

ANNUAL CYBERCRIME REPORT

2025



ANNUAL CYBERCRIME REPORT

2025

COMCYBER-MI

« Nos forces, pour votre cyber-protection »

Ministry of the Interior's
Cyberspace Command

Foreword	7
Key figures for 2024	8
Major trends and developments in cybercrime	9
1 Cybercrime ecosystem	10
1 Industrialisation of cybercrime	12
2 Communication methods used by cybercriminals	14
3 Cybercrime-as-a-Service	15
2 Modus operandi of cybercriminals	18
1 Main methods of action	20
2 Use of technology for malicious purposes	31
3 Hybrid modus operandi	37

3 Major investigations and legal developments **40**

- 1 |** Legal developments **42**
- 2 |** Major investigations feedback (OFAC, UNCyber and BL2C) **44**

4 Forecasting the evolution of cyber threats **50**

- 1 |** The use of AI to prevent future threats **52**
- 2 |** The Internet of things : a vector of emerging risks **54**

Useful information **56**

Lexicon **60**

KEY FIGURES FOR 2024



348 000*

digital offences recorded
in 2024

+74% digital offences
in five years



65%

property
offences



29,7%

assaults
on individuals



4,9%

attacks on
institutions and
public order



0,4%

infringements
of specific digital
laws and regulations



17 100

attacks on information
systems in 2024



-13% referrals for
ransomware attacks



107 331 complaints or reports of
internet scams registered on the
THESEE platform



222 364 reports of illicit
content registered on
the PHAROS platform

PERCEV@L

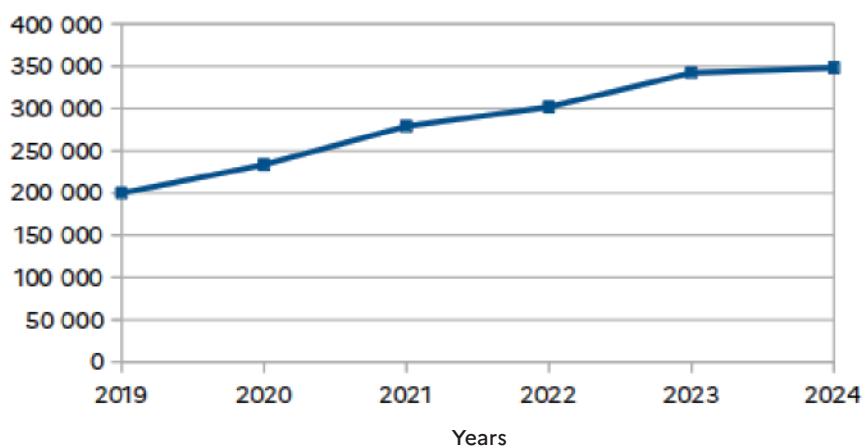
230 537 reports of
fraudulent use of credit
cards registered on the
Perceval platform



60 000

accused of digital
offences

Number of offences registered annually since 2019



NB : The figures presented are based on data compiled by the Ministerial Statistical Service for Internal Security, supplemented by other institutional sources: Section J3 of the Paris Public Prosecutor's Office, the National Police Anti-Cybercrime Office, and the National Gendarmerie Cyber Unit.

* This figure includes the 50,800 complaints filed on the Thesee platform.

Ransomware

Although the number of complaints lodged for ransomware attacks fell by 13% in 2024 compared with the previous year¹, the threat remains significant.

In order to increase efficiency and prevent detection by security systems, encrypting victims' data has become increasingly rare. Attackers now increasingly rely on data theft and threatening to disseminate it to force victims to pay the ransom.

The hierarchy of ransomware groups has undergone several upheavals.

Coordinated international law enforcement operations against LockBit in 2024 undermined its dominance. RansomHub has overtaken LockBit in terms of the number of reported attacks. Several highly active ransomware groups emerged in 2024. Some reuse leaked source code, while others develop their own ransomware with the help of artificial intelligence (AI).



Hacktivism

International conflicts have been strongly mirrored in cyberspace.

In 2024, 707 hacktivist attacks against France were claimed. Some hacktivist groups that used to act alone have joined forces with like-minded groups, giving rise to coalitions, some of which specifically target France.

At the same time, several cases of 'false flag' attacks have been observed.

In terms of modes of action, hacktivists continue to favour distributed denial of service attacks (DDoS) and website defacements.

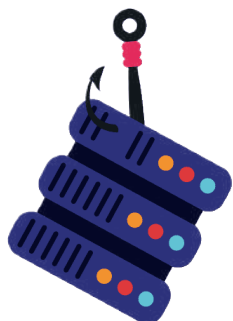
There have also been reports of attacks claimed against SCADA systems (supervisory control and data acquisition).



Data theft

Public awareness of the risks posed by data breaches increased significantly in 2024. Several sales of personal data concerning millions of French citizens over the past year have been reported in the media.

Cybercriminals have also recognised the potential profits to be made from selling or reselling this data. Some even sell recycled databases (previously leaked), AI-generated datasets, or information taken from publicly available sources



Artificial intelligence

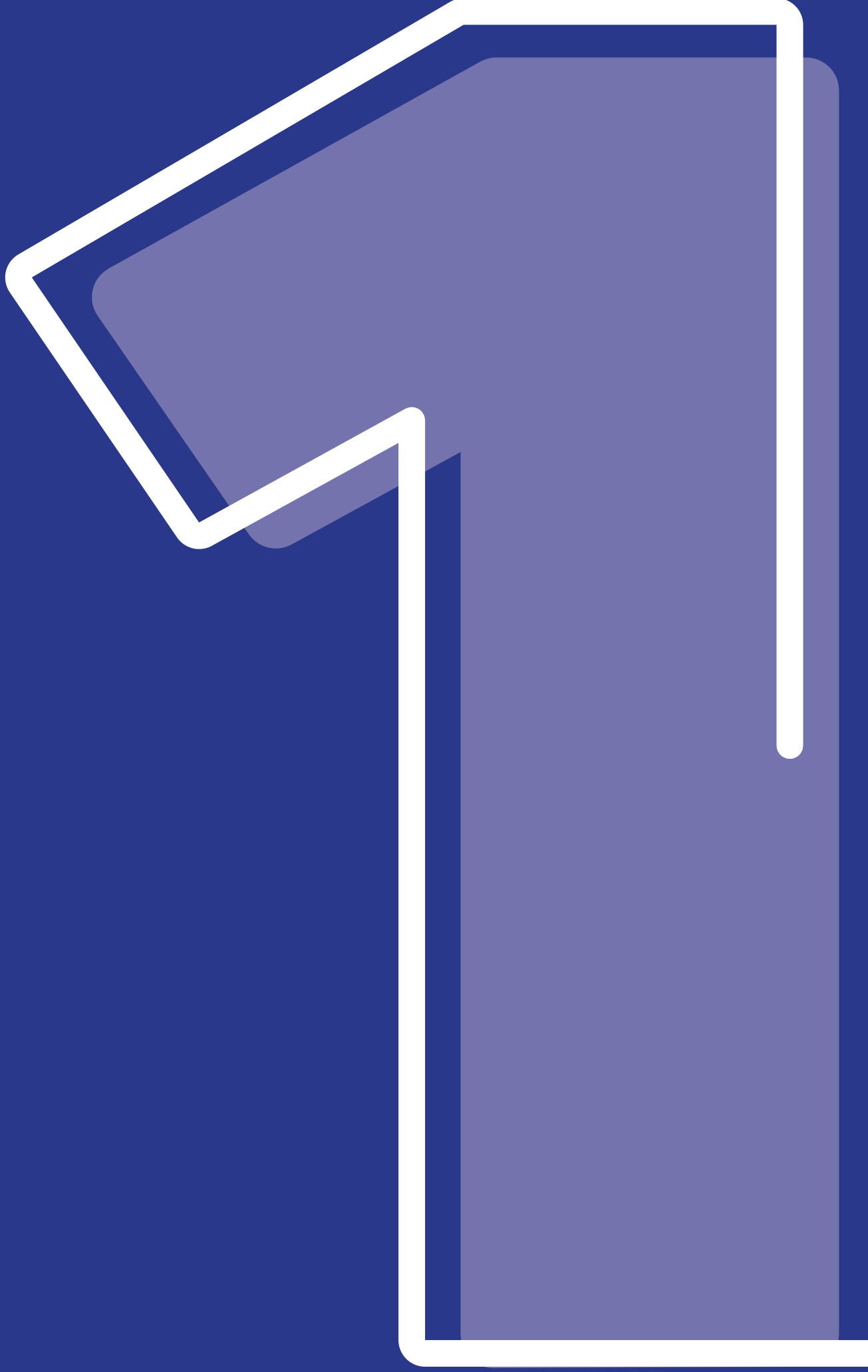
In 2024, the evolution of artificial intelligence, particularly generative AI, continued, both in terms of protection against cyber threats and for the benefit of attackers. Today, AI represents both an unprecedented threat and an unprecedented opportunity in cyberspace. Technologies based on large models (LLM : large language model, VLM : large vision model, LAM : large action model) can be exploited both to create malicious software and to better detect cyber threats.

AI also contributes to DDoS attacks, amplifying their impact many times over. In particular, it allows attackers to manage multi-vector attacks, adapting to targets in real time as circumstances change.

While it increases criminals' access to sophisticated techniques, thereby improving their effectiveness, law enforcement agencies must understand it if they are to effectively counter this growing trend in cybercrime.



1. Source: Paris Public Prosecutor's Office - 3rd Division - JIRS/JUNALCO - Section J3 - cybercrime



CYBERCRIME ECOSYSTEM

1 	Industrialisation of cybercrime	12
2 	Communication methods used by cybercriminals	14
3 	Cybercrime-as-a-Service	15

1

CYBERCRIME ECOSYSTEM

Cybercriminal groups are analysed in terms of their modus operandi. They are made up of individuals with their own computer skills or financial capacity. The primary responsibility of law enforcement agencies consists of locating them in order to arrest them, usually in the context of international cooperation. Some malicious actors can be categorised as script kiddies who acquire ready-to-use tools, while others have genuine expertise in IT security.

Cybercriminals have three main motivations : financial gain (ransomware, data sales), ideological (website defacement, DDoS attacks) or ego (technical challenges, seeking recognition).

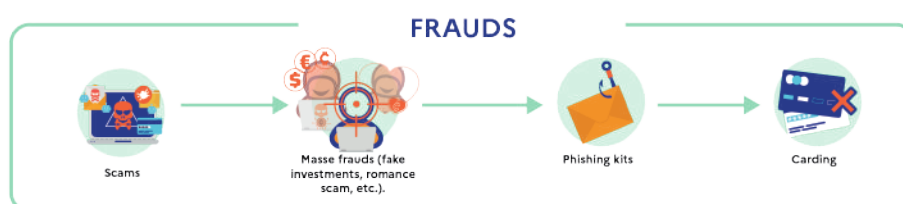
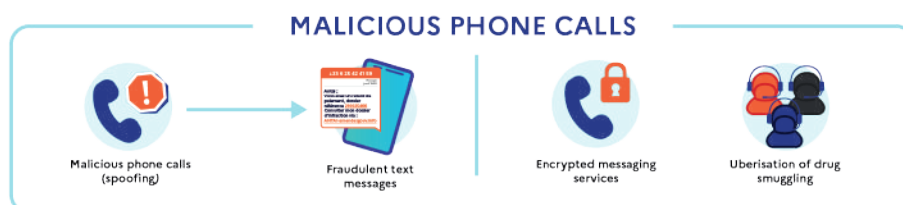
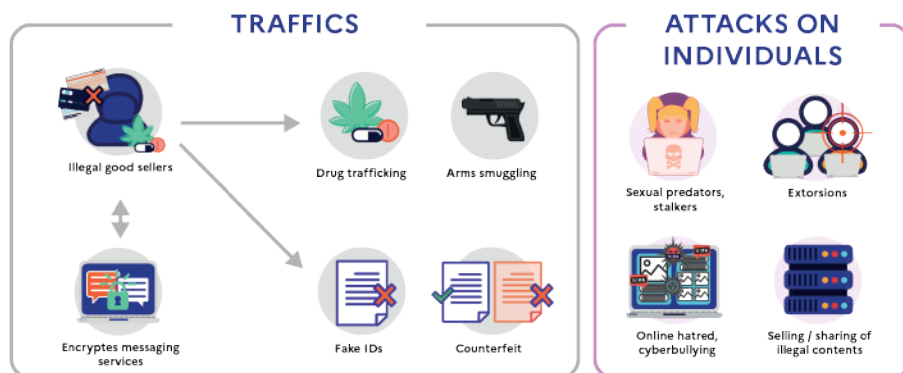
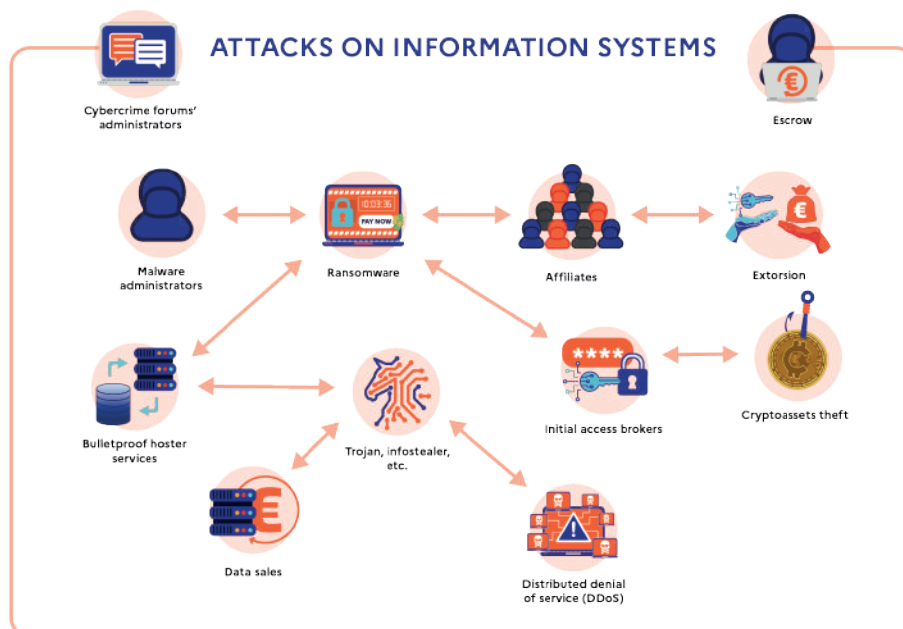
They may also be driven by other motives : deviance (child sexual abuse) or toxic behaviour (harassment). These threat actors may act alone, but they usually act as part of a coordinated effort.

While some collaborate out of opportunism or to increase their capacity to cause harm, others have formed genuine criminal groups, with their own organisation and modus operandi.

1 | Industrialisation of cybercrime

Over the past decade, the cybercrime landscape has expanded steadily, reaching a turning point in 2024 with the adoption of technical tools and the increasing specialisation of tasks within cybercrime ecosystems. This stage of industrialisation transformed the way cybercriminals interacted. To carry out their illicit activities, malicious actors benefit from numerous tools (servers, malware, etc.) and communication infrastructure (underground forums, encrypted messaging, social media), enabling them to interact with each other and optimise their actions. On cybercrime forums, for example, it is possible to buy access to company servers or lease malicious software to carry out massive cyberattacks or scams. These actors maintain close ties with money laundering operators, who use both traditional organised crime laundering methods and cryptoassets.

This ecosystem has evolved following legitimate market, to a process of distribution, automation and rationalisation of tasks between cybercrime actors. Some groups or individuals specialise in developing malwares, while others focus on selling initial access or databases. However, all these malicious actors are interconnected via numerous means of communication, mainly for opportunistic reasons. Therefore, they are able to subcontract certain tasks or offer services to other actors for compensation.



Online narcotics trafficking

Online drug trafficking is a criminal market that has taken on unprecedented proportions with the emergence of thousands of digital dealing points. The darknet, cybercrime forums, encrypted messaging and social media offer organised crime groups alternatives for their trafficking activities, providing both operational optimization tools and concealment methods. These technologies facilitate secure exchanges and contribute to the uberisation phenomenon of drug trafficking. They involve both retail sales for individuals and large quantities for drug traffickers.

2 | Communication methods used by cybercriminals

The cybercrime ecosystem may seem complex, given the multitude of threat actors involved. However, their activities can be grouped into four types of criminal infrastructure, enabling them to exchange information on a daily basis: cybercriminal forums and open discussion channels, encrypted messaging, social media and the use of telephones.

Cybercrime forums are central to exchanges between threat actors, facilitating the trade and outsourcing of illegal services and information. The exchanges carried out via these forums enable cybercriminals to exchange, purchase, contract and monetize services (malware, initial access, databases, recruitment of cybercriminals, knowledge sharing, etc.).

Although many cybercrime forums have discussion forums covering a wide range of malicious activities, some of them specialise in specific types of operation (ransomware attacks, data sales, etc.).

These forums are divided into sub-forums dedicated to specific topics, and sometimes target specific communities, for example by language (French, Russian and English speakers etc.). Some of these sub-forums are used by small groups of highly skilled cybercriminals.

Cybercriminals also use encrypted messaging, perceived as more secure, to discuss highly sensitive matters such as transaction amounts, recruitment of cybercriminals, etc. However, these platforms do not provide complete operational security, since large-scale law enforcement operations are also being carried out on this type of tool, following the example of Encrochat² or Ghost³ by the national gendarmerie and SkyECC⁴ by the national police. These operations identified tens of thousands of criminals and cybercriminals.

In addition, many cybercriminals use both social media to target many victims, and telephony, to exchange information via encrypted solutions or canvass victims. Cybercriminals and scammers use specialised tools to execute large-scale automated fraud campaigns or to steal personal or financial data.

These communication tools are used by cybercriminals to strengthen and secure their exchanges, but they are dismantled by internal security forces that specialise in fighting cybercrime.

2. <https://www.gendarmerie.interieur.gouv.fr/gendinfo/criminalite-organisee-et-enquetes/2020/retour-sur-l-affaire-encrochat>

3. <https://www.gendarmerie.interieur.gouv.fr/gendinfo/criminalite-organisee-et-enquetes/2024/les-gendarmes-cyber-chasseurs-de-ghost>

4. <https://www.europol.europa.eu/media-press/newsroom/news/new-major-interventions-to-block-encrypted-communications-of-criminal-networks>

3 | Cybercrime-as-a-Service

Cybercrime-as-a-Service (CaaS) involves providing ready-made skills or tools in exchange for payment. These exchanges are mainly carried out on closed forums, sometimes requiring a transfer of money or interaction with the platform administrators. This model is most commonly associated with ransomware operations. However, it also relates to other aspects of cybercrime.

The main services offered on these forums consist of selling, buying or renting :

- Exploits and initial access to compromise a victim's machine ;
- Malware for infection, remote access, or data encryption ;
- Anonymization services including bulletproof hosting infrastructure ;
- Various human technical skills.

CaaS is a generic term that can also be broken down into sub-categories :



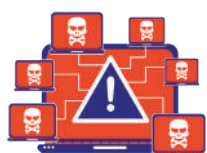
Phishing-as-a-Service

A cybercrime actor provides a customer with turnkey tools to launch a phishing campaign.



Malware-as-a-Service

The rental or sale of ready-to-use malicious software to steal information stored on an information system, such as passwords or private keys (e.g. infostealers).



DDoS-as-a-Service

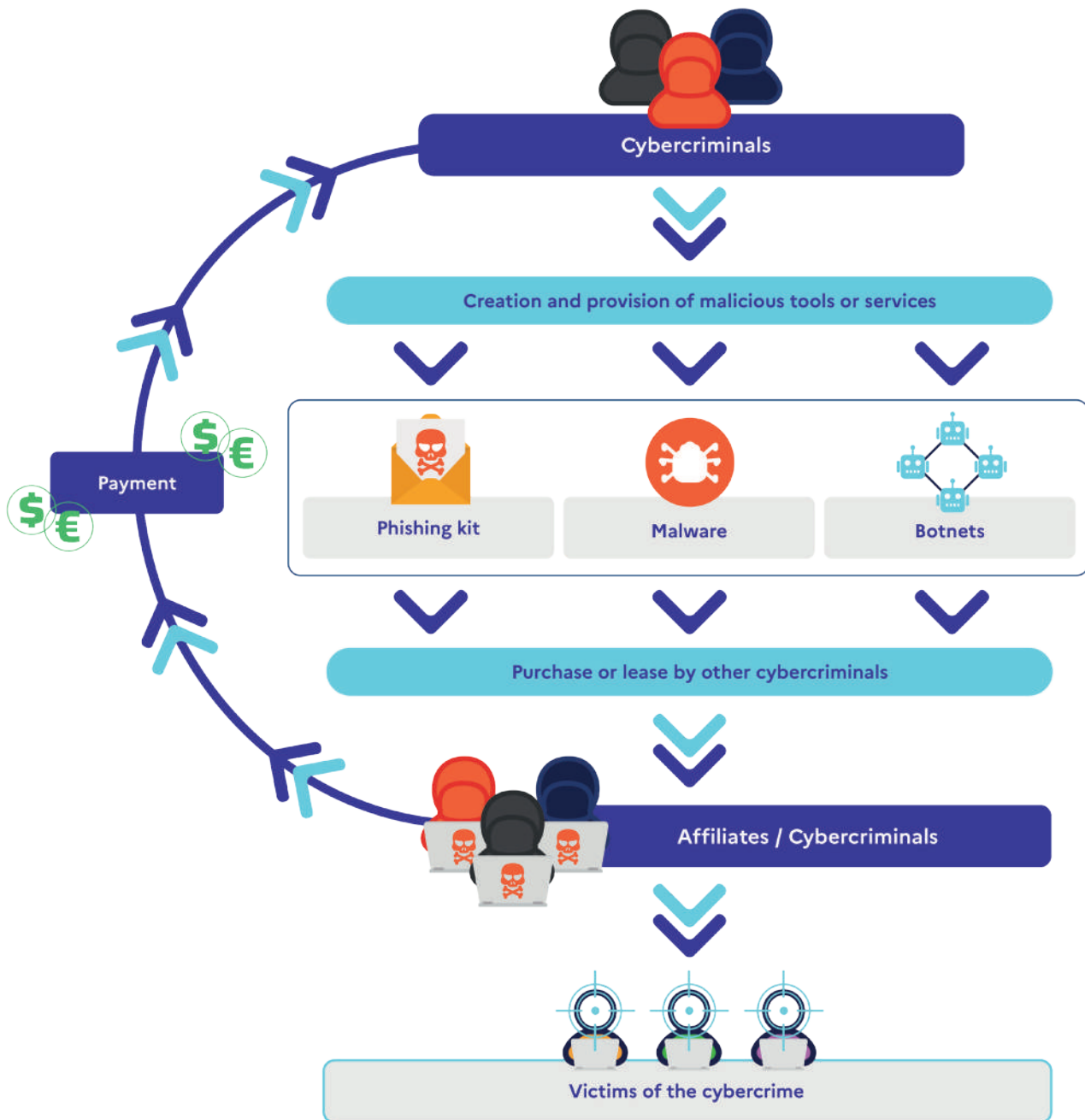
Botnet rental services for server saturation attacks.



Ransomware-as-a-Service

The provision of tools for deploying ransomware on a target's information system.

Cybercrime-as-a-Service is set to continue over the next few years. Attracted by the possibility of quick financial gain, an increasing number of threat actor, particularly minors and young adults, are adopting these ready-made services.



Modelling cybercrime-as-a-service

Ransomware-as-a-Service

Ransomware operations are enabled through CaaS models, making it widely possible to carry out attacks of this type. The administrator/affiliate model, similar to a corporate structure, is set up between developer groups that create malicious software and affiliates who deploy the software.

Affiliates provide developers with a percentage of ransom proceeds. New ransomware variants emerged in 2024, with several of these variants still being highly active (RansomHub, Qilin, Hell-Down, apt73/bashe, Termite, etc.). Two movements can be observed: on the one hand, the Termite group claiming eleven attacks between 17 November and 17 December 2024 with a modified version of the Babuk ransomware, whose source code was leaked in 2021, and on the other, the FunkSec group, which appeared at the end of 2024, claiming 85 attacks world-

wide in December, more than any other group over the same period. The group reportedly consists of self-taught actors. They use artificial intelligence to create ransomware and phishing emails. Threat actors in the field have shown their adaptability, especially when it comes to incorporating recent advances in AI.

However, some changes were observed throughout 2024. The LockBit ransomware family was active in the first half of 2024. However, coordinated action by coordinated law enforcement action (Operation Cronos) weakened it, reducing the number of attacks in France for the rest of the year.

FOCUS

Bulletproof hosting

Bulletproof hosting is a technical infrastructure service equivalent to web hosting, but designed to support criminal activities such as malware hosting, sending mass phishing emails or hosting illegal content. This service is usually paid for in cryptoassets and is a profitable venture for operators. It offers anonymization services and facilitates criminal activities, in particular by hosting command and control (C2) servers, used for botnet management. The bulletproof hosting service will therefore provide a server for clients conducting illegal operations. Bulletproof hosting services can vary depending on location, pricing, reputation and content policies.

This type of hosting remains a cornerstone for a large number of cybercrime platforms and is a sustainable solution in countries where the legislation and international cooperation are insufficient. Regarding illegal activities, bulletproof server hosts can adopt a more or less active stance. They undertake to protect and anonymise the identities and communications of their customers and implement operational security measures. For instance, many services can be paid for in cryptoassets and the host invests in solutions that mask their customers' IP addresses and servers.



MODUS OPERANDI OF CYBERCRIMINALS

1 	Main methods of action	20
2 	Use of technology for malicious purposes	31
3 	Hybrid modus operandi	37

2 MODUS OPERANDI OF CYBERCRIMINALS

Cybercrime encompasses all criminal activities targeting or utilizing computer systems. It takes many different forms : data theft, fraud, account compromise, ransomware, and identity theft.

In 2024, these threats continued evolving, becoming more frequent, sophisticated, and evasive, particularly through artificial intelligence integration and cryptocurrency adoption. This section examines primary cybercriminal methodologies, in terms of their techniques, organisation and the tools they employ.

It also highlights the professionalisation of certain groups and the emergence of ready-to-use services accessible even to people with little experience. Understanding these dynamics is crucial for effective threat identification and adapt protection measures, whether you are a citizen, a company or a public authority.

1 | Main methods of action

Phishing

Phishing refers to deceptive techniques designed to obtain personal, professional, or financial data (e.g., login credentials, banking details, sensitive documents) through social engineering.

This phenomenon is constantly increasing and continues as the significant initial attack vector due to its simplicity and profitability. It was perfected in 2024 when cybercriminals began using artificial intelligence.

Beyond widespread fraudulent activities, this mode of action makes it possible to break into information systems, execute malware, exfiltrate data for publication, monetization, or intelligence gathering. Threat actors are primarily financially motivated.

With several hundred million phishing attempts a year, this type of attack represents a growing global threat and is essentially based on mass criminality.

Several trends have emerged in recent years:



- Criminals seem to prefer mass phishing campaigns, mainly by e-mail or via phone calls ;



- Smishing (SMS phishing) has been on the rise since 2024 : it involves employing brief yet compelling messaging, sent from messaging applications or telephony software. Imprecise notification of a parcel's whereabouts or, conversely, a brief but precise instruction from a supposed authority increases the likelihood that victims will click on the link ;



nepascliquer.courriel.com

- phishers use inventive techniques to ensure that documents attached to emails or website links are not detected as malicious or at risk ;



- vishing (voice phishing): also on the rise, these phone calls are now a daily occurrence, targeting the entire population. Threat actors continuously evolve their social engineering narratives and organizational impersonation tactics, such as fraudulent banking representative schemes. These operations typically involve caller ID spoofing of legitimate numbers ;



- Remote working environments present exploitable attack surfaces for cybercriminals ;



- The use of artificial intelligence is enabling malicious actors to set up phishing campaigns that are increasingly credible and difficult for victims to detect.

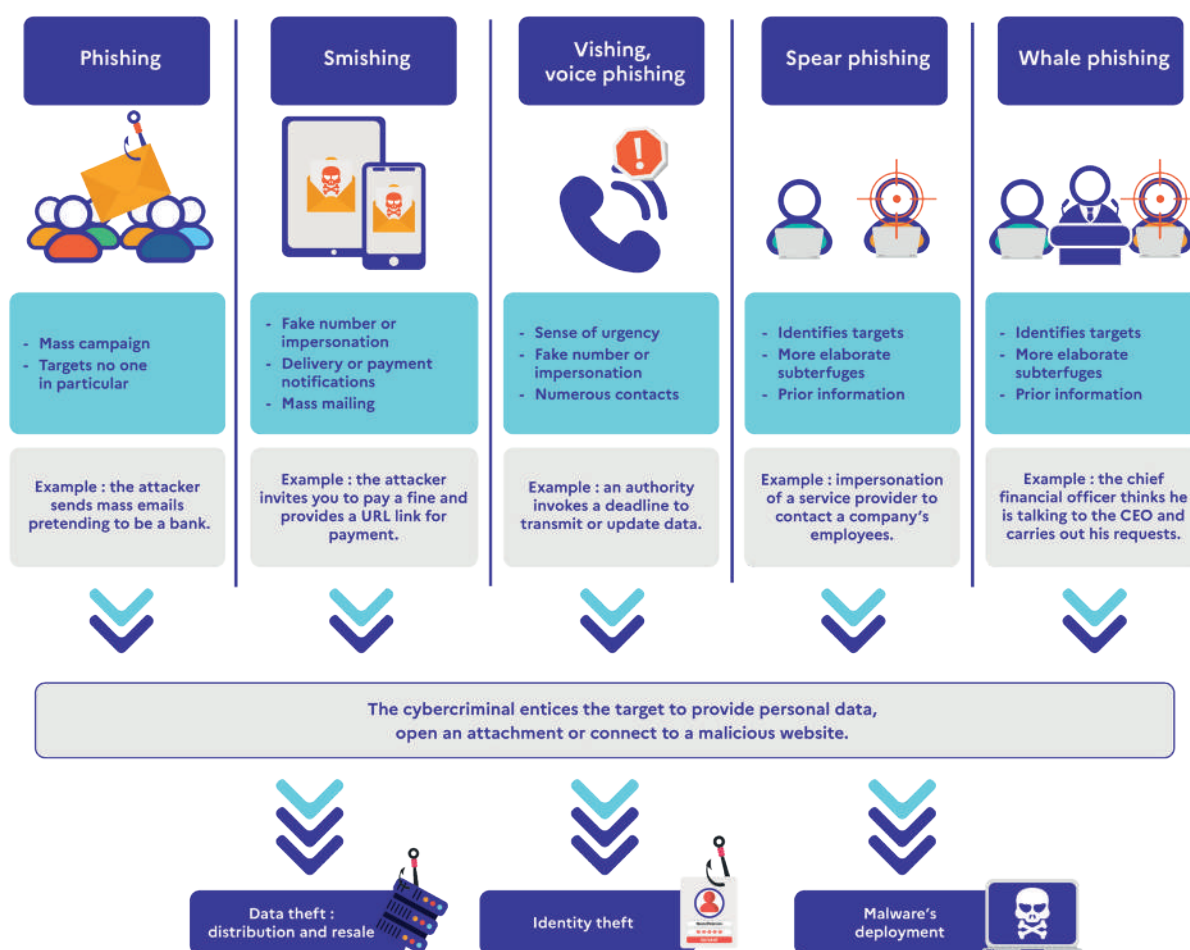
Human vulnerabilities remain the principal attack vector. Anyone in possession of devices capable of transmitting and receiving communications is likely to be the target of a fraudulent action.

Individuals, whether in a personal or professional capacity, are generally affected by untargeted and widely distributed phishing campaigns. Legal entities, through their employees, managers, service providers and customers, are more likely

to fall victim to targeted campaigns. A strategic person's digital footprint within a company is often the gateway to setting up a targeted phishing campaign (spear phishing).

Finally, these phishing campaigns, which use social engineering, can also be an entry point for cyber attacks on information systems, including ransomware deployment and data exfiltration.

There are various ways to mislead victims :



Typology of phishing methods

Digital identity theft (spoofing)

Spoofing is a method used by cybercriminals to impersonate as a legitimate organisation. This technique can be used to spoof several digital media, such as an email address, an IP address, a website or a telephone number. This modus operandi is particularly difficult to detect, since threat actors make spoofed credentials indistinguishable from authentic ones.

Cybercriminals use these techniques to establish a link of trust with their target, thereby gaining access to their systems or devices. Their aim is to steal information, financial extortion, or malware deployment on the victim's device.

Phone spoofing criminals manipulate their victims by exploiting their trust in the displayed caller ID. Telephone spoofing is mainly used to commit three types of crime: corporate number impersonation for executive fraud, fraudulent emergency calls (swatting attacks) and fake bank adviser fraud.



President fraud

Threat actors impersonate phone numbers to manipulate victims into disclosing sensitive data or authorizing financial transfers. More often than not, this involves impersonating a person whose functions are strategic for the company (a chairman, an accountant authorised to carry out financial transactions, a secretary with delegated authority, or a supplier or customer).



Telephone hoax (swatting)

Attackers use their victims' numbers and simulate emergency situations (shootings, violence) to trigger unnecessary intervention by law enforcement agencies, potentially resulting in serious consequences.



Fake bank advisor

Cybercriminals spoof a bank identification detail and simulate security alerts to obtain sensitive data, validate purchases or encourage bank transfers for the benefit of the attacker.

The modus operandi of cybercriminal networks specialising in telephone spoofing

Spoofing occupies an increasingly prominent place in the cyberthreat landscape, both because of its growing sophistication and because of its impact on legal cases, which it can make particularly complex. While spoofing is widely integrated into today's threats, its mechanisms and implications are generally poorly understood. Here are some key points to understand spoofing, with a particular focus on phone number spoofing.

To carry out attacks using spoofed telephone numbers, cybercriminals exploit legitimate tools designed to manage corporate telephone networks, whose uses they hijack.

Cybercriminals have built up a thriving economy around number theft, with a quasi-professional organisation that benefits from a brand image. They offer automated and customisable services, with simplified interfaces for choosing the number to spoof. They also apply structured pricing, including subscriptions and credits, which makes these tools accessible to even inexperienced users. This well-established organisation contributes to the spread of spoofing attacks, rendering these practices both accessible and effective.

Infostealers

Infostealers are malware designed to extract particularly sensitive data from infected devices, including credentials, financial information, browsing data, and personal information.

The use of this type of malware has increased sharply over the past few years, making it one of the most critical threats in 2024. Sold under

a Malware-as-a-Service (Maas) model via cyber-criminal forums and open discussion channels, these infostealers are accessible to individuals with few technical skills.

There are four steps to using infostealers :

Infection :

Infostealers penetrate systems via malicious attachments, hacked software or phishing links ;

Collection :

Following deployment, infostealers scan compromised systems for data extraction: IDs, passwords, cookies, cryptoasset wallets, bank cards etc;

Transmission :

The stolen data is sent to a server controlled by the cybercriminals, often through encrypted channels to avoid detection;

Exploitation :

Stolen data is used for fraud, resale, identity theft or as leverage for advanced attacks. It also feeds new phishing campaigns, perpetuating a cycle of compromise.

Impacts of an infostealers' attack :

For individuals

- Identity theft and usurpation of online accounts ;
- Direct financial losses (bank accounts, cryptoassets) ;
- Loss of privacy.

For organisations

- Compromise of information systems via stolen credentials ;
- Backdoor to more sophisticated attacks ;
- Leakage of confidential data and damage to reputation ;
- Costs associated with data breaches and regulatory non-compliance.

FOCUS

Operation Magnus⁵

October 2024's Operation Magnus targeted RedLine and META infostealer criminal infrastructure. Carried out jointly by several countries and coordinated by Eurojust, it led to the seizure of servers, domain names and Telegram channels used by these cybercriminal groups. Cybercriminal markets host numerous infostealer variants.

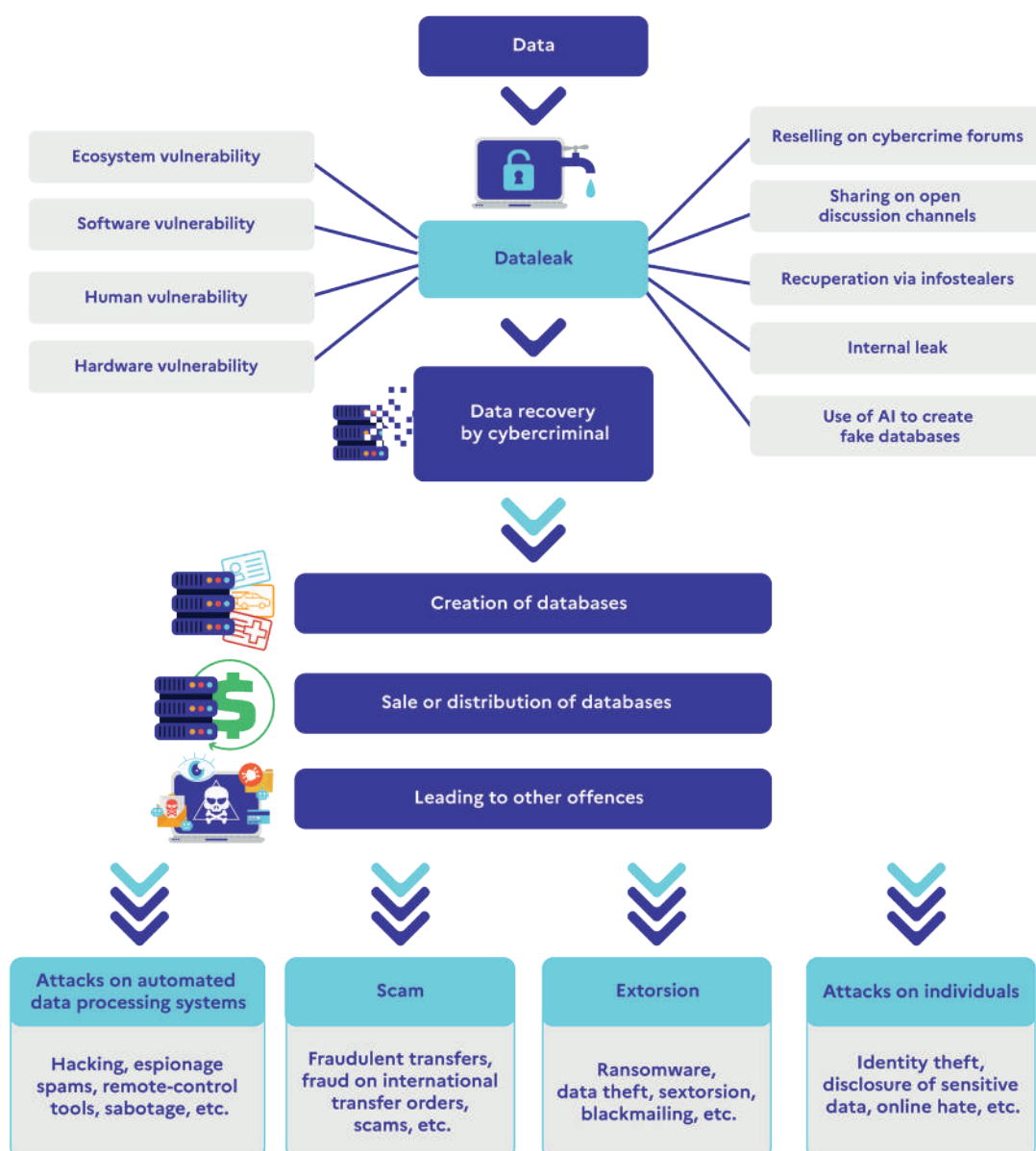
5. <https://www.eurojust.europa.eu/news/malware-targeting-millions-people-taken-down-international-coalition>

Data leaks exploitation

A notable cybercriminal phenomenon in 2024 was the exploitation of data leaks, whereby cybercriminals hack into databases, recover data, and then distribute or sell it on cybercriminal forums or discussion channels.

Exploitation of data breaches contain extensive information enabling cyberattack execution (hacking into servers or personal accounts, ransomware, espionage, etc.) or massive or targeted scams (fake investments, carding, fraud

on international transfer orders, etc.). Billions of data records are accessible online including credentials and passwords, personal and financial information, and can affect individuals as well as businesses and public authorities. A substantial portion of this data results from compromise of inadequately secured servers or the infection of devices by infostealers.



Modelling the exploitation of data leaks

As part of ransomware attacks, data stolen from victims' information systems is sometimes made available on 'dataleak sites', commonly referred as 'walls of shame'. These are sites or blogs hosted mainly on the darkweb where stolen data from

organisations that refuse to pay the ransom is published. In 2024, the Ministry of the Interior's Cyberspace Command (COMCYBER-MI) recorded 235 claims relating to data theft from French victims.

Threat actors

The theft and sale of fraudulently acquired data attracts several types of cybercriminals :



A rookie malicious actor who, seeking to increase their reputation by recycling databases obtained in previous releases or generating fabricated datasets using AI. They act opportunistically by either monetising this information or claiming responsibility for its theft.

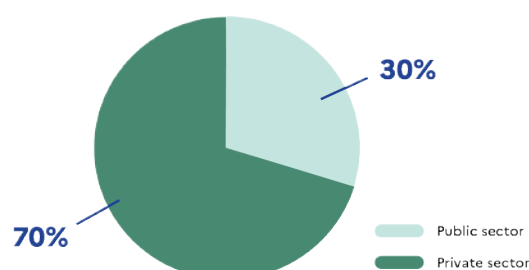
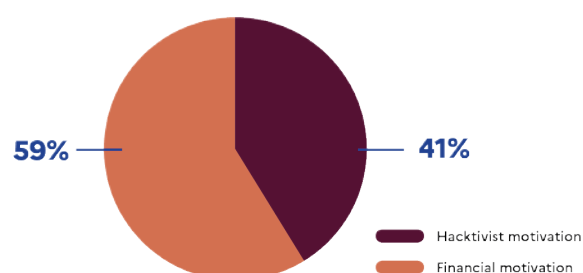


An experienced threat actor who has mastered intrusion techniques and operates alone or as part of a group. Some individuals may act out of defiance or for personal satisfaction. Unpredictable by nature, their motivations differ as much as their technical skills.

Threat actors are motivated by a variety of factors. The primary motivation is financial gain. The resale of collected data is a potentially lucrative activity, based on data sensitivity and scarcity.

Hacktivists also steal data. The aim is to damage the reputation of organisations or countries targeted in attack campaigns. These operations generally take place within opportunistic alliances formed by groups taking advantage of a mass effect and the technical capabilities of each.

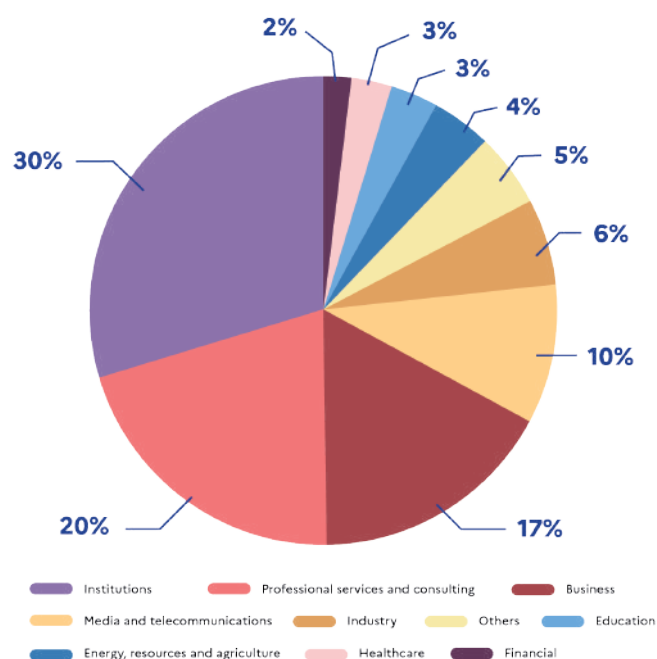
Finally, data breaches may result from other, less common factors : personal motivation, insider revenge, or negligence. Unintentional exposure of data resulting from accidental dissemination on the Internet, loss of storage devices by employee or a poorly configured security system, has potentially critical impacts.

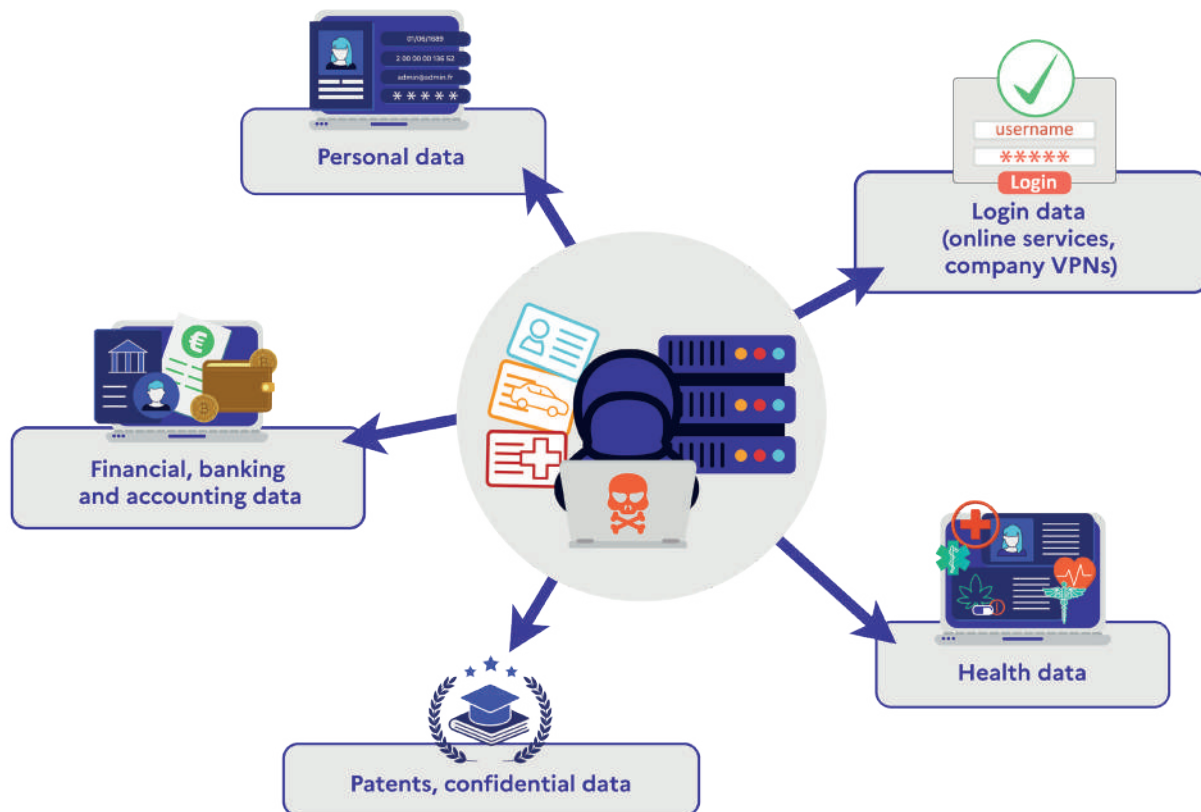


Economic sectors and types of data targeted

Based on documented cases of data exposure in cyberspace during 2024 monitored by the Ministry of the Interior's Cyberspace Command, no economic sector has been spared from this phenomenon.

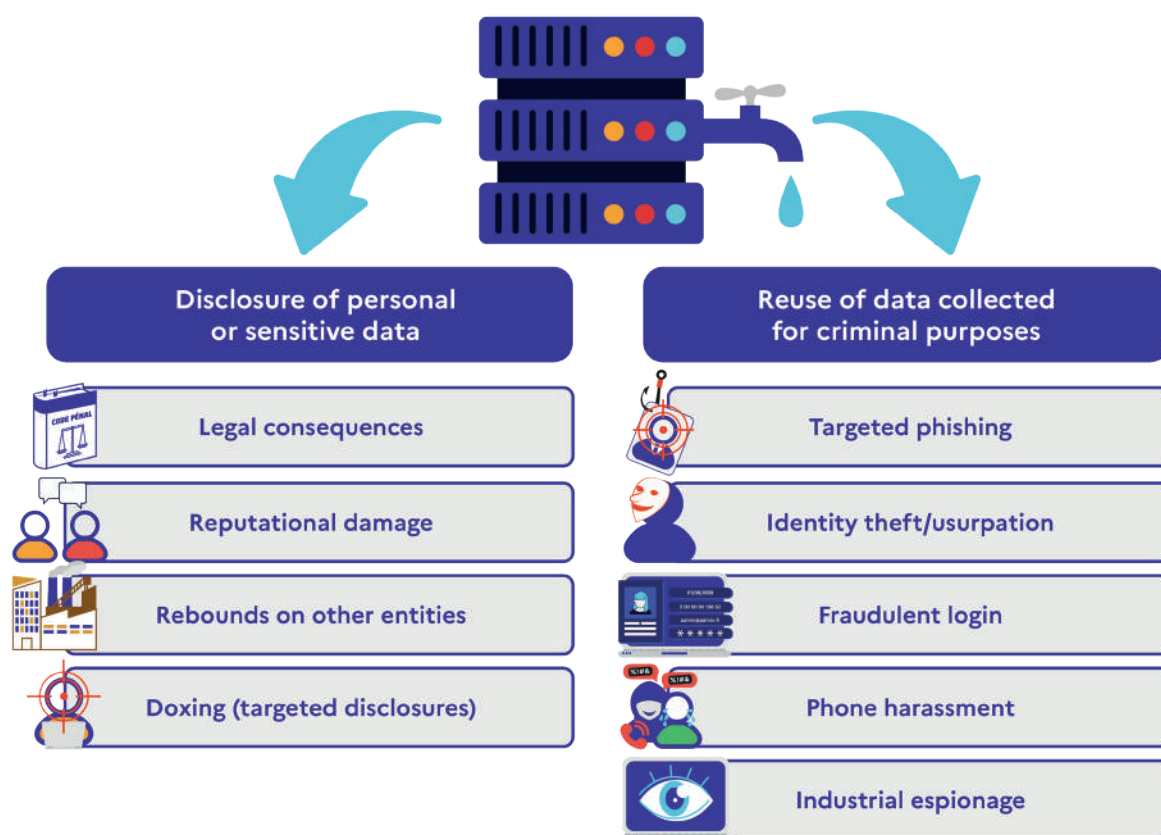
Nonetheless, government departments and public administrations appear to be prime targets, accounting for 30% of all claimed data leaks. The types of data leaked vary depending on the target (public administrations, public companies, online businesses, telecommunications, insurance companies, etc.).





Typology of stolen data

The consequences of a data leak can be manifold, impacting targeted organisations, customers and users, as well as partners in the supply chain.



Exploitation of data by threat actors

Ransomware

Ransomware can be defined as malware that denies access to systems or files through data encryption and demanding ransom payment for data decryption.

Ransomware attacks are carried out by organised cybercriminals with protean and evolving structures. One of the business models developed is Ransomware-as-a-Service (RaaS). This model provides malware, tools and expertise to

affiliates in exchange for a percentage of ransom payments. This system enables complex cyberattacks, even for individuals with a moderate technical level.

In Europe, nearly half of all ransomware attacks target small and medium enterprises (SMEs), which then struggle to maintain their activity, at the risk of going bankrupt.

Typology of attacks and modus operandi

Cybercriminal groups that specialise in ransomware generally have a similar approach to the modus operandi for their cyberattacks. There are, however, variations and characteristics that are unique to them, allowing them to be differentiated, beyond the names of the ransomware strains they use. The year 2024 marked a turning point in the composition of malicious groups, primarily due to coordinated action by law enforcement agencies, which led to the arrest of several individuals.

It should be noted that, although groups are distinguished by the name of the ransomware they use (e.g. LockBit, 8Base, RansomHub and Qilin), cybercriminals are not always exclusively associated with a single group. Some cybercriminals administer or use several different types of ransomware aimed at different targets simultaneously.

Various methods coexist and complement each other to reach victims:



Big game hunting :

This consists of highly technical targeted attacks on large organisations with high levels of resources.



Mass attacks :

Opportunistic attacks on vulnerable targets.

There are various techniques for infiltrating a victim's information systems :



- **Through initial access brokers** who provide hacked computer access to companies from cybercriminal forums.



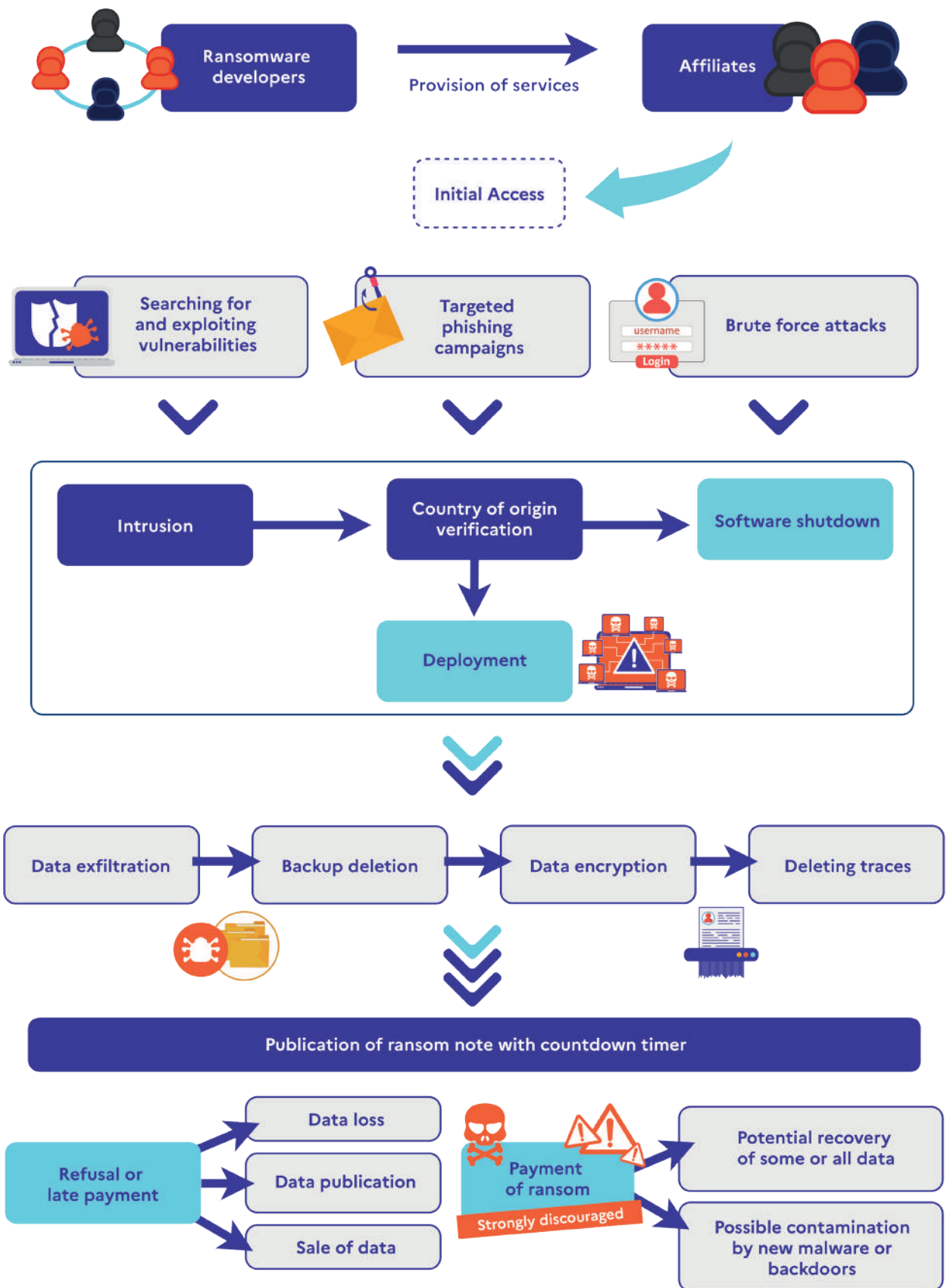
- **Supply chain attacks** : via supposedly less protected subcontractors who provide indirect access to the targeted company.



- **Social engineering** : using manipulative or deceptive techniques to trick the victim into providing data or performing actions at the attacker's instigation.



- **Use of employees of an organisation (insiders)** acting out of financial opportunism or a desire to cause harm.



Modelling a ransomware cyberattack

The most common technique used by active ransomware groups is the double extortion, ahead of the more recent triple extortion :

Double extortion : technique involving the encryption of stolen data, which cybercriminals then threaten to distribute via their platform or open discussion channels

Triple extortion : this technique has become very widespread over the last three years. In this method, data encryption and the threat of online publication are combined with business and network disruption through a distributed denial of service (DDoS) attack.

Some groups only ransom victims by threatening to release their data, without even encrypting the servers. The ransom demand sent to the victim is always accompanied by threats to sell or disclose information.

In 2024, a new modus operandi was observed was the use of two countdowns displayed on the cybercriminal group's darkweb page. For example, one countdown threatens to sell the data within three days, while another threatens to disclose the data for free within seven days.

Each group or affiliate is free to act using sophisticated and unique methods. These techniques are designed to exert psychological pressure on victims, putting them in a state of shock and resignation so that they agree to pay the ransom, which is usually paid in cryptoassets.

Additionally, cybercriminals adjust the amount demanded to the target's estimated ability to pay the ransom. In this way, victims would theoretically be able to pay.

FOCUS

Initial access brokers

Initial access brokers are malicious actors who specialise in identifying vulnerabilities that enable them to gain initial access to the victim's computer network. They then resell this access to other groups who carrying out cyber attacks, such as data exfiltration, ransomware, etc.

Profits can be paid out as a fixed sum by buying access or as a commission once a ransom has been paid for the cyber-attack.

This type of organisation illustrates the level of specialisation and structuring of the threat. Some cybercriminal forums specialise in resel-

ling of such access, with a system for rating users. More often than not, these 'brokers' obtain access to victims' networks by exploiting computer vulnerabilities, stealing credentials via infostealers or targeted phishing campaigns. In most of the sales observed, the access is offered in the form of remote RDP or VPN access, or access to a target's cybersecurity solution, in particular its firewall. These accesses can be sold for amounts ranging from a few hundred euros to several tens of thousands of euros, depending on the type of vulnerability or the profile of the target.

Botnets

Botnets are networks of digital devices connected to the Internet (such as computers, servers, connected objects, etc.), infected and controlled by cybercriminals using remote control servers (command & control).

Some botnets can consist of several million infected machines and are considered to be computer weapons.

Botnets can be a medium for several types of cyberattack :



DDoS attack :

Overload servers with network traffic from a multitude of infected systems to the point of making the service unavailable ;



Malware propagation :

Infecting systems to spread across networks and devices ;



Brute force credential stuffing :

Automatically executing programmes that force authentication by exploiting known connection data ;



Cryptomining :

Fraudulently hijacking a computer and its computing capacity to mine crypto-assets in the background.

Set up by cybercriminal groups with advanced technical expertise, botnets are also offered for hire as part of cybercrime-as-a-service. Platforms are managed to make these criminal tools available in exchange for payment.

This phenomenon can be particularly lucrative for its administrators, but some attacks are motivated by ideological factors.



Modelling how a botnet works

2 | Use of technology for malicious purposes

Criminal actors exploit legitimately developed technologies, but which are misused by cybercriminals to enhance their cyberattacks.

This is particularly true of artificial intelligence and cryptocurrencies.

Artificial intelligence : criminal innovations

Artificial intelligence offers new opportunities for criminals to increase both the number and effectiveness of cyber attacks. Deepfakes, which enable the creation of highly realistic audio and visual content, have rapidly found their way into the arsenal of cybercriminals.

Cybercriminals are exploiting AI to automate and intensify their malicious activities. Large language models are used to write highly convincing phishing emails or compromising videos, tailored to the behaviour and/or profile of the victims. These models open up new criminal opportunities, making it possible to bypass the protection

of information systems and human vigilance by generating unprecedented attacks. This evolving threat landscape places law enforcement in an asymmetric confrontation.

AI tools themselves are also the target of attacks. One of the most common methods is data poisoning, attacks that contaminate training datasets, thereby either completely compromising model outputs or manipulating predictive behaviors of the trained model. It is then possible to corrupt the model and its classification, detection or prediction capabilities.

Deepfakes, a rising threat

Deepfakes are forged content (video, audio, photos) capable of reproducing a person's appearance or voice with disconcerting realism. In 2024, this technology became widely available, enabling malicious individuals to create falsified content used for criminal purposes.

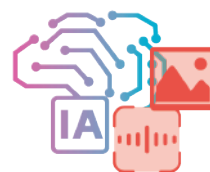
A deepfake can be produced using various techniques :



Replacing the face of one person with that of another in existing content (face swap) ;



Using of existing content to make an individual say fictitious things (facial reenactment) ;



Creating content entirely AI-generated, including the image and/or voice of an individual, without relying on pre-existing images or videos (full synthesis).

8. Large Language Model (LLM), Vision Language Model (VLM), Large Action Model (LAM)

Deepfakes, what are they used for ?

Disinformation

The creation of misleading content can be used to influence opinions, disrupt democratic processes or sow media confusion. The 2024 Olympic Games in particular were the scene of this type of attempts.

Frauds and scams

Cybercriminals use them to steal identities and deceive individuals and organisations.

Reputation harm

Deepfakes are used to generate defamatory content, sometimes of a graphic nature, used against targets for extortion or reputational destruction.

Every day, it is becoming more difficult for the general public to tell the difference between deepfakes and authentic content. Existing detection tools, while effective in some cases, are struggling to keep pace with the rapid development of algorithms.

Consumer applications and dedicated deepfake-as-a-Service (DFaaS) platforms have emerged, enabling anyone to create deepfakes without any technical skills, making it easier to use them for malicious purposes.

New phishing strategies and assistance to cybercriminals

AI-enhanced phishing

Phishing, an attack in which victims are duped by fraudulent e-mails or messages, has reached a new level of effectiveness thanks to AI in 2024. Using publicly available data (social media profiles, information from data leaks), cybercriminals rely on AI to generate personalised

and credible emails, impersonating trusted organizations.

The adoption of AI makes detection more difficult and increases the success rate of large-scale phishing campaigns.

Keys examples :



Mass AI phishing :

Automated generation of thousands of personalised phishing emails imitating various institutions, with intelligent adaptation according to victims' responses.



Spear phishing :

Personalised email based on AI analysis of the public professional data of a decision-maker within an organisation, incorporating precise references to their sector and projects.



Vishing :

Fraudulent call using a synthesised voice from a hierarchical superior to request an urgent transfer to an account held by the cybercriminal.

Assistance to cybercriminals

Large Language Models (LLMs) optimise cybercriminal activities, turning rookies into malicious actors and enabling experts to expand their scope.

Examples of assistance :



Creation of operating scripts :

Automatic generation of malicious scripts to target known or emerging vulnerabilities.



Accelerated code analysis :

Analysis of large code bases to find flaws faster than a human.



Malware adaptation :

Help in modifying existing malware code to make it compatible with new targets.

Potential and limitations

Autonomous programmes (agents) based on LLMs are already succeeding in executing complex cyber attacks with a high success rate.

These agents, designed to interact with third-party softwares and execute commands, exploit documented vulnerabilities to carry out malicious actions. However, their performance drops drastically when this information is missing.

To date, it remains difficult to accurately assess the maturity of these practices within the cyber-

criminal ecosystem, as well as the actual proportion of automation by AI in cyberattacks. Nevertheless, both the level of performance and the number of AI attacks are certain to increase.

Artificial intelligence therefore offers great prospects for cyber criminals. Fortunately, AI is also a weapon capable of reacting effectively and swiftly in the fight against cybercrime.

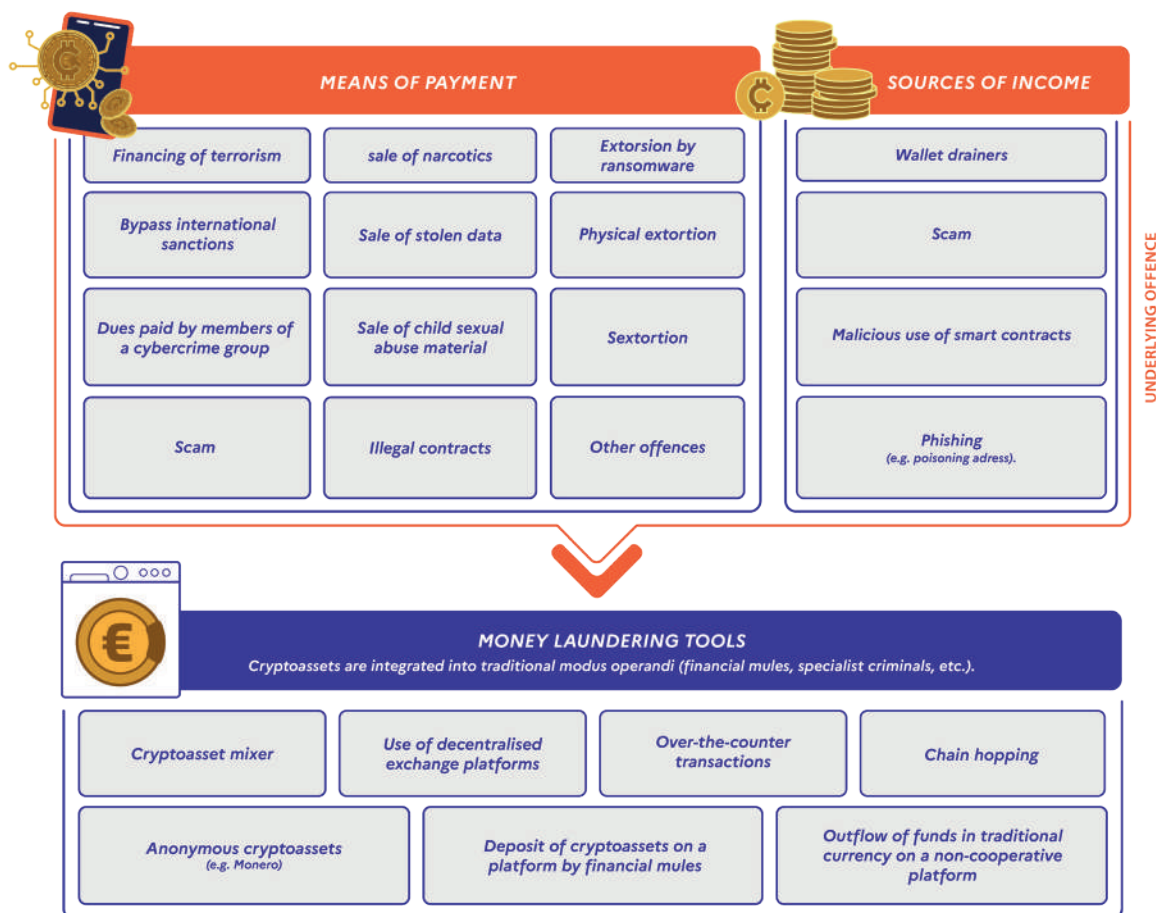
Cryptoassets and cybercrime

The use of cryptoassets by cybercriminals has grown significantly over the last ten years : financing denial-of-service cyberattack campaigns to disable websites, paying a ransom in the event of a ransomware attack, or making payments on cybercriminal forums (purchase of databases, malware, drug trafficking, etc.).

While most cryptoasset transactions are lawful, cryptocurrency facilitates illicit transactions

worth billions of dollars annually, a significant proportion of which are used for money laundering.

Their use for illicit purposes can be classified into three main categories: as a means of payment, as a direct source of income or as a money laundering tool.



Types of illicit use of cryptoassets

Cryptoassets as a means of payment :

The most widely traded cryptoassets, such as Bitcoin (BTC) and stablecoins, can be opportunistically used to commit a wide range of crimes. Sometimes, as a complement to the traditional financial system, they facilitate narcotics trafficking and commercialization of compromised data and as a means of payment.

These illicit transactions occur primarily on underground marketplaces. Cryptocurrencies also enable monetization of child sexual abuse material.

In the case of coordinated distributed denial of service (DDoS) or ransomware attacks, cybercriminal groups can collect funds from their affiliates.

Cryptoassets as a source of money laundering :

In terms of money laundering, criminals have rapidly incorporated emerging technologies into the range of tools at their disposal. To conceal the illegal origin of funds, they are able to combine cryptocurrency mixers (that obfuscate fund origins through multiple fragmented transactions across numerous addresses), instant exchangers (which allow funds to be converted between two cryptoassets) and cryptoassets enabling anonymised transactions such as

Monero (XMR).

In addition to these processes, blockchain analysis transactions show that criminals know perfectly well how to transfer their funds from one blockchain to another (chain hopping) to hide their operations. When cryptoassets are exchanged for traditional currency in the final stage of money laundering, the criminals choose countries where the exchange platforms do not cooperate with the authorities.



Modelling drug laundering using cryptoassets

Cryptoassets related scams

2024 has seen a sharp increase in scams involving cryptoassets, which can be used as a pretext, as a means or as the actual object of the offence.

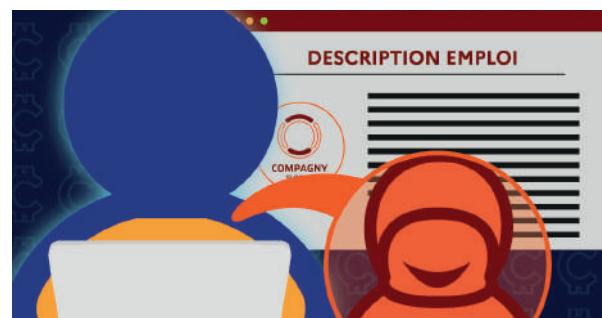
One of the most common *modus operandi* is fake investment. This method involves collecting funds from the victim under the pretext of investing the money on their behalf in one or more cryptoassets. The criminals present themselves as professionals and go so far as to impersonate legitimate cryptoasset exchange platforms, some of which are well-known.

The scammers promise high returns to win the trust of their victims. In the most sophisticated cases of social engineering, a website or even an application will display the amount of funds 'invested' by the victim, who will then be able to see their 'gains' and be inclined to invest more. The victim eventually loses confidence and realises the scam when they are unable to withdraw their funds on various pretexts (withdrawal fees, taxes, wallet security, computer bugs, etc.).



Fake romance scam :

These schemes exploit emotional manipulation within fabricated romantic relationships to defraud victims of cryptocurrency. This method can opportunistically combine psychological manipulation and fraudulent investment schemes : using a messaging application, a social media or a dating application, the scammer establishes contact, typically through fabricated accidental messaging, to establish a long-distance relationship with the aim of collecting funds. Transactions can be made by the victim under various pretexts (medical expenses to be paid, an irresistible investment opportunity, etc.).



False employment scam :

This involves exploiting the victim's greed and/or lack of financial resources. Contact is made via a messaging application by an unknown person offering an online job : simple tasks are requested of the victim, such as evaluating products on a merchant site or sharing advertisements, for which they are promised payment. Payment collection requires upfront cryptocurrency transfers under fabricated justifications.



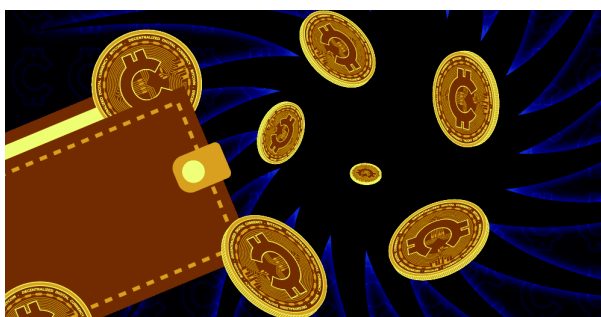
Cryptoasset scams

In some cases, the aim of the offence is to steal the victim's cryptoassets. Although often simplistically associated with cryptoasset theft, wallet drainers and smart contract schemes

Creation of tokens or memecoins :

On a dedicated blockchain, such as Ethereum and Solana, this process leads many gullible victims to 'invest' in cryptoassets that have no fundamental value. In many cases, project creators can artificially inflate the price of assets to attract victims and then suddenly liquidating their holdings.

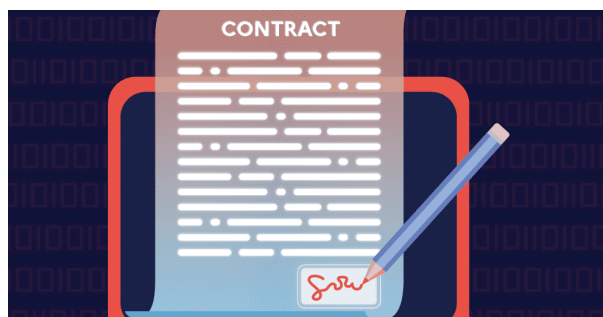
are, strictly speaking, techniques designed to deceive the holder of the funds and then stealing their cryptoassets and are therefore a technically advanced form of fraud.



Wallet drainer :

This is a set of manoeuvres designed to obtain permission to empty the victim's cryptoasset wallet (in the technical sense, i.e. one or more public addresses on a blockchain). It takes the form of a deceptive smart contract, which misleads the user.

Like a legitimate smart contract, this is a programme that automates one or more transactions if a condition is met, for example the gift of tokens allocated as a reward for an action (airdrop) or the granting of a non-fungible token after participation in an event (proof of attendance).



Smart contracts exploitation :

Decentralised finance (known as DeFi) is an ecosystem within cryptoassets that aims to recreate an open financial system. It is based on a set of smart contracts. Some protocols can manage hundreds of millions or billions of cryptoassets within their smart contracts. An error in the code of a protocol or manipulation through social engineering can enable malicious actors to steal all or part of it. In 2024, more than \$2.2 billion is believed to have been stolen as a result of exploiting flaws in smart contracts or directly on a blockchain.

FOCUS

Use of cryptoassets by drug traffickers

Cryptoassets can be used to broaden sources of revenue and to develop the methods used by organised crime groups to buy, sell and launder money, particularly in the drugs trafficking sector. Narcotics products can already be sold 'retail' in cryptoassets, across cybercrime forums, messaging platforms, and mobile applications.

It is likely that this phenomenon will follow the growth of the cryptoasset sector and its adoption by more and more users. Upstream, the 'wholesale' trade in narcotics is significantly conducted in stable cryptoassets (stablecoins).

3 | Hybrid modus operandi

While cybercrime takes place in digital space, its effects can sometimes be felt in the real world.

This demonstrates the escalation from digital exposure to physical threat, such as the violent extortion of cryptoassets, the sabotage of digital infrastructure or malicious disclosure of personal

information (doxing). These trends reflect the increasing porosity between the digital sphere and the real world. They also illustrate the evolution of threats towards more violent, ideological or destabilising approaches.

Physical extortion of cryptoassets

Cryptoassets holders are being targeted by certain organised crime groups who use violent methods to extract cryptoassets from their victims (kidnapping, physical threats, torture, etc.).

While the phenomenon has already been observed at blockchain conferences and events abroad, it is making gaining traction in France,

as criminals use new digital means to identify their targets.

High-profile individuals and industry veterans (influencers, leaders of cryptoasset platforms, etc.) are targeted due to their perceived wealth, the speed with which a cryptoasset ransom can be paid and sometimes a lack of discretion.

Sabotage of network infrastructure






Although less visible and less publicised in the media, the physical sabotage of network infrastructure is a critical threat, particularly given today's high level of digital dependency. These attacks are aimed directly at the physical equipment essential to the operation of society's communication networks and information systems. The stakes of such a threat are multiple :

- Geopolitical : sabotage can be used as a tool of hybrid warfare ;
- Economic : it can generate significant financial losses ;
- Ideological : sabotage can be a vector used to promote an ideology or a means of expression for hacktivist groups ;
- Security : these actions can undermine security (interruption of sensitive communications, emergency services, vital sectors, etc.).

The methods used vary depending on the target but generally involve physical or digital damage to property (vandalism, destruction, fire, etc.). Threat actor profiles span multiple categories, including hacktivist and criminal groups.

Sabotage impacts the target infrastructure, as well as all the services associated with it: communication services, Internet services, essential services, etc.

It is therefore a growing threat, particularly to critical infrastructure, and requires monitoring and redundancy of systems to limit the impact on essential services.

TARGETS	Critical infrastructures 	5G antenna 	Relay antenna/optical fibre 	Submarine cables 	Data center 
MODUS OPERANDI	<ul style="list-style-type: none"> • Fire • Destruction • Vandalism • Intrusion 	<ul style="list-style-type: none"> • Fire • Destruction • Vandalism 	<ul style="list-style-type: none"> • Fire • Destruction • Vandalism 	<ul style="list-style-type: none"> • Damage • Destruction 	<ul style="list-style-type: none"> • Fire • Intrusion
IMPACTS	Unavailability, disruption or interruption of service, personal injury	Unavailability, disruption or interruption of service	Unavailability, disruption or interruption of service	Unavailability, disruption or breakdown of international communications	Loss of data, unavailability or interruption of hosted services

Modus operandi used to sabotage network infrastructure

Personal information disclosure (doxing)

When it comes to harming people, certain cyberattacks can go beyond the purely digital spectrum and have effects on the physical dimension and on individuals. This is notably the case with doxing, a practice that takes place exclusively in the digital domain, but whose impact sometimes takes the form of physical harm (harassment, assault, etc.).

Doxing is a phenomenon associated with cybers-talking : this attack consists in disclosing or distributing personal information, such as a person's surname, first name, contact information, residential and workplace addresses, in order to harm them, their family or even their property. The term derives from 'documents' combined with 'dropping', alluding to the act of sharing information. The offence of doxing has been punishable under the French Penal Code since 2021.

However, the phenomenon is not new : doxing was first observed in the cybercriminal com-

munities in the 1990s. Indeed, this method was observed in the context of rivalries between cybercriminals, compromising the anonymity of these actors

To this day, threat actors continue to dox one another, usually out of revenge or rivalry.

However, doxing has expanded beyond the cybercriminal world and now applies to a wide range of use cases. Doxing is generally used by young people, and the information is posted on social media or platforms specifically designed for personal information disclosure, as part of a cyber-stalking campaign.

Doxing is also popular with hackers, who use this mode of action for ideological reasons. These actions can be part of international conflicts where actors wish to destabilize or endanger people. In the Russia-Ukraine conflict, for example, doxing is frequently used to destabilize opposing forces.

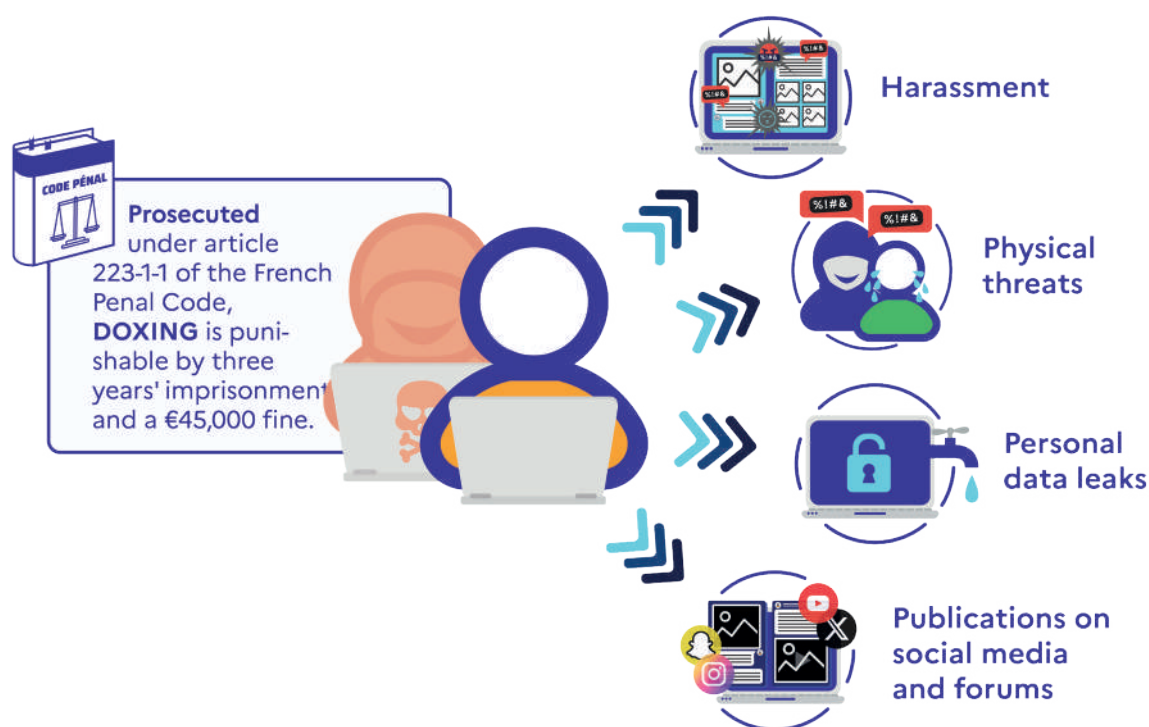
In the same way, cybercriminals disclosed the identities of Israeli athletes on online discussion channels during the Paris 2024 Olympic Games. Individuals affected are experiencing a shift from digital risk to physical risk.

Raising ethical questions, doxing is sometimes practised by individuals who think they are acting morally and who will dox individuals they perceive as deviant or criminal. Certain groups or isolated individuals, for example, work to dox suspected child sexual offenders as vigilante justice, believing they are assisting active investigations. However, this phenomenon often hinders these

investigations and contributes to the commission of crimes and offences such as the distribution of child sexual abuse material and physical assaults, sometimes on misidentified individuals.

Although the phenomenon is still difficult to quantify and qualify, doxing is becoming widespread in the cybercriminal sphere and has evolved into ideologically-motivated activity.

To counter this phenomenon, it is crucial to educate users about their exposure risks by sharing their personal data online. Encouraging them to practice consistent operational security can help mitigate the risks of data leaks.



Doxing modus operandi



MAJOR INVESTIGATIONS AND LEGAL DEVELOPMENTS

1 Legal developments	42
2 Major investigations feedback (OFAC, UNCyber et BL2C)	44

3

MAJOR INVESTIGATIONS AND LEGAL DEVELOPMENTS

1 | Legal developments

Cybercrime is constantly reshaping the contours of traditional crime. To address digital transformation challenges, the European Union has adopted a number of legislative texts aimed at strengthening security and providing a framework for emerging technologies.

Three major regulations illustrate this commitment :

- The NIS2⁹ directive, which strengthens cybersecurity in critical sectors and imposes new obligations on businesses and administrations ;
- The AI Act¹⁰, which establishes a legal framework for artificial intelligence based on its level of risk ;
- The MiCA¹¹ regulation, which aims to regulate cryptoassets and protect investors.



NIS2 Directive: strengthening cybersecurity

Adopted in January 2023 and coming into force on 17 October 2024 at European level, the NIS2 Directive aims to strengthen cybersecurity by extending its scope to critical sectors such as public administrations, local authorities and the space sector. It imposes greater obligations on sectors already covered, including banking, healthcare, energy, transport and cloud services.

A minimum of 15,000 entities in France would be affected, classified into two categories : essential entities (EE) and important entities (IE), according to their field, size and annual revenue.

The directive imposes technical measures (infrastructure protection, encryption, audits, back-ups) and human measures (compulsory training). Cyber incidents must be reported within 72 hours (24 hours for the most serious events), with detailed reports. Non-compliance penalties can reach €10 millions or 2% of worldwide revenue. The French National Agency for the Security of Information Systems (ANSSI) is overseeing these regulations and has set up a dedicated online space: MonEspaceNIS2 (monespacenis2.cyber.gouv.fr).



AI Act: supervising artificial intelligence

The legal framework for AI has recently evolved with the arrival of the AI Act. This regulation, which came into force on 2 August 2024, is a key challenge for security forces, to prevent any asymmetry between criminal possibilities and the capabilities of law enforcement agencies.

The AI Act regulates AI by use cases, to which it assigns a level of risk. It classifies systems according to four levels of risk :

- Unacceptable risk : prohibition of dangerous uses such as social scoring ;
- High risk : strictly supervised use, particularly for biometric surveillance ;

- Specific risk : compliance requirements in terms of transparency and data quality ;
- Minimal risk : simple obligation to inform users.

The text provides for European governance with the creation of an AI Office and imposes penalties of up to 7% of global revenue or €35 million.

Implementation will be spread out over the period up to 2026, taking care to combine ethics and innovation.

9. Network and Information Security

10. Règlement européen sur l'IA

11. Markets in CryptoAssets

MiCA Regulation: a framework for cryptoassets

In force since 30 December 2024, the MiCA Regulation aims to regulate the cryptoasset market and protect investors.

It distinguishes three categories of cryptoassets:

- Utilities : provide access to a service ;
- Backed by an asset ;
- Pegged to fiat currency.

NFTs¹² remain outside the scope of the regulation, unless specific criteria are defined by ESMA (European Securities and Markets Authority). Virtual assets service providers (VASPs), such as exchange platforms and digital wallets, must now obtain a European authorisation to operate.

The text strengthens consumer protection by imposing a right of withdrawal and clear information. It prohibits fraudulent practices such as insider trading and market manipulation, bringing the regulation of cryptoassets into line with stock market rules.

These three regulations reaffirm the European Union's desire to make the digital world safer, while providing a framework for innovation and strengthening user confidence. They imply major investments for businesses, local administrations and government departments to build a secure and innovative European digital ecosystem.

The fight against cybercrime : constantly evolving regulations

Two recent court rulings have significantly impacted on the legal framework for cybersecurity and personal data protection in Europe. They concern the use of digital data in judicial investigations and the use of information accessible on the Internet.

CJEU, Gr. Ch. 4 October 2024 (Case C-548/21)

The Court of Justice of the European Union (CJEU) has laid down a strict framework for the use of data contained in a mobile phone during a judicial investigation. According to this ruling, authorisation from a judge or an independent authority is now required to access mobile phone data, except in cases of justified urgency such as an imminent risk to public security or a terrorist threat.

This ruling overturns current practice in France, where in some cases the public prosecutor could authorise such access without independent judicial review. From now on, investigators must inform the owner of the telephone as soon as possible, unless this would compromise the ongoing investigation.

This reversal could have an impact on investigations of flagrancy, which are conducted under the authority of the public prosecutor, who is not a judge and therefore does not enjoy the guarantees of independence required by the Court of Justice of the European Union (CJEU). Adjustments to the French Code of Criminal Procedure will be necessary to comply with this case law.

Cassation Crim, 30 April 2024, no. 23-80.962

This decision by the French Court of Cassation (Supreme Court) concerns the collection of open-source information on the Internet. The Court ruled that the fact that data is publicly available online does not mean that it can be exploited without a legal framework.

In this case, a private investigator, commissioned by a company's security director, had collected personal information from social media and public databases in order to profile individuals, without informing them. The Court ruled that this collection was unfair and unlawful because it was carried out without the knowledge of the individuals concerned and for a misappropriated purpose.

This decision is a reminder that transparency and fairness are essential when it comes to the processing of personal data. Even if information is freely accessible online, its use must comply with the principles of the General Data Protection Regulation (GDPR). Any collection of personal data must be carried out with the consent of the person concerned or within the strict framework defined by law.

¹² Non Fungible Token

2 | Major investigations feedback (OFAC, UNCyber and BL2C)

OPERATION CRONOS (LOCKBIT)



Appearing at the end of 2019 initially under the name ABCD



Developed using the Ransomware-as-a-Service model



300 complaints from French victims recorded by the end of 2024



More than 7,000 successful cyber-attacks between June 2022 and February 2024



Targets all types of entities: hospitals, local authorities, transport, etc.



Billions of euros worth of damage, and hundreds of millions of dollars held to ransom.

Facts and events :

Active since 2019, the ransomware group has targeted numerous companies, hospitals and public administrations in France and around the world.

The investigation :

In 2020, section J3 of the Paris public prosecutor's office opened an investigation, led by the National Gendarmerie. An international taskforce was set up, including France, under the coordination of Europol and Eurojust. In February 2024, Operation Cronos neutralised part of the criminal group's network. This action targeted the servers used to deploy the ransomware and the associated financial flows, while identifying several individuals involved in its operation.

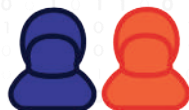
KEY RESULTS OF THE INVESTIGATION



34
servers seized



More than 200
cryptoasset
accounts frozen



2 individuals
arrested



Sanctions against the administrator LockBitSupp, including the freezing of criminal assets

THE MAIN ACTORS IN INTERNATIONAL COOPERATION



AN INTERNATIONAL RESPONSE

- In 2020, an investigation was opened by the J3 section of the Paris public prosecutor's office. The investigations were entrusted to C3N, now the operations division of the Cyber National Unit ;
- An international taskforce was quickly set up, which led to the arrest of an affiliate in Canada in October 2022 ;
- In February 2024, an international operation called Cronos, led by France and coordinated by Europol, disrupted the LockBit group's operations ;
- The operation was successful thanks to the cooperation of 14 countries around the world.

OPERATION ENDGAME



Launched in May 2024, operation Endgame aimed to dismantle several botnet networks used to spread malware on a large scale. Several botnets were decommissioned, including IcelD, Smokeloader, Pikabot and BumbleBee. Involved in cybercrime campaigns affecting millions of systems worldwide, these infrastructure were used to deploy ransomware and exfiltrate sensitive data. These cyber attacks had a direct impact on critical sectors, including healthcare establishments. Coordinated by Europol and Eurojust, the investigation mapped the command and control (C2) infrastructure of the botnets and identified the main operators involved. The authorities traced the financial flows associated with these criminal activities, uncovering money laundering circuits via cryptoassets.

OPERATION'S RESULTS



More than 100
servers seized



99 cryptoasset wallets
containing more than €70
million frozen



Four suspects arrested,
including three by the
French authorities



16 searches
carried out



Seizure of over 2,000
domains linked to the distribution
of malicious software



10 international
arrest warrants issued

STAFF ENGAGED

Coordinated by the Cybercrime Bureau of the National Police (OFAC), this investigation was the subject of a joint referral by the National Court for Combating Organised Crime's cybercrime unit (J3), the BL2C and the UNCyber.



- Identification of the SystemBC administrator.
- Mapping of infrastructure in collaboration with ANSSI.
- Coordination of the dismantling of dozens of control servers.



- Identification of a key actor in the BumbleBee dropper.
- Cooperation with the Armenian authorities to interview an individual and conduct searches.



- Target : the PIKABOT cybercriminal service is a complex loader operating as malware-as-a-service (MaaS). It was leased by cybercriminals to distribute other malware such as ransomware or data exfiltration tools.
- Identification and arrest in Ukraine of the main administrator of PIKABOT and an accomplice, and searches of the homes of the administrator and an accomplice in Ukraine, in conjunction with the local authorities.
- Seizure and decisive dismantling of PIKABOT's technical infrastructure, including two key remote servers located in Ukraine, enabling criminal operations to be terminated immediately.



Coordinated by
Europol and Eurojust



Participating EU
Member States



Non-EU
participating states



Authorities involved
in the operation's
coordination centre



PLASTIC DEFENSE

Facts and events :

In February 2024, a judicial operation led by the National Cyber Unit dismantled the group suspected of being part of a major arms trafficking operation using 3D printers. This represented the first case of its kind in France, solved thanks to coordinated work between French and Belgian investigators.

The investigation :

In November 2022, C3N, the Centre for Combating Digital Crime (now the UNCyber Operations Division), identified a French-speaking profile on the darknet, a 26-year-old offering 3D printed weapons for sale. This production method is accessible to many people and can be used to produce untraceable lethal weapons.

Key results :

- Two administrators and a dozen other individuals were arrested ;
- Seizure of equipment (3D printers, computers, etc.) and several thousand euros ;
- Seizure of several dozen 3D printed weapons and ammunition of various calibres.



FRANCE TRAVAIL

Facts and events :

On 12 March 2024, Section J3 of the Paris public prosecutor's office referred to the BL2C following a massive intrusion into the information system of France Travail (formerly Pôle Emploi). Nearly 43 million people were potentially affected by the theft of sensitive data such as social security numbers, contact details, credentials, dates and places of birth, exposing victims to a high risk of scams via text messages and emails.

The investigation :

The investigations revealed that between 6 February and 5 March 2024, the fraudsters had impersonated authorised Cap Emploi agents by contacting France Travail's technical support team in order to reset their passwords. Once connected, they massively exfiltrated the data to external servers using anonymisation techniques (VPN, ON/OFF numbers). However, in-depth analysis of the digital and telephone traces enabled the suspects to be identified.

Key results :

- On 17 March 2024, three young individuals in their twenties were arrested simultaneously at their respective homes ;
- Exploitation of the material seized confirmed their direct involvement ;
- Two individuals were arrested in connection with kidnapping and extortion in an organised gang.



COCO

Facts and events :

In June 2024, the National jurisdiction against Organised Crime (JUNALCO) ordered the shutdown of the Coco.gg chat platform. The platform was accused of facilitating criminal activities, including child sexual abuse, grooming and drug trafficking.

The investigation :

This investigation, opened in December 2023 and entrusted to the National Cyber Unit (UNCyber) and the National Anti-Fraud Office (ONAF) in conjunction with COMCYBER-MI and authorities under the coordination of Eurojust. The operation successfully identified the administrators and track financial flows. Between January 2021 and May 2024, 2,305 legal proceedings were opened, involving 480 identified victims.

Key results :

- Shutdown of the coco.gg platform and seizure of the servers ;
- Bank accounts associated with the platform frozen ;
- Arrest of the platform's founder.



EPSILON

Facts and events :

Between 2023 and 2024, three French companies suffered cyber attacks, resulting in the theft of several million items of customer data. The sensitive information extracted (credentials, passwords, bank card numbers, cryptoassets) was then sold on a cybercriminal forum. One of the victim companies also received a ransom demand for 15 bitcoins, which it did not comply with.

The investigation :

The investigation which was entrusted to the anti-cybercrime brigade (BL2C), revealed the attacks were conducted using a information-stealing malware (infostealer) called EPSILON, designed to automatically recover sensitive data from infected workstations. The cybercriminal group administering this malware claimed responsibility for these attacks, as well as for the compromise of the BFMTV/RMC X account for propaganda and self-promotion purposes.

Key results :

- Three members of EPSILON were arrested on June 4th and 5th 2024 and charged ;
- Numerous items of digital equipment were seized, along with access to the group's infrastructure ;
- Seizure of cryptoassets worth several thousand euros ;
- Two other key members of the group were arrested in December 2024



GHOST

Facts and events :

In September 2024, in partnership with Europol, several European countries and the FBI, the Centre for Combating Digital Crime (C3N), which is now the operations division of the National Cyber Unit, and COMCYBER-MI, dismantled the GHOST encryption solution, which was mainly used by organised crime groups.

The investigation :

The dismantling of the GHOST platform is the result of a long-term investigation led by UNCyber and COMCYBER-MI, which played a leading role. This highly technical work was carried out over more than a year at COMCYBER-MI's National Centre for Digital Expertise (CNENUM), and more specifically in the reverse engineering laboratory, which employs many experts with rare skills.

Key results :

- Shutdown of a platform used mainly by organised crime groups ;
- 51 people arrested in connection with organised crime, mainly drug trafficking ;
- Several targeted assassinations prevented;
- Criminal assets and drugs seized.



POWER OFF

Facts and events :

In December 2024, illegal platforms used to carry out DDoS attacks against organisations were shut down following international judicial cooperation.

In return for payment, these platforms allowed services to be paralysed for a few minutes to a few hours.

The investigation :

The operation, called PowerOFF, was coordinated by Europol, with the participation of 15 countries, including France, and the involvement of the Cybercrime Bureau (OFAC) of the National Police.

The investigations identified the administrators of the platforms, as well as hundreds of users who had ordered or carried out DDoS attacks via these services.

Key results :

- Seizure of 27 DDoS platforms ;
- Arrest of three administrators, notably in France and Germany ;
- Identification of more than 300 users of these services, who could face prosecution.



SIM SWAPPING

Facts and events :

In 2023, two complaints revealed cybercriminal attacks targeting holders of cryptoassets. Cryptoasset holders had fallen victim to SIM swapping, a technique that involves hijacking their mobile phone number through identity theft in order to obtain a new SIM card. This process enabled the criminals to bypass double authentication by SMS and therefore empty the victims' digital accounts.

The investigation :

Entrusted to the Paris Police Prefecture's Cybercrime Unit (BL2C), the investigation revealed the involvement of a structured criminal group made up of ten individuals. The perpetrators specifically targeted holders of digital assets who subscribed to the same phone operator, and used the complicity of an internal employee to activate the new SIM cards. Once control of the lines had been obtained, the codes received by SMS enabled the cryptoassets to be transferred to intermediate 'mule' accounts controlled by other accomplices. More than 200 potential victims were identified, around thirty of whom had already lodged a complaint.

Key results :

- 10 suspects were arrested simultaneously throughout France and overseas.
- Following further investigations and an in-depth examination of the seized material, three secondary perpetrators were dealt with through a penal settlement. Meanwhile, the seven main defendants were referred to the Criminal Chamber of the Paris Judicial Court.



MATRIX

Facts and events :

Discovered four years ago by Dutch police, Matrix was an encrypted messaging system designed and specifically developed for illicit activities. To access this messaging system, users had to buy phones costing between €1,300 and €1,600. The messaging system was used as a communication channel for all forms of organised crime, including drug trafficking.

The investigation :

An investigation coordinated by the European agencies Europol and Eurojust, involving the OFAC (Cybercrime Office of the National Police), led to the interception and decryption of more than 2.3 million messages in 33 languages. The Matrix infrastructure was based on more than 40 servers in several countries, including France.

Key resultst :

- The messaging system was dismantled.
- Three individuals from Eastern Europe have been arrested, including one in Paris.
- Seizure of a villa in Spain valued at 15 million euros, four luxury vehicles, 145,000 euros in cash and 500,000 euros in cryptoassets.



FORECASTING THE EVOLUTION OF CYBER THREATS

1 The use of AI to prevent futur threats	52
2 The Internet of things : a vector of emerging risks	54

4

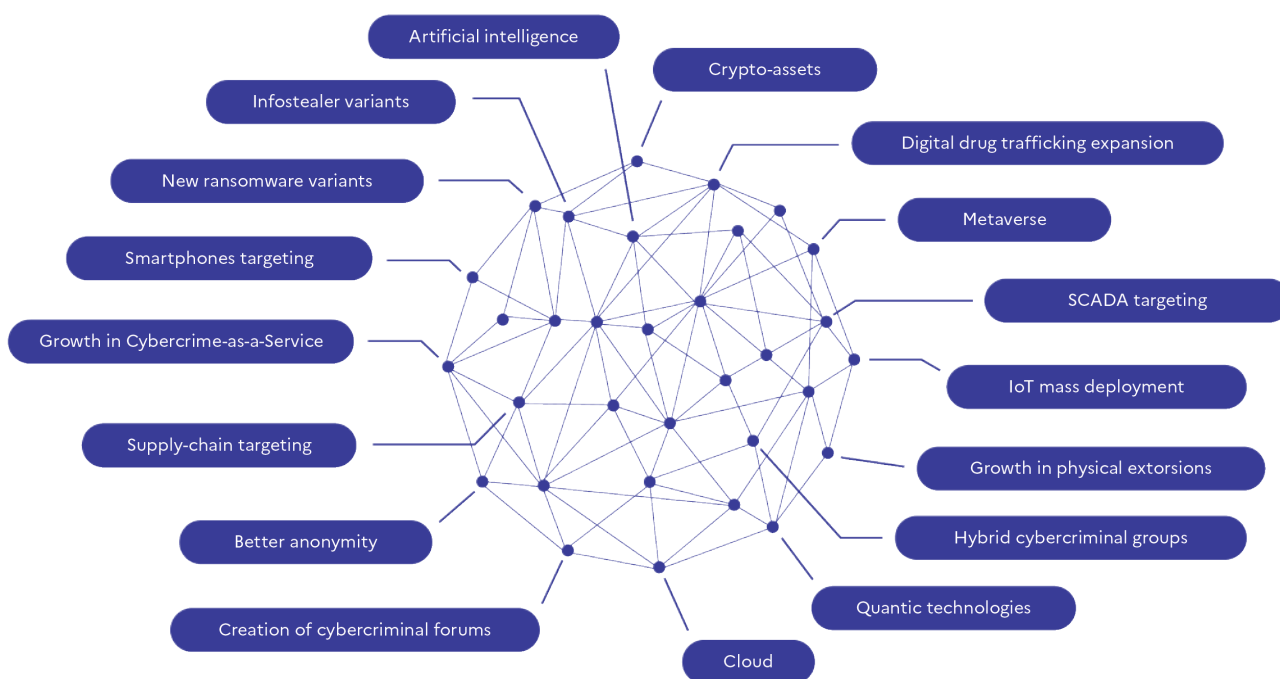
FORECASTING THE EVOLUTION OF CYBER THREATS

In a world where technologies and practices are evolving at an accelerating pace, cyber threats are transforming and becoming more complex, making prevention more essential than ever. To anticipate tomorrow's risks, it is no longer enough to react : we must analyze and strategically prepare. This part of the report explores emerging trends and critical technologies.

It highlights the central role of artificial intelligence in detecting future threats and the systemic risks

associated with the widespread use of connected objects.

The aim of these complementary approaches is to provide government departments, private sector stakeholders and general public with an informed and proactive vision, so as to enhance national cybersecurity resilience in the face of tomorrow's threats.



The evolution of cyber threats

1 | The use of AI to prevent future threats

To have a positive impact, the use of artificial intelligence needs to be part of a strategic vision to avoid misuse and develop responsible AI to protect general public.

Its deployment meets a twofold imperative : ensuring national cybersecurity sovereignty and neutralising emerging attacks while respecting the ethical and legal framework.

The CapIA strategy, developed over the last four years, adopts a collaborative approach in which artificial intelligence supports the work of investigators without compromising their decision-making requirements. This strategy, which notably includes COMCYBER-MI, aims to build a trusted AI system to serve the security of citizens.

Strategy

Although misused by cybercriminals, AI is also an essential tool for protecting information systems, revealing deception and detecting malicious behaviour.

Confronted with the threats posed by generative AI (deepfakes, phishing), the Ministry of the Interior's Cyberspace Command has adopted to the CapIA strategy, developed within the National Gendarmerie and embracing the multi-faceted nature of AI.

The four pillars are :



Sovereignty in AI :

The ability to master and develop these tools at national or European level is essential and requires a commitment to applied research and development ;



Mastery of AI :

By developing a talent management policy and a range of training courses from acculturation (Cultur'IA magazine) to expert-level training (creation of the AI and Security Chair), the aim is to understand the limits and opportunities of using AI. In-depth knowledge of AI is needed to ensure transparency and accountability to the general public and to national and European parliamentary representatives ;



Responsible AI :

The National Gendarmerie has published an ethics charter for AI applications that are in line with the institution's values, starting in 2021. It is also involved in the issues of European regulation of AI use and experimentation with its use in major events ;



A shared AI :

COMCYBER-MI has entered into partnerships with academia, industry and associations. The challenge lies in explaining, exchanging and improving practices in order to face over increasingly imaginative criminal exploitation.

Innovative tools for detection and protection

Artificial intelligence offers an unrivalled ability to process masses of heterogeneous data (text, images, video, voice files) to identify threats that are imperceptible to the human eye. One of the key initiatives is the Authentik AI project.

Developed over a number of years in-house by a multi-disciplinary team (AI engineers, lawyers, work-study students) under the leadership of General Patrick Perrot, the aim of this project is to identify synthetic media in order to facilitate the recognition of deepfakes, by cross-referencing technical and contextual markers detected in these media.

As part of the detection of images of sexual exploitation of minors, the ODIP project (Child Sexual Abuse Material Detection Tool) is being developed to assist investigators in the materia-

lization of the offence. Winner of two awards at the 2024 Datacraft awards, this project comprises two main stages :

- the creation of digital representations of content involving child sexual exploitation, making it possible to detect illegal content without actually viewing it,
- training the AI model based on these vector representations, so that it can automatically identify this content when analysing a digital material.

This project, developed in-house by COMCYBER-MI, responds to the need to protect investigators from the traumatic exposure of sensitive content and to radically optimise the processing of digital evidence.

13. <https://www.numerama.com/cyberguerre/1900240-nos-outils-ia-permettent-deja-deviter-des-traumatismes-entretien-avec-le-general-de-gendarmerie-en-charge-de-lia.html>

Training and acculturation as pillars of the CapIA strategy

In addition to implementing advanced AI tools, mastering of these innovations also depends on a solid training system, from basic training to PhD level. In this context, the CapIA strategy defines the main areas of training in compliance with the RIA, which requires training for the staff of an organisation implementing AI. To bridge the gap between the awareness level of all COMCYBER-MI staff and the expert level, CapIA is setting up short training courses for specialist investigators.

In order to ensure that this knowledge is disseminated, *Cultur'IA*, a bimonthly magazine available online, offers a theoretical and practical approach, covering legal aspects, technological developments and practical applications in the field of security.

At the same time, the establishment of an AI and Security Chair, currently supported by a partnership between COMCYBER-MI and the Institut Supérieur Electronique Of Paris (ISEP), aims to structure doctoral courses and strengthen the skills of managers and future experts. These educational and partnership initiatives illustrate both a commitment to innovation and to an in-depth understanding of deployed tools, ensuring that technological achievements remain firmly rooted in robust ethical and operational thinking.

The CapIA strategy, of which COMCYBER-MI is a part, aims to protect both civil liberties and the democratic model of society by offering greater efficiency in the fight against crime in one of the areas where crime has the fewest countermeasures : cyber space.

2 | The Internet of Things : a vector of emerging risks

The Internet of Things (IoT) refers to all the connected objects that collect and exchange data and provide services in our everyday lives.

These objects, often equipped with sensors, can process information to trigger actions or transmit them. IoT refers specifically to objects capable of operating in a network. These can include humidity sensors, window sensors, thermometers, locks, air conditioners and connected vehicles.

The connected objects market is characterised by its extremely rapid expansion, with an estimated 45 billion connected objects worldwide by 2030, which will have a significant impact on our lifestyles.

Uses and developments

The connected objects that make up the Internet of Things (IoT) can be found in a wide range of sectors, including industry, agriculture, the automotive industry, healthcare and home automation. The IoT is transforming our daily lives, offering numerous possibilities for improving and managing tasks. These uses are also increasingly interconnected with artificial intelligence solutions. It stands out for its ease of deployment and implementation, and its ability to adapt to changing needs. It enables tasks to be automated,

Despite its many advantages, the IoT represents an ever-growing threat. These objects collect vast quantities of sensitive data and are vulnerable to cyber-attacks. The risks associated with the security, privacy and interconnection of these devices make their management critical.

The increase in the number of connected objects raises concerns about privacy breaches, data breaches and security vulnerabilities that could be exploited by cybercriminals.

Moreover, these connected objects can be diverted from their original purpose in order to carry out malicious actions such as DDoS and espionage by harnessing their computing power and functionalities.

productivity to be increased and resources to be optimised. It provides remote access and facilitates decision-making.

For example, the deployment of IoT in the agricultural sector is helping to optimise greenhouse management by providing real-time information on conditions such as temperature, humidity and lighting. This data can be used to adjust greenhouse management parameters according to defined and modifiable criteria to optimise growing conditions.

14. <https://www.calameo.com/books/0027192924fd5d12ea20e>

Risks and misuses

In the field of cyber security, vulnerabilities are detected on a daily basis. As the number and variety of connected objects around us continues to grow, the digital risks are all the more present. Millions of vulnerabilities are detected in connected objects every year.

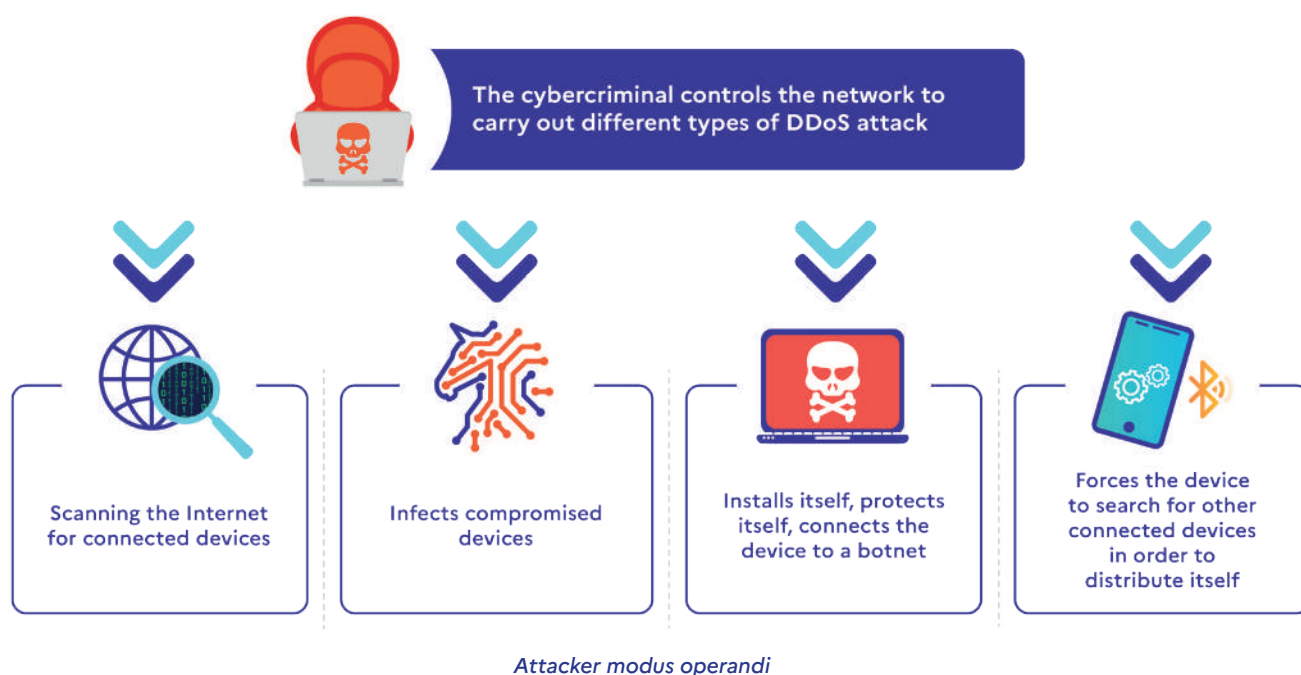
The risks associated with the Internet of Things include inadequate security consideration at the design stage of objects and their means of communication. These risks are exacerbated by poor user practices, such as using weak passwords or forgetting to update products.

The criminal exploitation of IoT can be divided into two main categories: cybercrime and traditional crime.

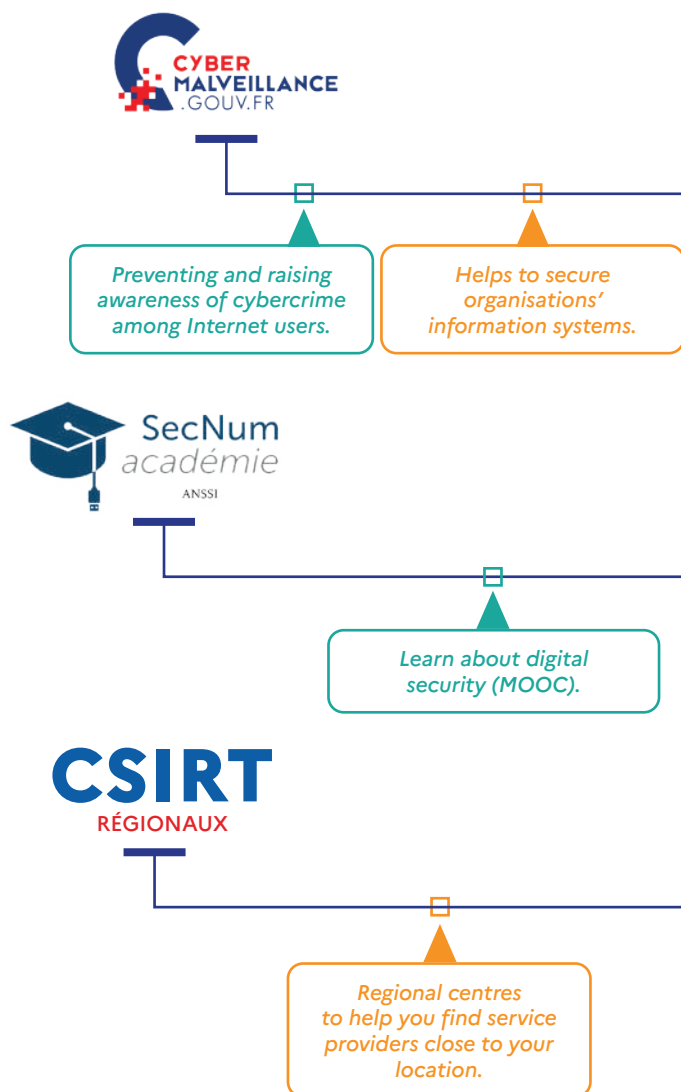
Cybercriminals use tools to hack connected objects and platforms, aiming to create botnets to carry out DDoS attacks, run phishing campaigns, spy, steal data and gain access to computer networks.

Traditional criminals use these objects to optimise their traffic, spy, harass or facilitate burglaries and car thefts. The Internet of Things offers many opportunities, but also raises challenges in terms of security, privacy and environmental impact.

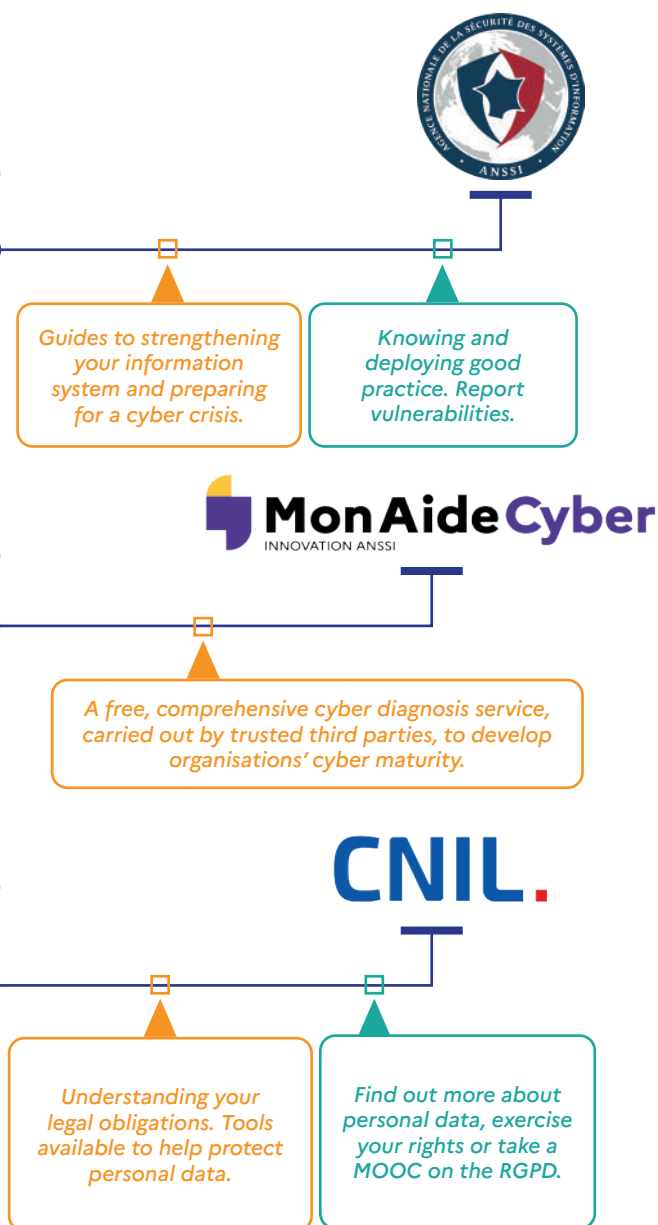
Although regulations such as the GDPR, NIS2 and the Cyber Resilience Act can limit some of the risks, the increasing production and use of connected objects will create an ever-expanding attack surface.



Find out more



Building cyber security

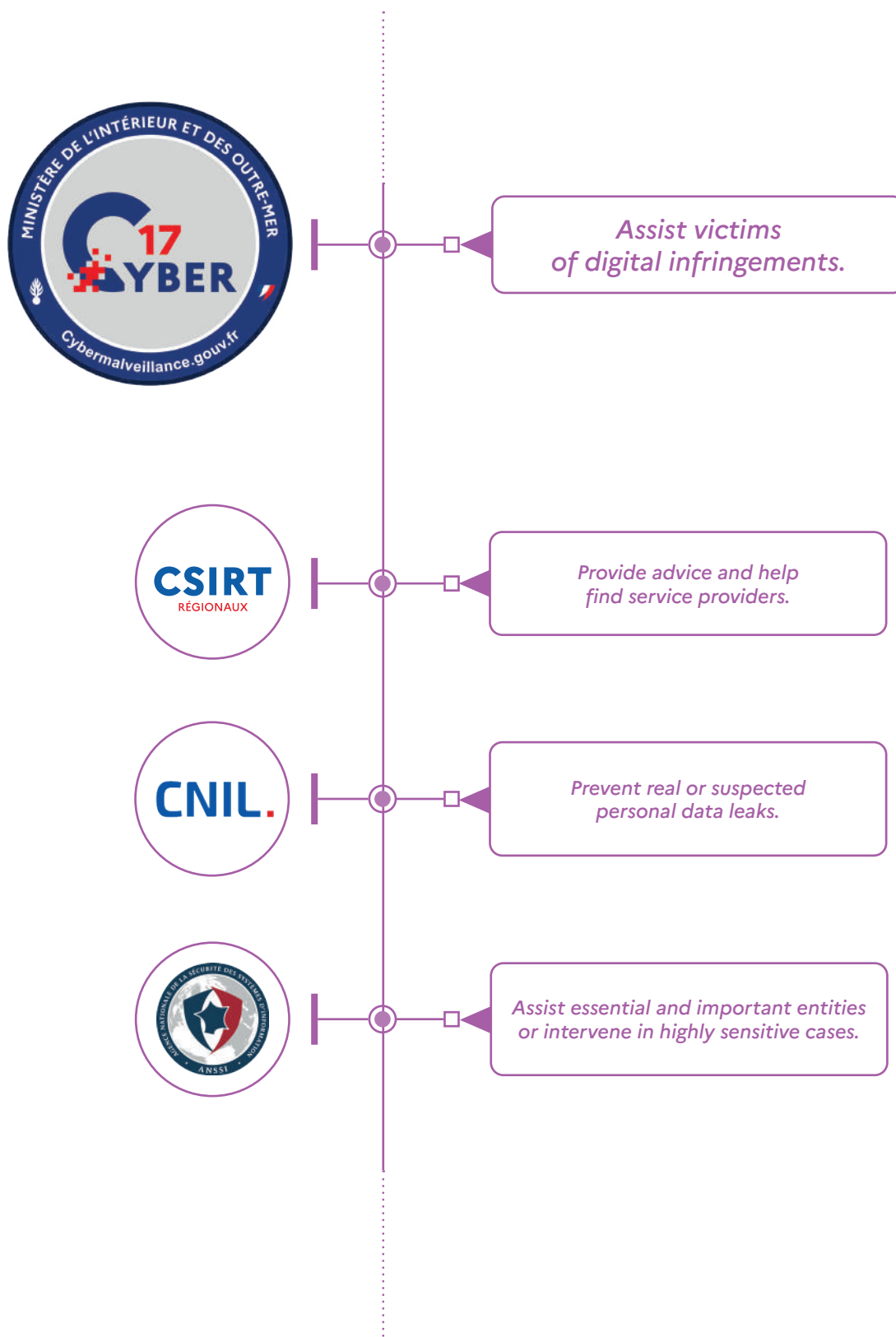


HAVE ANY DOUBTS ABOUT AN E-MAIL ?

Report it as spam :



Responding to cyber-attacks



MA SÉCURITÉ

Call 17 to contact the police by telephone or on the website :

masecurite.interieur.gouv.fr



Ma Sécurité
Application Grand Public

17CYBER

Contact 17Cyber for personalised help and advice, live or via chat, from a police officer :

<https://17cyber.gouv.fr/>



CYBERMALVEILLANCE.GOUV.FR

Cybermalveillance allows you to learn about threats and find assistance as a victim :

cybermalveillance.gouv.fr



CSIRT RÉGIONAUX

CSIRT RÉGIONAUX

The regional CSIRTs respond to requests for support and connect with local partners :

cert.ssi.gouv.fr/csirt/csirt-regionaux



ANSSI

The French National Agency for the Security of Information Systems assists essential and important entities, provides guides and publishes a cyber MOOC for everyone :

cyber.gouv.fr

CNIL

CNIL

The National Commission on Informatics and Liberty regulates personal data. It supports professionals and helps individuals :

cnil.fr

Affiliates :

Cybercriminals who carry out cyberattacks, sometimes sophisticated, using malicious tools made available by developers or designers. The profits generated by affiliates are shared with developers via a commission system.

ANSSI :

French National Agency for the Security of Information Systems.

Automated data processing system :

Set of physical and application elements used to process data (networks, computer media, etc.).

Big Game Hunting :

Strategy of cyber attacks targeting large companies or institutions to demand ransoms or obtain substantial gains via sophisticated techniques.

Blockchain :

Distributed ledger operating in a network with a wide variety of nodes (peer-to-peer computers) validating and ordering transactions by consensus. The transactions are recorded in a public, exhaustive and global ledger, replicated in all network computers.

Botnet :

A contraction of 'bot' and 'net', meaning 'network of robots'. It is a network of compromised machines administered by one or more malicious actors.

Bulletproof hosting :

Attack consisting of automatically testing combinations of stolen logins and passwords, to check whether they work and carry out a cyber attack.

CJUE (Cour de justice de l'Union européenne) :

Highest court in the EU, interprets European law and ensures its uniform application in the Member States.

CNIL :

National Commission on Informatics and Liberty.

Cookies :

Files stored by websites on the browser to retain information about the user.

Credential stuffing :

Hosting services that tolerate illegal content (phishing, malware), operating from lax jurisdictions, making them difficult to shut down.

Cryptoassets :

Digital asset using cryptography and blockchain technology in particular to secure and verify transactions.

Cryptoassets mining :

Action aimed at securing a blockchain by lending its computing power for the purpose of generating new blocks and choosing the order of transactions. When they mine a block, miners are paid in newly created cryptoassets. This process is legal, but some cybercriminals use the computing power of their victims' machines to mine cryptoassets without their knowledge, for the benefit of the criminal.

Cybercrime-as-a-Service (CaaS) :

Online provision of cybercriminal services or advice. Several variations exist depending on the type of phenomenon, such as RaaS (ransomware), BaaS (botnet), MaaS (malware), etc.

Cyberespace :

Communication space formed by the worldwide interconnection of automated digital data processing equipment.

Cyber forum :

Public space for virtual exchanges between Internet users. A means of communication favoured by cybercriminals, accessible on both the clearweb and the darkweb.

Cyber-harassment :

Intentional act or comment by an individual or group of individuals using electronic forms of communication, repeatedly directed against a victim, causing a deterioration in the victim's living conditions.

Darknet :

Networks such as Tor or Freenet that allow access to resources hidden from the traditional web. The sum total of information accessible on darknets forms the darkweb.

Darkweb :

Hidden part of the web accessible with specific software. Many illegal activities are available there, including the sale of malicious software and the exchange of illegal content.

Data Poisoning :

Intentionally altering the training data of an AI model to bias its results or create unintended behaviours.

Dataleaks :

Malicious or accidental disclosure of sensitive data (emails, passwords, bank details, etc.).

DDoS-as-a-Service (DaaS) :

Consists of making available or renting software dedicated to the implementation of DDoS cyberattacks. Attackers can be paid to carry out certain cyber attacks, in exchange for proof.

Decentralised finance (DeFi) :

Ecosystem of financial services based on blockchain technology and smart contracts to operate in a decentralised way, without traditional intermediaries.

Deepfake-as-a-Service (DfaaS) :

Service providing AI-generated faked videos (deepfakes) on demand, accessible even to non-technical people via specialised paid platforms.

Deepfake :

Technique for manipulating digital content based on artificial intelligence. In particular, it can be used to create false content, making it possible to impersonate a person.

Denial of service (DoS) :

Aims to make a server inaccessible by sending multiple requests until saturation or by exploiting a security flaw in order to cause a breakdown or operate at a severely degraded level, using one or more computer media.

Distributed denial of service (DDoS) :

Distributed version of DoS with the same objectives, which uses several machines, usually a botnet.

Doxing :

Unauthorised public disclosure of personal information about a person (name, address, telephone number), often to intimidate or harass them.

Drainer (cryptoassets) :

Malicious software used to induce a user to sign a transaction enabling the user's cryptoassets to be siphoned off.

ESMA (European Securities and Markets Authority) :

European authority supervising the European Union's financial markets, ensuring their stability and protecting investors.

Face swap :

Technique for modifying images and videos in which the faces of two people are swapped.

Facial reenactment :

Deepfake technique reproducing an individual's facial expressions in real time on another face.

False Flag Attacks :

A deceptive attack designed to make it appear that it originates from another actor (country or group) in order to disguise the origin of a cyber-attack or harm a third party.

False transfer orders :

A modus operandi that consists of diverting a transfer to a criminal's account, for example by posing as a supplier of the victim.

Fake bank adviser scam :

A fraudster posing as a bank employee to obtain financial information or transfer validations under the pretext of a 'security' procedure.

Fake jobs scam :

Fraudulent job advertisements aimed at obtaining sensitive data (bank details, identity documents) or scamming people out of money by charging false fees.

Fake president scam :

A scam in which a criminal assumes the identity of a company director in order to demand a bank transfer.

Fake romance scam :

Sentimental scam where a con artist creates an emotional bond with the victim in order to extract money or personal data.

G7 :

The G7 ('Group of 7') is an economic discussion and partnership group that brings together every year the heads of state and government of the 7 most industrialised countries in the world (France, the United States, Canada, Japan, the United Kingdom, Italy, Germany).

GDPR :

General Data Protection Regulation.

Hacktivisme :

Digital activism using hacking to promote ideological, political or social causes, often by attacking websites or leaking data.

ICANN (Internet Corporation for Assigned Names and Numbers) :

Non-profit organisation recognised as being in the public interest, bringing together participants from all over the world who work to preserve the security, stability and interoperability of the Internet.

Initial access broker :

Cybercriminals selling illegitimate access to information systems to other cybercriminals who will exploit them as part of a larger-scale attack.

Information system :

Organised set of resources used to collect, store, process and distribute information.

Infostealers :

Malicious software designed to steal sensitive information (passwords, bank cards details, cookies, browsing history) from an infected computer.

Insiders :

Individuals inside an organisation (employees, subcontractors) exploiting their legitimate access for malicious purposes.

Internet of Things :

Network of connected objects (watches, sensors, domestic appliances) capable of collecting and transmitting data via the Internet.

LAM (Large Action Model) :

AI model designed to plan and execute complex actions, often used to automate practical tasks in software or physical environments.

LLM (Large Language Model) :

Artificial intelligence model trained on large volumes of text to understand, generate or summarise natural language.

Malware :

Malicious software, or any programme developed with the aim of damaging an information system or network.

Malware-as-a-Service (MaaS) :

Rental or sale of ready-to-use malware, often with technical support.

Memecoins :

Cryptoassets of memes (e.g. Dogecoin, Shiba Inu), created with no technological purpose but which can increase in value via speculation.

MiCA regulation (Markets in CryptoAssets) :

European regulation governing cryptoassets, aimed at protecting investors and preventing abuses on digital markets.

Mixer :

Cryptoassets mixing service to prevent tracing.

Modus operandi :

Method used repeatedly by a group or individual to commit cyber attacks or fraud.

NIS2 Directive (Network and Information Security 2) :

European directive of 2022 reinforcing cybersecurity obligations for operators of essential services and critical businesses.

NFT (Non-Fungible Token) :

Digital token created on a blockchain, representing a work of art, a virtual object or a property right.

Offences against automated data processing systems :

Computer offences under the French Penal Code, aimed at hacking, altering or hindering the operation of computer systems (data theft, sabotage, intrusion, etc.).

Open Source software:

Software whose source code is entirely accessible on the Internet free of charge. It is potentially modular and reusable. A lot of software used by cybercriminals is open source.

Personnal Data :

Identifying elements relating to an identified or identifiable natural person (surname, first name, date of birth, social security number, etc.).

Phishing :

A technique used to mislead a target into providing personal information such as login details or identity information by sending an email that appears to be from an institutional site.

Phishing-as-a-Service (PhaaS) :

Sale of turnkey phishing kits or services on cybercriminal forums, encrypted messaging systems or other.

Public address (cryptoassets) :

String of alphanumeric characters used as a reference point for sending and receiving cryptoassets on a blockchain.

RaaS, Ransomware-as-a-Service :

A business model for buying or renting ransomware in which part of the profits earned by an affiliate are paid back to the developers of the malicious program.

Ransomware :

Malicious software that demands ransom by encrypting data and/or exfiltrating data.

RDP (Remote Desktop Protocol) :

Protocol allowing remote connection to a computer.

Remote control servers (C2 / Command and Control) :

Servers used by cybercriminals to control compromised machines remotely.

RIA (Rich Internet Application) :

Web applications offering a user experience similar to installed software, with dynamic interactions (e.g. Google Docs, Figma).

SCADA (Supervisory Control and Data Acquisition) :

Industrial systems that supervise and control critical infrastructure (electricity, water, gas). They enable remote control of equipment via sensors and automated systems.

Script kiddies :

Novice hackers who use tools available on the Internet without understanding how they work, often to carry out low-level cyber attacks.

Smart contract :

Software on a blockchain, self-executing under pre-defined conditions.

Smishing :

Word derived from the contraction of 'SMS' and 'phishing'. It refers to phishing by SMS.

Social engineering :

A psychological manipulation technique that exploits trust or ignorance for malicious purposes. This *modus operandi* is used to carry out scams as well as cyber attacks.

Spearphishing :

Targeted phishing aimed at a specific person or entity, with a personalised message. This method is particularly used to infect the victim's computer and carry out a cyber attack.

Spoofing :

The theft of someone's identity to gain their trust, access their systems, spread malware, steal their data and capture their digital or financial assets.

Supply Chain Attacks :

Compromising a legitimate supplier or service provider in order to infiltrate an end target, through the dependencies they have on each other.

Swatting :

A malicious call intended to unduly trigger the intervention of law enforcement or civil security forces (e.g. a false bomb threat).

Typosquatting :

Malicious action which consists of registering a domain name very similar to another domain name, to commit fraud or cyber attacks.

Vishing (voice phishing) :

Phone scam using social engineering to trick the victim into providing sensitive data or performing harmful actions.

VLM (Very Large Model) :

Next-generation AI model, even larger than LLMs, with billions of parameters, often multimodal (text, image, code).

VPN (Virtual Private Network) :

Virtual private network creating an encrypted tunnel between the user and a server. This technology allows users to change their IP address.

Wallet :

Interface (software or hardware) used to access and manage cryptoassets linked to one or more public addresses.

Website defacement :

The result of a cyber attack that has altered the appearance or content of a website, therefore violating the integrity of the pages by altering them.

NOTES

Managing editor :

Major general Christophe HUSSON

Editorial team and contributors :

This report has been compiled with contributions from :

- the cabinet of the Ministry of the Interior ;
- the Ministerial Statistical Service for Internal Security ;
- the Paris Police Prefecture ;
- the General Directorates of the Ministry of the Interior : National Police, National Gendarmerie, Homeland Security ;
- and the Ministry of Justice (section J3 of the Paris public prosecutor's office).

The report was produced by the Cyber threats Analysis and Grouping Centre (CECyber) of the Ministry of the Interior's cyberspace command.

Graphic design and production :

Command of the Ministry of the Interior in cyberspace
Communication Outreach and Multimedia Section

Cover illustration :

Image generated with Freepik IA and used in accordance with the free Freepik licence (www.freepik.com)

Contact :

Ministry of the Interior's Cyberspace Command

rapport-ccmi@gendarmerie.interieur.gouv.fr

COMCYBER-MI

« Nos forces, pour votre cyber-protection »

Ministry of the Interior's
Cyberspace Command