IOCTA

Internet organised crime threat assessment

2023

EUROPOL

Internet Organised Crime Threat Assessment (IOCTA) 2023

Luxembourg: Publications Office of the European Union, 2023

PDF ISBN: 978-92-95220-83-6 ISSN: 2363-1627 doi:10.2813/587536 QL-AL-23-001-EN-N

Cite this publication: Europol (2023), Internet Organised Crime Threat Assessment (IOCTA) 2023, Publications Office of the European Union, Luxembourg.

Your feedback matters.

By clicking on the following link or scanning the embedded QR code you can fill in a short user survey on the received strategic report.

Your input will help us further improve our products.

https://ec.europa.eu/eusurvey/runner/eus_strategic_reports

Key terms

Account takeover (ATO): the act of illegally accessing a victim's online account.

Affiliates: cybercriminals who carry out ransomware attacks using ransomware-as-a-service platforms (affiliate programs) that are ran by criminal groups. Affiliates are able to use the tools on the platform in exchange of a percentage of their criminal proceeds earned through it.

Botnet: a network of computers or Internet-connected devices that are infected with malware granting someone illegal control over them.

Bulletproof hosting: a service offered by some sites or web hosting firms that allows their customers considerable leniency on the content they can upload. Such hosting providers tend not to respond to lawful requests for information.

Crypters: software that obfuscates and encrypts malicious payloads, making them less detectable by traditional anti-virus programs.

Droppers: programs designed to deliver malicious software to a device. They usually do not have malicious functions themselves and are designed to evade and de-activate the system's security features (e.g. anti-virus, endpoint detection) before installing malware and other malicious tools (i.e. payloads).

Decentralised finance (DeFi): technologies that do not rely on third parties to facilitate the exchange, loan and payment of cryptocurrency.

End-to-end-encryption (E2EE): a method to secure communication that prevents third parties from accessing data while it is transferred from one end system or device to another. The data is encrypted on the sender's system/device and only the intended recipient can decrypt it.

Pig butchering: a combination of romance scam and investment fraud. With this modus operandi criminals build a trust relationship with the victim and convince them to invest savings in fraudulent cryptocurrency trading platforms. The scam is perpetrated over time, resulting in the loss of large amounts of money.

Phishing: the act of deceiving a person in order to steal their money or personal information. Phishing is most commonly done through fraudulent emails or websites.

Smishing: a form of phishing using text messages or common messaging apps.

Vishing: a form of phishing using voice calls and voicemails.

Spoofing: disguising a communication from an unknown source as being from a known, trusted source. Spoofing can apply to email senders, phone numbers, websites, and IP addresses.

Introduction

Cybercrime, in its various forms, represents an increasing threat to the EU. Cyber-attacks, online child sexual exploitation, and online frauds, are highly complex crimes and manifest in diverse typologies. Offenders continue showing high levels of adaptability to new technologies and societal developments, while constantly enhancing cooperation and specialisation. Cybercrimes have a broad reach and inflict severe harm on individuals, public and private organisations, and the EU's economy and security.

The year 2022 shifted the world's attention from the COVID-19 pandemic to Russia's invasion of Ukraine, which among other things put the political divides of the cybercriminal underground under a magnifying glass. Law enforcement action, hacktivism and fallout within criminal groups revealed known truths, confirmed speculations and provided insights about the inner workings of business structures - as well as the threat actors governing them. The instability in the region has resulted in the displacement of some cybercriminals active in the area, creating opportunities for law enforcement to arrest high-ranking threat actors previously outside their reach.

The carry-over effects of the geopolitical situation could be seen by the barrage of disruptive **cyber-attacks** against not only Ukrainian and Russian targets, but also worldwide, especially in the EU. The boost in these malicious activities targeting EU Member States is mostly due to a significant number of Distributed Denial of Service (DDoS) attacks affecting national and regional public institutions. These attacks were often politically motivated and coordinated by pro-Russian hacker groups in response to declarations or actions in support to Ukraine.

The invasion of Ukraine also showed once again cybercriminals' adaptability and opportunism. **Online fraudsters** responded swiftly to the circumstances and exploited the crisis by developing a variety of narratives related to it. They targeted victims across the EU under the guise of supporting Ukraine or Ukrainians. Fake webpages were created to solicit money, using URLs that included misleading key words. Emails pretending to raise funds for the humanitarian effort were sent from fraudulent addresses. In some cases, fraudsters impersonated celebrities that led or supported real campaigns or spoofed the humanitarian organisations' domains, inviting victims to donate in cryptocurrencies[1].

The threat of **online child sexual exploitation**, while not affected by these geopolitical developments, has been further increasing in terms of quantity and severity. Offenders of all crime areas continue to take advantage of legal and criminal privacy services to mask their actions and identities as their knowledge of countermeasures increases.

This IOCTA report is accompanied by three spotlight reports discussing recent developments in the main cybercrime typologies. Visit the Europol website to download or sign up for a publication notification.

1 Bleeping Computer, 2022, 'Help Ukraine' crypto scams emerge as Ukraine raises over $37 million, accessible at: https://www.bleepingcomputer.com/news/security/help-ukraine-crypto-scams-emerge-as-ukraine-raises-over-37-million/

Cybercriminal services are intertwined and their efficacy is co-dependant

Cyber-attacks are challenging to investigate as they consist of multiple steps from initial intrusion, via lateral movement and privilege escalation, to data exfiltration and exploitation, with multiple actors working on parts of the criminal process, and an important crime-as-a-service dimension.

Cybercrime services are widely available and have a well-established online presence, with a high level of specialisation inside criminal networks and collaboration between illicit providers. The services offered to perpetrate cybercrime are often intertwined and their efficacy is to a degree co-dependant. The illicit service providers cater to a large number of criminal actors by offering monitoring, delivery and obfuscation services. Such services are often offered for sale or advertised on dark web forums and marketplaces.

For example, initial access brokers (IABs) and dropper-services cater to a variety of cybercriminals and are pivotal for ransomware attacks and online fraud schemes. Malware developers and fraudsters both need channels to reach a large numbers of victims. In this context, dropper and phishing services are widely used to monitor victims and deliver malicious payloads needed to access the targeted networks. These services work with botnets to meet the demand for distribution volume.

The success rate of these operations is also dependant on the sophistication of obfuscation methods to conceal their malicious intent. Criminal groups running delivery services have a close working relationship with crypter developers. This software obfuscates the malicious payloads by encrypting them, making them less detectable by antivirus (AV) programs.

Counter antivirus (CAV) services are also very popular among cybercriminals for ensuring their criminal activities remain undetected. Malware developers and criminals providing crypter services use CAV services to scan their code against AV solutions in order to identify which parts of it are detected as being malicious. They then use this information to obfuscate the code so AV programs and firewalls do not recognise it. Some mature malware groups even hire their own pentesters to make sure that their malware will bypass antivirus software.

Virtual Private Networks (VPNs) are the most common services cybercriminals use to shield communication and Internet browsing by masking identities, locations and the infrastructure of their operations. They cater to malware operators, fraudsters, child sexual exploitation (CSE) offenders and any other cybercriminal who is in need of masking their illicit activities online. VPN providers host a number of proxies, which users can route their traffic through in order to conceal their actual location (IP) and content of their traffic. While VPN services are not illegal, some of them are designed for and advertised to criminals. Full anonymity offered by end-to-end encryption (E2EE) and a lack of cooperation with lawful requests for information from law enforcement are characteristic of these VPN services. Criminal VPN providers are aware of the needs of criminals and actively advertise their services on criminal markets.

All of these providers require infrastructure that offer them resilience to disruption and concealment from law enforcement. Many Internet Service Providers (ISPs) frequently used by criminals do not engage in extensive customer monitoring practices such as Know-Your-Customer (KYC) procedures and storing of customer and metadata (e.g. IP address), facilitating criminal activities. Some of them do not provide customer information upon lawful requests except for an automated confirmation of an email address, leading to a limited availability of identifying information on a suspect. Additionally, hosting is a complex international business area where servers are often resold to other datacentres located in different regions. This type of hosting is referred to as bulletproof hosting, which has been notoriously difficult for law enforcement authorities to address for many years.

VPNLab takedown – OPERATION OVERLORD[2]

VPNLab, one of the most prolific services used by cybercriminals, was taken down in a law enforcement action in January 2022. The action day followed coordinated investigative efforts from Canada, Czechia, France, Germany, Hungary, Latvia, the Netherlands, Ukraine, the United Kingdom and the United States, with the support of Europol and Eurojust. Europol provided analytical and forensic support, facilitated information exchange and coordinated more than 60 operational meetings.

Like most VPNs, this service shielded communications and Internet browsing. VPNLab was used in support of serious criminal acts, such as setting up of infrastructure and communication behind ransomware operations and malware distribution. The service, active since 2008, was advertised on the dark web for as little as USD 60 per year and did not cooperate with lawful requests from law enforcement authorities.

Various servers of VPNLab were located in the EU, and some in third countries. The investigative measures taken against VPNLab have demonstrated how the take down of one service can help further numerous other investigations. For example, many users of VPNLab used the service to connect to domains of companies who were compromised by a ransomware group.

Similar techniques for different goals

The defence against different forms of cybercrime is as strong as the weakest link, which continues to be human oversight. Phishing emails, malicious document files, social engineering techniques and unpatched soft- and hardware are the most common ways criminals introduce themselves into their victims' systems.

Social engineering, and in particular phishing, are extensively used by all types of cybercriminals. This technique uses deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes[3]. Social engineering has increased in both volume and sophistication, while at the same time EU regulatory developments[4] have made frauds with compromised payment cards more difficult, resultantly shifting the criminal focus onto users rather than digital systems. Phishing is a key access vector for most types of online fraud schemes and malware-based attacks, aiming to intrude into systems, steal data or extort money. Phishing emails containing malware, Remote Desktop Protocol (RDP) brute forcing and VPN vulnerability exploitation are the most common intrusion tactics used by cybercriminals. Legitimate software and tools built into operating systems are then misused to establish persistence and traverse their victims' networks. The increased availability of phishing kits allows more criminal networks to be successful in phishing attacks, regardless of their level of organisation and technical expertise. Phishing can also have different manifestations, depending on the mean of communication exploited. Common alternative manifestations are smishing (SMS phishing) and vishing (voice phishing).

---

2 Europol, 2022, Unhappy New Year for cybercriminals as VPNLab.net goes offline, accessible at https://www.europol.europa.eu/media-press/newsroom/news/unhappy-new-year-for-cybercriminals-vpnlabnet-goes-offline

3 Europol, 2017, Serious and Organised Crime Threat Assessment, accessible at https://www.europol.europa.eu/socta/2017/

4 Directive (EU) 2015/2366 (payment service directive 2 – PSD 2) provides the legal foundation for the further development of a better integrated internal market for electronic payments within the European Union (EU). It establishes comprehensive rules for payment services, with the goal of ensuring harmonised rules for the provision of payment services in the EU and a high level of consumer protection. Full Directive available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L2366

Impersonation is a technique widely used by criminals involved in child sexual exploitation and online fraud schemes, in order to deceive victims. Child sexual exploitation offenders make extensive use of social media to engage with their victims, interacting with them often behind a false identity. Online fraudsters impersonate legitimate businesses, institutions, non-governmental organisations and individuals to solicit money transfers or obtain access to the victims' sensitive information. Charity scams are a particularly unscrupulous type of online fraud scheme using impersonation. Profiteering from the generosity of individuals towards those in need, criminal actors take advantage of current emergency situations posing as genuine organisations to obtain donations, victimising both the donor and the legitimate charity. Scams exploiting crises have been increasingly detected in the past years, first in relation to the COVID-19 pandemic, and more recently in the context of the Russian invasion of Ukraine and the earthquake in Türkiye and Syria.

Spoofing is an example of a very effective technique to gain victims' trust, allowing fraudsters to make a phone call or to send a text message that show a caller ID different from that of the telephone from which the call is actually placed. Spoofing is often used by fraudsters to appear like a credible person or service to lure victims into giving up sensitive data, such as two-factor authentication (2FA) tokens or PINs. In some cases, ransomware operators use spoofing to call victims to carry out ransom negotiations while concealing their identities. Some criminal networks provide spoofing-as-a-service to other criminals.

Common intrusion techniques applied to perpetrate cyber-attacks are also used by criminals involved in online fraud schemes in order to access and manipulate payment and digital systems while undetected. Malware is injected into Automated Teller Machines (ATMs) to manipulate their operating system and eject cash. Digital payment systems are also hijacked through malware infections with the goal of stealing customers' card data in a process called digital skimming.

These illicitly obtained credentials are often used for carding, usually performed by bots that test the validity of stolen card data and use them to make purchases. Thanks to the bots, criminals are able to make parallel automated operations to attempt purchase authorisation.

Takedown of the iSpoof platform – OPERATION ELABORATE[5]

'iSpoof.cc' was a website that provided criminals with various services including Automated Interactive Voice Response (IVR), Interception of Telepins and live monitoring of calls. The website could be used to target victims worldwide. The successful takedown of this platform in November 2022 led to the arrest of 142 suspects. The website is believed to have caused an estimated loss in excess of EUR 115 million. Law enforcement authorities from Australia, Canada, France, Germany, Ireland, Lithuania, the Netherlands, Ukraine, the United Kingdom and the United States, with the support of Europol, cooperated in this case. Europol developed intelligence packages to the national investigators, provided a secure platform to exchange large files of evidence and identified additional users of the criminal service who were already known for their involvement in other high-profile cybercrime investigations. After iSpoof was taken down, the UK Metropolitan Police (MET) announced that 10 million spoof calls had been made using the site between June 2021 and July 2022. The MET recreated an introductory video from iSpoof, previously created by the criminal administrators to explain how to use the platform, with an edited voiceover to deter future users of spoofing services and to show users of iSpoof that the police now has access to their data. The MET also texted 70 000 numbers to make them aware that they had been targeted by iSpoof scammers. These pro-active measures show that seized databases and/or wiretapped servers

5 Europol, 2022, Action against criminal website that offered 'spoofing' services to fraudsters: 142 arrests, accessible at https://www.europol.europa.eu/media-press/newsroom/news/action-against-criminal-website-offered-%E2%80%98spoofing%E2%80%99-services-to-fraudsters-142-arrests

The central commodity of this illicit economy is stolen data

The central commodity of this illicit economy is stolen data, which is bought for and produced by different cyber-attacks. Affiliates of ransomware programs, fraudsters and hackers seek victim information for gaining access to their systems and bank accounts. Criminal markets are booming with stolen credentials and victim data produced by the aforementioned actors through compromising databases and social engineering techniques. Child sexual exploitation offenders groom victims in order to obtain sensitive information that can be then exploited for extortion purposes. Data theft is a core threat as stolen data can be used in a wide array of criminal activities, including commodification, access to systems, espionage, extortion and social engineering.

Crime-as-a-service providers collaborate closely with IABs whose portfolios consist of access information of high-value victims. Unfortunately, cybercriminals do not hold exclusivity in high regard and sell data to whoever is willing to purchase it.

In order to successfully execute their operations, cybercriminals require access to leaked sensitive information of victims, such as (databases of) personal data. Criminal hacking forums often offer this type of information for sale. A notorious example of this phenomenon was RaidForums, taken down in Operation Tourniquet, a coordinated law enforcement action carried out in April 2022.

There has been a change of the type of stolen data that is available on criminal markets. It is no longer only static (e.g. credit card details and login credentials), but is compiled of a number of datapoints retrieved from victims' malware-infected devices. There is an increase in activity on marketplaces for stolen data and in the demand for IABs[6]. Listings posted by IABs include advertisement of systems they have access to, sometimes accompanied by company revenue.

The services of IABs are more catered towards high-end cybercriminals, who want access to high-value victims. This is in contrast to platforms such as Raidforums, which offer less targeted 'wholesale access' of stolen data that is more relevant for less technically skilled cybercriminals. Some IABs are active on the clear and dark web. IABs have a variety of stolen victim data on offer (e.g. login credentials, browser cookies, mobile device identifiers, email addresses, user names, and passwords).

In order to counter unauthorised access to personal accounts, fingerprinting technologies have been developed.

RaidForums shutdown – OPERATION TOURNIQUET[7]

RaidForums started its operations in 2015 and grew to be one of the world's biggest hacking forums with a community of over half a million users. It focused on the harvesting and re-selling of 'exclusive' personal data and databases from compromised servers. RaidForums made a name for itself by hacking rival forums and releasing (doxing) personal information about their administrators.

The high-profile database leaks that were sold on the forum usually belonged to corporations across different industries. They included data of millions of credit cards and bank account numbers, routing numbers as well as usernames and passwords needed to access online accounts. This type of data can be used to steal funds online, but also to launder criminal proceeds through various accounts that cannot be linked to the criminal actors (i.e. money mule accounts).

Next to the forum admin, two accomplices were arrested. Europol coordinated various independent investigations into RaidForums (by Portugal, Romania, Sweden, the United kingdom and the United States), which led to the take down of the service in April 2022.

---

6 Sophos, 2022, Genesis Brings Polish to Stolen-Credential Marketplaces, accessible at https://news.sophos.com/en-us/2022/08/04/genesis-brings-polish-to-stolen-credential-marketplaces/

7 Europol, 2022, One of the world's biggest hacker forums taken down, accessible at https://www.europol.europa.eu/media-press/newsroom/news/one-of-world's-biggest-hacker-forums-taken-down

This online anti-fraud system recognises suspicious fraudulent traffic by collecting unique identification information from a specific user device. Digital fingerprints are composed of attributes used for browsing and digital behaviour. Digital fingerprints can therefore be used to accurately impersonate the browser activity on the victim's machine in order to bypass anti-fraud detection systems. This type of data is taken from malware-infected computers, compiled into packages and sold.

Fraud against payment systems is often driven by the theft of personal information that can be then used in multiple ways. This type of data can in fact be used for further criminal acts including identity theft, obtaining additional information on victims and performing fraudulent financial transactions. It can also be used for refining social engineering in order to perpetrate more targeted and effective online fraud schemes impacting individuals whose information was stolen during the primary criminal process.

The quick development of a widespread data trade ecosystem has increased the threat of account takeover (ATO). This process occurs when criminals illegally access a victim's online account for their own gain. Targeted accounts (such as online banking, email accounts or social media profiles) are valuable to criminals as they can hold funds, provide access to specific services, or contain important private information that can be sold online. ATO is also carried out either to directly access the victim's account or to harvest data to be traded further. Nowadays, ATO is considered quite an easy technique to implement, as brute force, cracking tools and account checkers are sold on cybercrime forums for a very low price.

Same victims, multiple offences

Cybercrime is often interlinked, presenting a concatenated set of criminal actions that often results in the same victim being targeted multiple times. This is particularly apparent in child sexual exploitation offences, malware attacks and online fraud schemes. For instance, investment frauds are in some cases linked to other types of frauds, such as romance scams (i.e. pig butchering) and therefore re-victimising the target. Following the theft of the investments and the realisation of the fraud, criminals often contact their victims posing as lawyers or law enforcement agents offering help to retrieve their funds, in exchange for a fee.

Victim information is often monetised to its full extent - meaning that it can be sold to several buyers - which leads to targets being re-victimised by fraudsters and malware distributers alike. The power of information is undeniable, as ransomware groups have now used it as a hostage for several years. In addition, compromised organisations can be exposed to several simultaneous or consecutive cyber-attacks because the IABs usually do not offer exclusivity of their assets to the buyers. Due to this, the same compromised credentials can be used by different cybercriminals[8].

Victims of child sexual exploitation suffer re-victimisation both offline and online. Hands-on abusers often perpetrate their offences for a significant amount of time and, in several cases, encourage other offenders to abuse the victim as well. The depiction of sexual abuses on children results in their repeated victimisation. The child sexual abuse material (CSAM) produced by offenders is in fact shared at many levels, from closed communities of trusted perpetrators to large communities on online forums. The receivers of this imagery in most cases share it further, resulting in the same CSAM being encountered by investigators over many years and the same victim being impacted.

Underground communities to educate and recruit cybercriminals

Dark web forums are heavily used by cybercriminals for communication, knowledge-sharing, exchange of digital commodities and recruitment. Recent

8 SOPHOS, 2022, Multiple attackers: A clear and present danger, accessible at https://news.sophos.com/en-us/2022/08/09/multiple-attackers-increase-pressure-on-victims-complicate-incident-response/

research[9] reports that young individuals also make use of such environments, engaging in risky behaviour online. Among the young participants of the survey, 51 % reported to use online forums and chat rooms, out of which 12 % use dark web forums and 11 % dark web marketplaces.

Ransomware groups make use of forums on the clear and dark web to recruit new affiliates, pentesters, company insiders[10], IABs and money mules. Ransomware leak sites have also been identified as places where affiliates are being recruited. Similarly, child sexual exploitation offenders make extensive use of these types of forums to digitally meet likeminded individuals, enhance their criminal knowledge, exchange and consume CSAM.

Virtually all types of criminal services are available for sale in these environments. Criminal hacking forums selling stolen data are booming. Crime as-a-service providers are aware of the needs of criminals and actively advertise their services on criminal markets, from criminal VPNs to IABs.

Dark web forums are also an important source for gathering information on operational security (OpSec). Users give recommendations on how to avoid detection and identification in dedicated forum discussions. Guidelines and tutorials on topics such as fraud methods, child sexual exploitation, money laundering, phishing and malware are widely distributed. Furthermore, manuals and FAQs are available on how to operate on a dark web marketplace and to conduct illicit trades.

Law enforcement action and (rival) DDoS attacks have created instability in dark web marketplaces, decreasing their average lifespan. Several known market places retired or performed an exit scam on their users in 2022.

What happens with the criminal profits?

Cybercriminals use a variety of services to launder their criminal proceeds, depending on the volume and the form of their profits. They often utilise their own money laundering capabilities (with money mules, straw men, and crypto mixers), however some networks contract professional money launderers in a crime-as-a-service collaboration. Mirroring the global dimension of cybercrime, these networks are composed of members located in different countries, adding complexity to the laundering scheme. However, law enforcement has successfully unveiled criminal networks providing professional money laundering services.

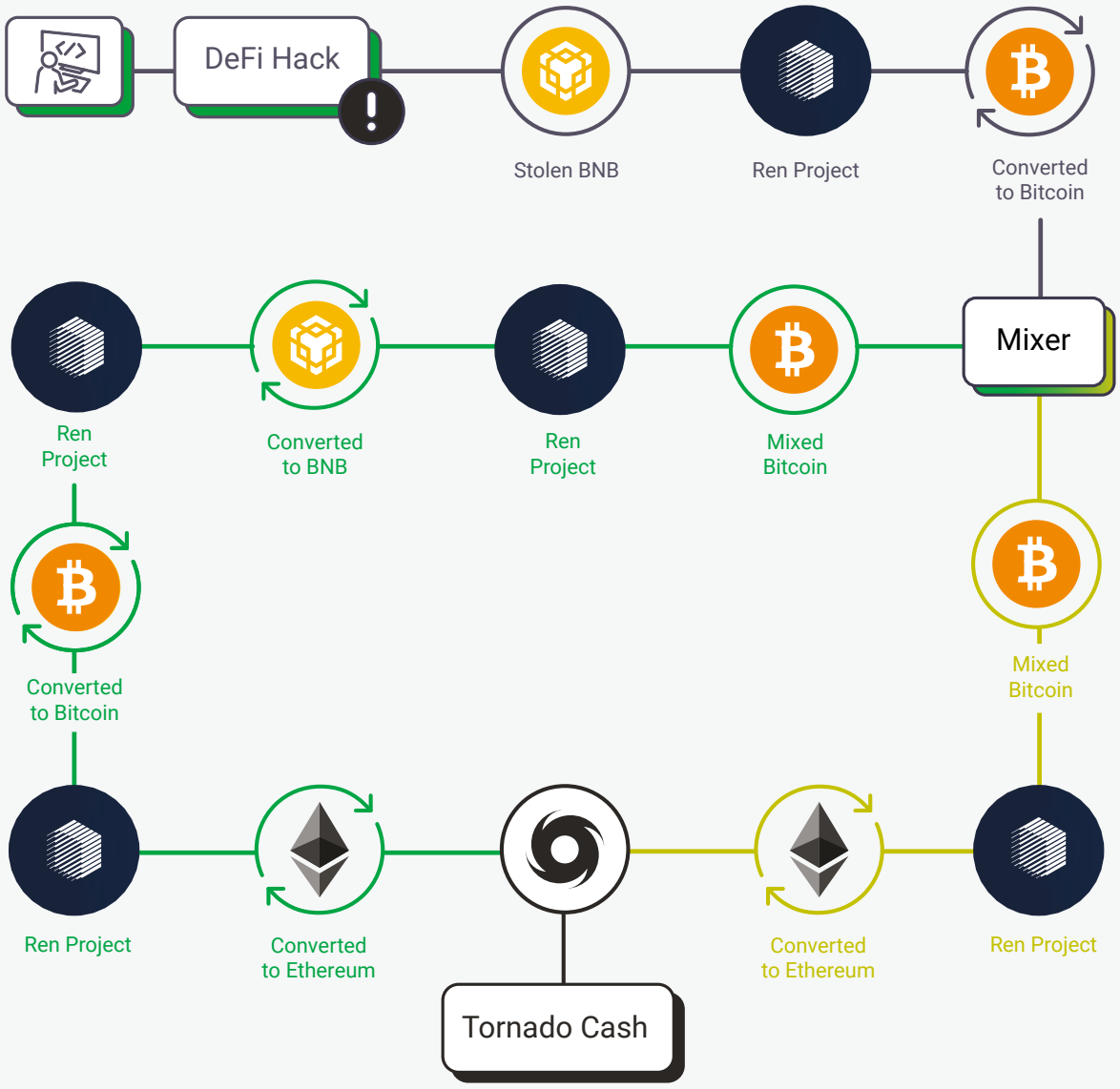
Ransomware groups receive cryptocurrency payments from victims directly to their dedicated wallet. From there funds are usually funnelled through a mixer and distributed automatically between the administrators, the affiliate carrying out the attack and the service providers. The split of the profits received by the affiliate is based on their rank, which is determined by the success rate of their attacks and the criminal profits generated. At entry level the affiliate shares are low (around 20-40 % of the ransom), but at higher ranks they can receive up to 80 % of the profits because they have proven to be a lucrative business partner for the criminal groups running the service.

Cybercriminals involved in cyber-attacks and related services, as well as those trading and administrating dark web marketplaces, carry out their financial transactions almost exclusively in cryptocurrencies. For this reason, they make extensive use of obfuscation techniques to anonymise their financial activities before cashing out the illicit profits. These techniques include the use of mixers, swappers, over-the-counter trading and decentralised exchanges. In many cases, obfuscation methods are used prior to sending the funds to exchanges. The use of several obfuscation methods deployed on top of each other is a common practice. This requires highly skilled investigators to utilise various methods to follow cryptocurrency (demixing, tracing cross-chain swaps, analysing liquidity pools, etc.), which slows down investigations. Still, mixers are the most commonly encountered obfuscation method. Mixers facilitate obfuscation by blending the funds of many users together, concealing the financial trail.

---

9 The CC Driver European Youth Survey 2021 cover participants aged between 16 and 19 years old. It aims to explore and identify the drivers that may encourage and enable some young people to engage in cybercrime. Accessible at https://www.ccdriver-h2020.com/post/cc-driver-2021-european-youth-survey

10 TrendMicro, 2022, Ransomware spotlight – LockBit, accessible at https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-lockbit



This visual illustrates a complex cryptocurrency case. In this Decentralised Finance (DeFi) hack, the cryptocurrency BNB is stolen and sent to RenProject, a protocol that allows for the movement of value of cryptocurrency across blockchains. BNB is converted to bitcoin, which is then sent to a mixer (and therefore needs to be demixed by investigators, a complex labour-intensive task). The funds are then split, which often happens in ransomware cases[11]. The split funds are converted to RenBTC, with some on the Ethereum blockchain and some on the BNB blockchain. The former are converted to Ethereum, after which they are deposited to mixer Tornado Cash. The latter is converted back to bitcoin on the Bitcoin blockchain (through REN) and then converted to RenBTC on Ethereum blockchain and eventually into Ethereum, after which it is sent to Tornado Cash.

---

11 Splits in criminal cryptocurrency cash-outs often point to various criminals and affiliates involved, and might lead to payments for criminal infrastructure.

Criminal networks involved in fraud accrue their profits in both fiat and cryptocurrencies. The laundering of their criminal funds usually happens very quickly after the fraud has taken place; this means that by the time the victim realises the scam, the money is already split through accounts based in multiple countries and laundered. Online fraudsters in particular make frequent use of gambling platforms to launder profits, as they can be used to obscure the origins and flows of illicitly-obtained funds.

All the above types of cybercriminals make use of money mules to launder illicit profits, whether in fiat or cryptocurrencies. Money mules are key facilitators for the laundering of illicit profits generated by cybercrime as they enable criminals to swiftly move funds across a network of accounts, often in different countries.

While money mules are sometimes recruited in criminal forums, social media remains a key recruitment environment. Sometimes, the victims of frauds are unwittingly used as money mules themselves. The use of neo banks has been observed in several investigations into criminal offences involving the use of money mules

Europol's support

Europol's mission is to support EU Member States and cooperation partners in preventing and combating all forms of serious international and organised crime, cybercrime and terrorism. In 2013, Europol set up the European Cybercrime Centre (EC3) to strengthen the law enforcement response to cybercrime in the EU and thus to help protect European citizens, businesses and governments from online crime. EC3 offers operational, strategic, analytical and forensic support to Member States' investigations. At the level of operations, EC3 focuses on cyber-dependent crime, child sexual exploitation, illicit trade on the dark web and alternative platforms as well as online fraud schemes including payment fraud.

European Money Mule Action - EMMA 8[12]

A total of 25 countries, supported by Europol, Eurojust, INTERPOL and the European Banking Federation (EBF) have joined forces for the annual iteration of operation EMMA, aimed to crack down money mules and their recruiters. During an operational phase carried out between mid-September to the end of November 2022, 8 755 money mules were identified alongside 222 recruiters, and 2 469 individuals were arrested worldwide. With the coordination of the EBF, around 1 800 banks and financial institutions supported law enforcement authorities in this action, together with online money transfer services, cryptocurrency exchanges, Fintech and KYC companies, and multinational computer technology corporations. In some cases, the ease of opening bank accounts with misused or stolen personal details largely facilitates the mules' work. In many countries, cryptocurrencies remain the main means to cash money out.

Following recent trends, Asia and Africa are the final destinations of many of the illegal transactions. Several countries reported how the mules involved in respective investigations are mainly from abroad and, consequently, the money is sent using foreign accounts.

12 Europol, 2022, 2 469 money mules arrested in worldwide crackdown against money laundering, accessible at https://www.europol.europa.eu/media-press/newsroom/news/2-469-money-mules-arrested-in-worldwide-crackdown-against-money-laundering

About this report

The Internet Organised Crime Threat Assessment (IOCTA) is a strategic analysis report that provides an assessment of the latest online threats and the impact of cybercrime within the EU. The report provides a law enforcement centric view of the threats and developments related to cybercrime, in order to inform decision-makers at strategic, policy and tactical levels in the fight against cybercrime, with a view to updating the operational focus for EU law enforcement authorities.

The IOCTA is chiefly informed by operational information shared with Europol by EU Member States and third partners, combined with expert insights and open source intelligence. The following analysis is based on a set of indicators established by Europol, focusing on developments related to criminal actors and networks, criminal processes, infrastructure used, financial transactions, and the impact on society.

This ninth edition of the IOCTA appears in an updated format. The current summary presents the main overarching findings concerning the different typologies of cybercrime, namely cyber-attacks, online fraud schemes, and online child sexual exploitation. It is accompanied by a series of spotlight articles covering each of these crime areas in-depth.

EUROPOL

This publication and more information on Europol are available on the Internet.

www.europol.europa.eu