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No. 883293. The content of this document represents the view of the authors only and is their sole responsibility. The European Commission does not accept any responsibilty for any use that may be made of the information it contains.

The state of cybercrime in Europe[1]

The new reality brought forth by the global pandemic requires rapid adaptation and it is likely that the pace and organisation of personal and professional life has been permanently transformed. Inevitably, these developments have also spurred innovation among cybercriminals as they have strived to capitalise on new opportunities.

Ransomware groups, which continue to be a key threat, have been increasingly taking advantage of widespread teleworking by scanning potential targets' networks for insecure remote desktop protocol (RDP) connections and keeping a keen eye on disclosed virtual private network (VPN) vulnerabilities. Mobile malware operators have leveraged the increase in online shopping by using delivery services as phishing lures to trick their victims into downloading their malicious code, stealing their credentials or perpetrating different forms of delivery fraud. Mobile banking trojans have become a specifically noteworthy threat due to the increased popularity of mobile banking. Criminals have continued utilising COVID-19 narratives for the online sale of counterfeit medical products and vishing (phishing via telephone) to steal login credentials. There are also reports that distributed denial of service (DDoS) attacks for ransom might be making a comeback due to an increased reliance on online services. During lockdowns, children spend an even larger part of their day online, which has led to a steep increase in online grooming. Minors are now more likely to self-produce and share explicit material for online reputation or monetary gain or due to coercion.

In addition to being successfully opportunistic, threat actors have continued to mature in their methods and organisation. Cybercriminals continue to move towards a more calculated target selection and there is a rise in ransomware affiliate programs seeking cooperation with hackers and other malware developers. Ransomware operations are becoming increasingly focused on high-value attacks on large organisations and their supply chains while social engineers are shifting their attention towards upperlevel management.

Perpetrators continue to be increasingly ruthless and methodical in their modi operandi. Last year Europol wrote about the rise of ransomware crews deploying double-extortion methods by exfiltrating victims' data and threatening to publish it. In the past 12 months, the arsenal of coercion methods has expanded with cold-calling journalists, victims' clients, business partners and employees. In addition, many of the most notorious ransomware affiliate programs deploy DDoS attacks against their victims to pressure them into complying with the ransom demand.

These modi operandi are becoming more popular with criminals conducting investment fraud as well, which European law enforcement reported as one of the key threats. Those organising these schemes are setting up local call centres to increase their credibility with different language-speaking victims, as well as retargeting their 'customers'. Once a person has realised that their investments have been stolen, fraudsters contact them again under the pretext of representing law firms or law enforcement agencies, offering to help retrieve their funds.

In light of these developments, the market for criminal goods and services is booming. Personal information and credentials are in high demand as they are instrumental in improving the success rate of all types of social engineering attacks. Unfortunately, the market in personal

information flourishes as ransomware and mobile information stealers produce an abundance of marketable material as a by-product of the primary attack. It is also not a coincidence that Malware-as-a-Service (MaaS) offerings have increased, with ransomware affiliate programs leading the charge.

Although Bitcoin currently remains the go-to cryptocurrency of choice for Dark Web users and vendors, Monero and other privacy coins are rising in popularity. Criminals are increasingly converting their illicit earnings made in Bitcoin using cryptocurrency obfuscation methods like swapping services, mixers and coinjoins. Child sexual abuse material (CSAM) is actively traded on peer-to-peer (P2P) networks and the Dark Web, where cryptocurrencies are also used for payments, with law enforcement reporting an increase in for-profit distribution.

With all these opportunities, the administrators of online criminal markets have not remained idle. The increase in law enforcement activity in the past few years has incentivised them to enhance their operational security to protect their profits. They have established new mechanisms for protection against DDoS attacks from competitors and prefer hosting their services in countries where international judicial cooperation for law enforcement is more challenging.

Additionally, many platforms have stopped automating their Pretty Good Privacy (PGP) encryption to prevent the decryption of exchanged messages in case the authorities seize the market. Illegal markets have expanded to different encrypted communication channels due to increased legal action taken by law enforcement. These include channels like Telegram and Wickr.

It is apparent that digitisation affects all forms of criminality. Methods and tools used by cybercriminals are increasingly adopted in other crime areas and the digital criminal ecosystem continues to evolve at an alarming pace. The privacy and convenience offered by communication, distribution and cryptocurrency platforms are beneficial in all illegal activity. Online anonymity is exacerbated by the wide-scale adoption of encryption technologies, which can benefit lawful users and criminals simultaneously, creating a paradoxical situation for policymakers. In addition to legitimate services, international law enforcement is keeping a keen eye on VPN and crypto phone providers that cater to the criminal elements of our society.

To combat the aforementioned advancing threats, law enforcement officers need to be able to have timely access to data and to conduct lawful undercover work to keep society safe. Companies, especially those operating outside the European Union, have to improve their Know Your Customer (KYC) and information disclosure practices. Law enforcement agencies need more training and tools to have officers capable of uncovering and disrupting criminal activity in the digital realm. Finally, it is vital to continue improving our collective information technology (IT) literacy and awareness as cybercrime has become entrenched in our society.

1. Cross-cutting crimes and challenges

The continued increase of cyber- and computer-related crime is to a large degree enabled through the evolution and maturation of the criminal markets that provide all the necessary tools, goods and services to novice and established criminals. Network intrusions and social engineering are components of a multitude of attack vectors.

Criminals are increasing their operational security by hiding their online activity, using more secure communication channels and obfuscating the movement of illicit funds. The universality of these practices creates monetary incentives for the expansion of both the crime-as-a-service business model and grey infrastructure.

1.1 Crime-as-a-service continues to proliferate

The **crime-as-a-service** (CaaS) model remains a prominent feature of the cybercriminal underground and is a cross-cutting factor throughout the cybercrime sub-areas. The availability of exploit kits and other services (as discussed later in this document) not only serves criminals with low technical skills, but also makes the operations of mature and organised threat actors more efficient.

In the past 12 months, European law enforcement agencies have reported an increase in **Malware-as-a-Service** (MaaS) offerings on the Dark Web, of which ransomware affiliate

programs seem to be the most prominent. In these programs, the operators share profits with partners who can breach a target network and either harvest all the information required to launch an attack or deploy the malware themselves.

Related to the activities of ransomware and mobile malware operators, **access-as-a-service** (AaaS) is also in high demand as it is an enabler for both advanced malware crews and low-level criminals renting the tools to access targeted networks.

The by-product of the rise of multi-layered extortion schemes and wide-scale mobile information theft campaigns is an influx of **personal information** to illegal markets. This type of data can drastically improve the success rate of **social engineering** deployed in any form of attack. As it stands, social engineering remains an important vector for acquiring access to an information system or, in cases of fraud, the victim's bank account.

1.2 Expansive use of grey infrastructure enhances criminals' operational security

Various services, tools and technologies continue to help facilitate cybercrime. Some of these are legitimate services that are widely used, but are inadvertently useful for achieving the goals of cybercriminals: **secure communication, anonymity, obfuscation** and **laundering of criminal proceeds**, and more. Other services can be classified as operating in a 'grey' area. Such services are often located in countries with very strong privacy laws or a history of not cooperating with the international law enforcement community. **Grey infrastructure** services include bulletproof hosters, rogue cryptocurrency exchanges, and VPNs that provide safe havens for criminals.

The most well-known feature of legitimate services that are abused by cybercriminals is strong end-to-end encryption. **Messaging application** providers are unable to disclose the contents of the messages exchanged on their service even when subpoenaed.

Other legitimate tools and techniques that are abused by cybercriminals include **cryptocurrencies** and **VPNs**. Some of these services are a part of the grey infrastructure that allows cybercriminals to thrive: they abuse jurisdictions with lagging legislation for hosting, do not store user data in a sufficient manner, and/or do not comply with lawful requests. Although not all users of such services are necessarily criminals, the level of criminality associated with such services is often so high that national law enforcement agencies, after finding enough evidence of criminal abuse, could consider them to be criminal enterprises.

2. Cyber-dependent crime

A number of developments pertaining to the dominant threats within the cyber-dependent crime threat landscape have emerged:

2.1 Ransomware continues to dominate and proliferate

The use of traditional mass-distributed ransomware seems to be in decline and perpetrators are moving towards **human-operated ransomware** targeted at private companies, the **healthcare** and **education** sectors, **critical infrastructure** and **governmental institutions**. The shift in the attack paradigm indicates that ransomware operators choose their targets based on their financial capability to comply with higher ransom demands and their need to be able to resume their operations as quickly as possible.

This seems to indicate that spending more time on large corporations and public institutions is an effective approach for cybercriminals in terms of the return on investment. However, threat actors have started to consider law enforcement attention drawn to their operation to be an important criterion in their internal **cost-benefit analysis** and some ransomware affiliate programs have started changing their policies to restrict their partners from attacking certain targets.

Since the beginning of the pandemic, cybercriminals have been taking advantage of the fact that most companies have had to at least partially resort to **teleworking**, which meant that IT security policies have become more relaxed and the overall number of vulnerabilities and attack surfaces have increased.

Criminals have realised how much potential there is to compromise **digital supply chains** – organisations need to grant network access to update distributors, which makes these third-party service providers an ideal target. Furthermore, IT-infrastructures are extremely intertwined, so a successful intrusion does not only put one company's clients at risk, but potentially also opens doors to compromise other service providers, giving the attack even greater scalability.

Additionally, threat actors have started utilising **fileless malware** (using a system's native tools to execute a cyberattack) more extensively to avoid common detection methods that scan for malicious file attachments or the creation of new files.

European law enforcement agencies and Europol have identified several **new extortion methods** that cybercriminals use to pressure their victims.

Ransomware crews have started using Voice over Internet Protocol (VoIP) services to call journalists, the organisation's clients and business partners for further coercion. In some cases, ransomware operators also threaten their victims with DDoS attacks and the publication of their employees' personal information if they do not comply with the ransom demand.

Private partners have reported a sharp rise in the number of ransom payments made (over 300% increase)[2] between 2019 and 2020, with known transactions totalling over $400 million. Additionally, the average paid ransom amount increased from $115,123 in 2019 to $312,493 in 2020 (over 170% increase).[3]

Over the past year, a rise was identified in **ransomware affiliate programs**, whether sold publicly to a wide range of potential users or offered privately to a smaller group of hackers.

Public ransomware affiliate programs are not an entirely new phenomenon, as actors breaching a victim's system and then paying a RaaS operator to use their malware has been an observed dynamic in the cybercriminal ecosystem for quite some time. More cause for concern comes from the rise of **private affiliate programs** that are usually operated by better known ransomware groups. These threat actors are seeking out developers and hackers to improve the functionality of the malware or gain access to high-value targets' infrastructure.

2.2 Mobile malware becomes a reality

The number of **mobile malware** reports to law enforcement has increased significantly during the reporting period.

The Android banking trojan threat landscape now includes new tactics and techniques for stealing credentials, such as manipulating the banking apps on the user's device using the Automated Transfer System (ATS) modules powered by the Android Accessibility Service. Banking trojans like Cerberus and TeaBot are also capable of intercepting text messages containing one-time passcodes (OTPs) sent by financial institutions and two-factor authentication (2FA) applications such as Google Authenticator.

FluBot is currently one of the most prolific mobile banking trojans wreaking havoc in Europe and the United States. A key part of the malware's functionality is its ability to install display overlays for Google Play verification and various banking apps, which enables the theft of victims' credentials (banking, credit card and crypto wallet). It spreads through self-propagation by sending phishing text messages from the infected device to its contact list.

2.3 Monetarily incentivised DDoS attacks re-emerge

Law enforcement and private partners are reporting a re-emergence of DDoS attacks accompanied by ransom demands, as well an increase in high-volume attacks compared to the previous year. Cybercriminals have been targeting internet service providers (ISPs), financial institutions, and small and medium-sized businesses (SMBs).

Usually, a small-scale demonstration attack against the target entities' services precedes the ransom demand. The attackers have started to claim to be associated with well-known advanced persistent threat groups (APTs) like Fancy Bear and Lazarus in order to scare the victim into paying the ransom.

3. Child Sexual Abuse

The main trends and threats related to online child sexual exploitation have stayed relatively stable throughout the reporting period. While a series of factors have affected the evolution of these criminal activities, law enforcement did not detect significant changes.

3.1 The production and dissemination of child sexual abuse material remains a major concern

Law enforcement agencies and non-profit organisations engaged in child protection detect an overwhelming amount of material every year. In many cases, perpetrators produce Child Sexual Abuse Material (CSAM) in the victim's domestic environment, most often created by those in the child's circle of trust.

Children are accessing the internet unsupervised at a very young age and spend long hours online. This exposes them to substantial threats. Additionally, the increasing normalisation of sexual behaviour online is changing young people's attitude towards sharing explicit content with each other.

3.2 The production of self-generated material is a key threat

During the reporting period, law enforcement agencies reported a surge in the detection of self-generated material exchanged on social media, also displaying children of a younger age. Law enforcement agencies report a rise in online grooming cases over the last year, especially on social media and gaming platforms.

The production of self-generated material is in many cases a consequence of sextortion. Minors also produce material both for financial gain and to boost their online status on particular platforms, seeking likes and other indicators of approval.

In some cases, abusers persuade victims to have meetings in real life, transforming the online abuse into a physical one that can also last over time through coercion or extortion.

3.3 Cases involving live distant child abuse (LDCA) continue to increase

Travel and contact restrictions prompted by the COVID-19 pandemic have likely influenced the threat of LDCA, making it a viable alternative for those who would normally be transnational child sex offenders. This way of producing new material is often referred to as 'capping', which comes from the phrase to capture victims' material.

3.4 Peer-to-peer (P2P) file sharing networks remain important channels for the distribution of CSAM

CSAM is usually stored online or locally on password-protected drives. Offenders often make use of end-to-end encrypted communication channels, social media platforms and image boards to share illicit content. Private groups dedicated to the exchange of CSAM continue to proliferate on messaging applications.

Peer-to-peer (P2P) file sharing networks remain an important channel for sharing CSAM directly with other users or within small groups. Some countries have reported a considerable overall increase in the use of P2P distribution networks.

3.5 The Dark Web persists as an important platform for the exchange of CSAM

Despite successful law enforcement actions in taking down platforms focused on child sexual abuse, groups facilitating the exchange of CSAM on the Dark Web keep proliferating and are a persistent threat.

Offenders often share illicit content in these groups through direct links to image hosts in the Clearnet and Dark Web where the CSAM is stored. They also make use of cyberlocker sites where users pay content providers for each sign-up and subsequent download of their content.

Forums are well-structured and users are hierarchically organised depending on their roles. Users take up roles depending on their contribution to the community and can be administrators, moderators or users. In some cases, users take up the role of moderator on several platforms, facilitating distribution of CSAM with wider audiences.

The use of these specialised platforms opens a forum of exchange for like-minded people where offenders can share experiences, methods to commit abuse, and successful countermeasures to evade or hinder detection.

These networks are well structured, controlled and quite cohesive. New users have to gain the trust of the community in order to be accepted in the group, for example by contributing newly created or posted CSAM. The online absence of one of the members can be a worrisome development, which will be flagged within the community. Affiliation rules normally include active participation in the community and inactivity may lead to loss of membership. In some cases, communities are not limited to the online dimension, with high-ranked group members also meeting in real life.

3.6 CSAM for profit continues to be a growing threat

With the exception of LDCA, offences related to child sexual abuse are not usually motivated by financial gain. However, the monetisation of CSAM is a growing threat. The annual revenue of CSAM sites is estimated to have more than tripled between 2017 and 2020. Cryptocurrencies are the payment method of choice for these types of transactions.

In some cases, offenders pay minors directly for the exchange of self-generated content. Law enforcement agencies have observed increased number of minors using sites meant for sharing explicit adult content. Some of these platforms fail in preventing access by minors who register with fake identification and sell or appear in explicit videos.

4. Online fraud

Criminals continue making significant profits as well-known types of online fraud continue to be effective. While criminals have not had to re-invent their *modi operandi*, they continue to refine them, making them more targeted and technically advanced.

4.1 Online shopping in times of COVID-19 leads to delivery fraud

The COVID-19 pandemic has had a significant impact on the European fraud landscape. European law enforcement agencies have reported an overall increase in online fraud as criminals have exploited increased online activity.

Some of these crimes, such as phishing or the sale of counterfeit medical products, make use of COVID-19-

related lures, while others seek to exploit the side-effects of the pandemic. These include the relaxation of established security procedures due to employees working from home and a widespread shift to online shopping.

Delivery fraud has emerged as a new criminal focus in the second year of the pandemic. Criminals offer goods and receive payment without delivery, defraud online shops with weak security measures, or use delivery services as phishing lures. Posing as delivery services, criminals contact potential victims with links to phishing websites pretending to offer information about a parcel delivery, with the aim of obtaining user credentials and payment card details.

4.2 Criminals mix *modi operandi* as phishing and social engineering increase

Facilitated by the ongoing pandemic, the number of COVID-19- related phishing attempts conducted mainly via telephone (vishing) and text messages (smishing) has risen considerably.

Criminals have increasingly made use of compromised information from data breaches to improve their chances of success by creating highly targeted campaigns. Traditionally successful crimes such as **business email compromise, CEO fraud, extortion** and various types of scams, all profit from the availability of potential victims' personal data. As this data can be key in improving the success rate of criminal activities, this has led to a perpetual fraud cycle, in which the black market for compromised information is booming.

In line with other developments, fraudsters increasingly combine traditional social engineering attempts with technical components especially when targeting elderly victims. The increased use of remote access trojans (RATs) in vishing, for instance, exploits a lack of technical knowledge on the part of the target, potentially leading to full account access and significant financial harm.

4.3 Investment fraud, BEC and CEO fraud cause devastating losses

Investment fraud has emerged as the most dominant type of fraud in the last 12 months. Criminals have continued to target victims with fraudulent investment opportunities. With different assets on offer, cryptocurrencies emerged as the most popular, as the price surge earlier in 2021 attracted a number of new investors.

At the same time, criminals are further refining and improving this type of fraud. Authentic-looking advertising campaigns, the illicit use of celebrities, and even personal recommendations through online dating schemes all help bring unsuspecting victims to these fake platforms. In addition, criminals are becoming more professional, running local call centres to target different languages, creating more legitimate-looking websites, using remote access software to take over victims' accounts, and operating complex money mule networks.

This mixing up of different *modi operandi* is a key trend in investment fraud. Increasingly, criminals are hitting their victims twice: following the theft of the investments, criminals contact the victims pretending to be lawyers or law enforcement agents offering help to retrieve their funds. With the help of spoofing and detailed knowledge about the theft, they are often able to defraud their victims several times.

Investment fraud poses a significant challenge for law enforcement. The use of cryptocurrencies means that perpetrators can launder criminal proceeds quickly and efficiently, while uncooperative exchanges, or those with weak know-your-customer (KYC) measures, make them difficult to identify. At the same time, fake investment websites do not directly target legitimate financial institutions, but abuse their brands to target members of the public, leading to a decreased incentive for the industry to take action. Since many victims have incurred significant losses – in some cases entire life savings – investment fraud is a serious type of crime with potentially devastating consequences.

As investment fraud takes the spotlight, **business email compromise** (BEC) and CEO fraud have remained key threats in the past 12 months, with some countries reporting a further increase in the number of cases. Continuing to lead to significant losses, both types of crime have grown in sophistication and become more targeted. Heavily relying on social engineering,

attacks have increasingly focused on upper-level management, as well as on impersonating other staff members or changing invoice data in commercial transactions.

4.4 Card-not-present fraud under control as travel restrictions curb ATM attacks

Card-not-present (CNP) fraud appears to be largely under control. In countries that did see an increase in CNP cases, criminals often made use of the circumstances of the COVID-19 pandemic. Food delivery services, gaming platforms and other e-commerce platforms were targets of fraud or were exploited to steal card data.

As more and more transactions are taking place through online shops, there has been an increase in the use of online **skimming** for the purpose of stealing card data. While the modi operandi have not changed, criminals have added a number of new e-skimmers, particularly JS sniffers, to their arsenals.

Automated teller machine (ATM) logical attacks significantly decreased when hard lockdowns were imposed in many EU Member States. This development is mainly due to the COVID-19 restrictions preventing criminals from travelling. As logical attacks on ATMs faded, criminals with technical abilities moved towards other digital attack surfaces, such as mobile devices. The drop in ATM attacks was not a permanent trend, however. As soon as lockdowns and travel restrictions were relaxed, many EU Member States started reporting a significant increase in this type of crime.

5. Dark web

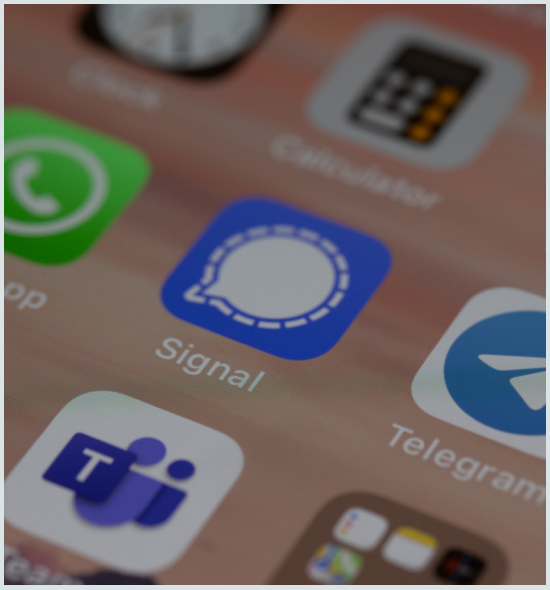
With regard to the Dark Web, EU law enforcement agencies have reported few major changes in the threat landscape. While the infrastructure of Dark Web marketplaces has not changed drastically, several smaller developments that had already been taking place for some years have now become more commonplace.

5.1 Criminals further strengthen operational security

EU law enforcement have cited the increasing **operational security** (OpSec) of vendors and marketplaces as a growing concern. Examples of increased sophistication of markets are the mechanisms that administrators have put in place to protect Dark Web platforms against DDoS attacks, and domain hosting in countries in which cooperation with EU Member States may be difficult. Administrators of platforms even cooperate in some cases by protecting their marketplaces against DDoS attacks and by making user guides on how to operate on the Dark Web. Furthermore, vendors may be increasingly aware of the **forensic techniques** used by law enforcement agencies to identify them, and try to protect themselves accordingly. The availability of **free penetration testing** services for vendors, to see how secure their operational security is, exemplifies this awareness.

Many markets have stopped automating PGP encryption on their platform because of previous law enforcement successes in intercepting and decrypting PGP messages in the back end of seized Dark Web marketplace servers. In this way, market administrators are trying to make users more aware of their encryption measures, which conversely could be a complicating factor for some non-technical users.

5.2 Similar goods and services, but more extortion and novel weapons



The types of goods and services for sale on the Dark Web have remained largely the same. However, the presence of ransomware groups on dedicated hidden services on the Dark Web offering their malware 'as-a-service' has increased.

Several countries reported that the exposure of data of individuals and companies had gained further traction as a business model for ransomware groups on the Dark Web. Governments have expressed similar warnings about such **advanced extortion** concerning ransomware groups that not only encrypted data, but also threatened to use DDoS attacks and leak stolen data if ransoms were not paid.

Weapons appear to be traded increasingly on encrypted chat applications, such as Telegram and Wickr, but sold slightly less on Dark Web marketplaces. Europol assisted in the arrest of an Italian national suspected of hiring a hitman on the Dark Web. Furthermore, several EU law enforcement agencies mentioned hitmen being ordered and weapons purchased on the Dark Web being seized. In the Netherlands a person was sentenced to 8 years' imprisonment for several attempts to order a contract killing via platforms on the Dark Web and encrypted chat applications. Furthermore, weapons were being sold on a Dark Web marketplace taken down in May 2021 by French authorities. In September 2020, an illegal workshop for printing three-dimensional weapons was dismantled in Spain, revealing a novel modus operandi. During one of the house searches in the joint operation by the Spanish Tax Agency and National Police, law enforcement agents encountered various 3D printers, one of which was in the process of printing a small firearm.

Furthermore, vendors have not stopped seizing the opportunity to abuse the uncertainty surrounding the pandemic by offering **fake vaccines** and masks for sale, consequently scamming buyers.

5.3 Fragmentation and displacement of Dark Web users

EU law enforcement identified the threat of **fragmentation** on the Dark Web, which is visible in various modi operandi. EU law enforcement reported a further increase in single vendor shops and smaller markets on Tor. Also, for example, the usage of encrypted communication platforms outside of Dark Web marketplaces for the sale of illicit goods and services has increased. For example, one country indicated that 70% of vendors that appeared to operate from the country of the respondent, listed on their Dark Web market profile a Wickr user name, while 20% listed Telegram contact info. This increasing usage of mainstream platforms with strong encryption, which are mostly used for legitimate purposes, poses a challenge for law enforcement agencies. It also shows the need for Dark Web investigators to broaden their focus on other platforms.

In some countries, takedowns of Dark Web marketplaces with a local or national focus may have led to this partial displacement to mobile applications.

5.4 More use of Monero and non-cooperative swapping services

Bitcoin has by far remained the go-to cryptocurrency of choice for users of the Dark Web. However, the criminal usage of privacy coin **Monero** on Dark Web marketplaces has further increased, becoming the most established privacy coin on the Dark Web. Zcash was also seen as a payment option, but its usage has not come close to Monero. While criminals still make most payments in Bitcoin, recipients are increasingly converting them to Monero and other

currencies by using **swapping services**. These services often operate on the Clearnet and in a grey area, utilising jurisdictions with lenient legislation and vague or non-existent KYC procedures. Some other services, such as Kilos, are operating on the Dark Web and even admit to 'skirting legal procedures'.

The use of swappers falls within a bigger trend of adopting more complex money laundering methods. In the last few years, many different obfuscation methods have gained popularity, such as mixers, CoinJoin, swapping, crypto debit cards, Bitcoin ATMs, local trade and more.

5.5 Grey facilitating infrastructure helps criminals thrive

The continuous thriving of cybercriminals can in part be attributed to the fact that grey infrastructure still facilitates them in many ways. This includes converting cryptocurrencies to exchanges with lacking KYC policies in place, bulletproof hosters that do not store useful client information, and the fact that grey infrastructure can operate (on paper) in countries where regulations are less stringent than in the EU.

6. Recommendations

6.1 Remove certain legal obstacles for investigators

Legislative limitations make it difficult for LEAs to enter closed groups with strong access controls and legal barriers around the retention and sharing of data persist. Investigations would benefit from longer data retention, but also from faster and higher quality data exchange with service providers. Clearer rules for registering IP addresses and domains could increase this data quality. The e-evidence directive may contribute to this.

Increased international cooperation in investigations may also shorten the waiting time in some cases, as international partners might be able to obtain information more quickly. Also, increased international cooperation, for example in blockchain analyses, could minimise cases where multiple authorities are chasing the same leads. Still, such cooperation is not always feasible and improved legal alignments are needed.

6.2 More officers, tools and training needed

More technically skilled officers and training are needed to adequately address cybercriminality. The development of cutting-edge technologies – ideally in cooperation with law enforcement – and a stronger focus on undercover activities will contribute to the goal of fighting cybercrime and enhancing victim identification. Data analysis tools, such as for cryptocurrency tracing and decryption, are of increasing importance in investigating many types of cybercrime, but are often expensive. Still, some free initiatives exist that may help investigations, such as the new decryption platform, which was inaugurated by Europol and the European Commission in December 2020.

6.3 A broader cooperative focus

In addition to individual targets and marketplaces, those who continuously facilitate cybercriminals and their infrastructures should not remain unpunished. Examples include bulletproof hosters, criminal VPNs, illicit cryptocurrency exchangers, and money laundering platforms. Coordinating activities internationally can contribute to effective and timely enforcement responses. However, improvements in collaboration and task division between departments in national agencies, such as economic crime and cybercrime, should not be overlooked.

6.4 Integrate law enforcement in the cybersecurity ecosystem

Law enforcement has an essential and complementary role to play in the response to cyberattacks. LEAs play a vital role in addressing the main gaps identified in the Network and Information Systems[4] (NIS) 2.0 Impact Assessment, specifically in the joint situational awareness and joint crisis response in the event of cyber incidents of a suspected malicious nature. One of the best ways to enhance the joint situational awareness and de-conflict the actions during a cyber-incident or crisis response would be to involve Europol's Europol's Cybercrime Center (EC3) as observer in the relevant NIS Cooperation Group[5] Work Streams, Computer Security Incident Response Teams (CSIRT) Network and the Cyber Crises Liaison Organisation Network (CyCLONe).

LEAs need a victim to report the incident in order to launch an investigation and provide support. Europol recommends that it be mandatory for major cyber incidents affecting critical sectors or essential service providers of a suspected criminal nature to be reported to LEAs and EC3, just as they have to be reported to the CSIRT when it comes to other root causes. Law enforcement agencies should be firmly embedded within the cybersecurity crisis management frameworks. The role of LEAs at national level within the national cybersecurity crisis management frameworks should be enhanced, and clear roles and responsibilities should be assigned to the competent authorities. If the LEAs and the LE response protocol were added to the international cyber incident response framework of the NIS2,[6] they would assist the NIS competent authorities and CSIRTs by sharing expertise in complex cross-border investigations.

6.5 Streamline information sharing and enhance awareness campaigns

After receiving a legal request by a law enforcement agency, companies based outside the EU may in some cases release limited amounts of information. Such information could be more helpful to law enforcement agencies if these companies had to operate according to similar rules as in the EU. Also, standard machine readable data would help investigators process data from such requests quicker.

Intensified public-private partnerships may contribute to the diminished success of cybercriminals. For example, expertise and information sharing with financial institutions can help to obtain data on cybercriminals and may help rapidly block their criminal proceeds. Law enforcement agencies should also explore new partnerships, such as with KYC providers, to enrich their intelligence in different areas, such as on money mules. Companies can also contribute to a decrease in fraud by increasing validation on the consumer side.

Awareness of potential victims of cybercrime should be raised at all ages, specifically in the field of child sexual exploitation where children, parents and caregivers should become aware of potentially risky online behaviours. Awareness campaigns on fraud with internet marketing, online investment and e-commerce fraud are also needed to help reduce fraud and prevent victimisation.

References

1 The information in this report has been provided by EUROPOL and is from EUROPOL's Internet Organised Crime Threat Assessment (IOCTA) 2021, see: Europol 2021, Internet Organised Crime Threat Assessment (IOCTA) 2021, Publications Office of the European Union, Luxembourg, at: https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2021#downloads.

2 Chainalysis (2021) Ransomware 2021: Critical Midyear Update. https://blog.chainalysis.com/reports/ransomware-update-may-2021

3 PaloAlto Networks (2021) Unit 42 Ransomware Threat Report. https://start.paloaltonetworks.com/unit-42-ransomware-threat-report.html. 2021

4 European Commission (2021) NIS Directive. https://digital-strategy.ec.europa.eu/en/policies/nis-directive

5 Europan Commission (2021) NIS Cooperation Group. https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group

6 European Commission (2020) Proposal for directive on measures for high common level of cybersecurity across the Union https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union

Image Credits

p. 2 - Image from torstensimon on Pixabay - https://pixabay.com/illustrations/eu-stars-privacy-shield-symbol-5837837/

p. 6 - Photo by cyndidyoder83 on Plxabay - https://pixabay.com/photos/teen-iphone-smartphone-girl-5224456/

p. 7 - Photo by Claudio Schwarz on Unsplash - https://unsplash.com/photos/q8kR_ie6WnI

p. 9 - Photo by TheDigitalWay on Pixabay - https://pixabay.com/photos/credit-card-bank-card-theft-1591492/

p. 10 - Photo by Dimitri Karastelev on Unsplash - https://unsplash.com/photos/EhNLOlxlOXI

p. 11 - Photo by Rūdolfs Klintsons from Pexels - https://www.pexels.com/photo/close-up-shot-of-gold-coins-7767495/