RÉPUBLIQUE
FRANÇAISE

Liberté
Égalité
Fraternité

CYBER THREAT OVERVIEW 2023

CYBER THREAT OVERVIEW

2023

SUMMARY

This third edition of the *Cyber Threat Overview* describes the main trends observed by the French National Cyber Security Agency (ANSSI) in 2023. This document focuses on the **motivations** of attackers, their **capabilities** and the **opportunities** they exploit to compromise information systems. It provides concrete examples of incidents ANSSI had to handle during the year. The level of cyber threat keeps on increasing against a backdrop of new geopolitical tensions and France hosting international events. Today, ANSSI assesses that attackers linked to China, Russia and cybercrime pose the greatest threat to the most critical networks and to the French ecosystem in a systemic way.

This year, once again, the threat of strategic and industrial espionage mobilised ANSSI's teams the most. The Agency has seen a significant increase in the targeting of entities working in strategic sectors (think tanks, research institutes, defence industrial and technological base) or that are responsible for the transmission of sensitive data, such as telecommunication companies and managed service providers (MSP). For this purpose, attackers keep on perfecting techniques which enable them to gain access to information systems, to propagate, to exfiltrate information or pre-position themselves, and to avoid detection. At the same time, ANSSI noticed an increasing number of attacks against both corporate and personal mobile phones in order to spy on targeted individuals. This trend is largely driven by the proliferation of commercial cyber intrusion capabilities.

Financially motivated attacks also remained at a high level in 2023, with a resurgence in the number of ransomware attacks against French organisations. The cybercrime ecosystem also keeps on diversifying thanks to the leaks of ransomware source codes and to the wider availability of tools leveraged by actors with limited technical skills. Cybercrime still constitutes an important threat to the public sector and entities which are particularly dependent on service continuity, especially in the health and energy sectors. This year, to tackle this threat, ANSSI took part in an international task force aimed at taking down Qakbot's infrastructure. In some cases, the attackers' financial motivations are not clearly identified, which suggests some cybercrime intrusion sets may be exploited by state-sponsored actors to carry out espionage or destabilisation operations.

In 2023, ANSSI noted an upsurge of attacks aimed at promoting a political agenda, hindering access to online content or undermining an organisation's reputation. In France, these destabilisation efforts have mainly taken the form of distributed denial of service attacks (DDoS) conducted by pro-Russian hacktivist groups highly responsive to current events, but with limited impacts. ANSSI was also informed of the compromise of part of the information system of a French media which led to the disclosure of exfiltrated information in retaliation for previous publications. In a context of international tensions, attackers could also be encouraged to gain access to, and maintain persistence in, critical networks, especially in the energy, transport and logistics sectors. Although no sabotage operation has been detected on French soil,

destructive malware keeps on being used to target Ukrainian entities. Pre-positioning operations were also detected against several critical infrastructures in Europe, North America and Asia.

To achieve their goals, attackers still rely on numerous technical weaknesses. Amongst those weaknesses, exploitation of "zero-day"[1] and "one-day"[2] vulnerabilities remains a prime point of entry for attackers. ANSSI would like to reiterate that CERT-FR regularly issues alerts and security notices on its website along with recommendations. Even though some attacks are particularly challenging to prevent, attackers also too often benefit from bad administration practices, delays in applying patches and lack of encryption mechanisms. Finally, the major events France is scheduled to host in 2024, first and foremost the Olympic and Paralympic Games of Paris (JOP2024), could provide attackers with additional opportunities to act. In the run up to this event, ANSSI and all stakeholders are pursuing their efforts to improve the security of information systems involved in accordance with the threat and to implement a reinforced detection and incident response system. ←

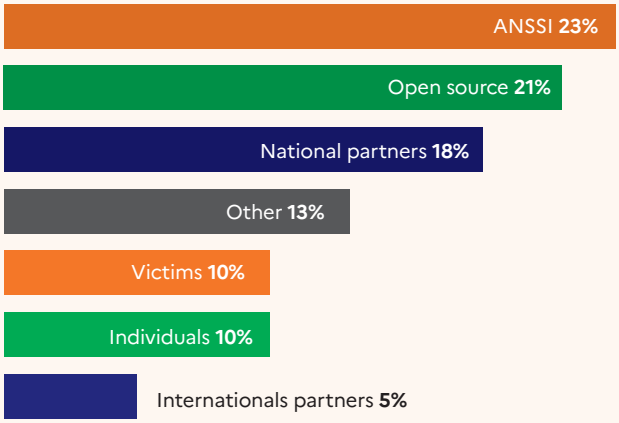
[1] A vulnerability that has not been the subject of a publication and for which there is no security patch while it is being exploited.

[2] A vulnerability for which a security patch is available but which has not been deployed by the user, allowing the vulnerability to be exploited.

Origin of security incidents managed by ANSSI in 2023

To identify security events impacting French entities, ANSSI relies on multiple sources of information. This information comes primarily from in-house resources (23%), ranging from monitoring for the benefit of public authorities to scans[3] and threat analyses. These capabilities are supplemented by open source monitoring, which accounts for 21% of identified events.
10% of security events are reported to ANSSI directly by the victims. The severity of those events is often more important than the average, as they are often associated with high impact incidents such as the compromise and encryption of an information system by a ransomware. Finally, nearly 23% of alerts reported to ANSSI came from exchanges with national and international partners, whether private or institutional.

→ **Origin of security incidents managed by ANSSI in 2023**



Major incidents and cyber defence operations represent ANSSI's highest level of commitment when responding to a security event. They are reserved for the most severe and complex events. These events are reported to ANSSI directly by the victims or thanks to the joint efforts of the Agency and its national and international partners.

[3] See *section 3.A.*

→ 1

THE CHANGING MOTIVATIONS OF MALICIOUS ACTORS

A **STRATEGIC AND INDUSTRIAL ESPIONAGE**

In 2023, the threat of computer espionage has once again mobilised ANSSI's teams the most. This bears witness to the human, financial and technical means devoted by state and private actors to collect strategic, industrial or personal data on French networks. The year was notable for the upsurge in attacks carried out by intrusion sets publicly linked to the Russian government against organisations located in France.

This year, in addition to the public organisations which are the usual victims of espionage, ANSSI noticed an ever-increasing targeting of think tanks, research institutes and companies from the defence industrial and technological base. Attackers target organisations working in strategic sectors or that they consider close to the French government. These attacks are not limited to the metropolitan area: in 2023, ANSSI responded to a computer security incident in overseas France caused by an intrusion set publicly linked to China.

To carry out their campaigns, attackers keep on trying to compromise intermediaries, for instance by targeting subcontractors, service providers or companies within the telecommunication sector. In 2023, ANSSI handled the compromise of a telecom operator's network equipment, conducted by a state-sponsored intrusion set, likely to carry out an espionage operation on telecommunications. ANSSI observes that attackers specifically target poorly secured administration protocols to compromise network equipment. Moreover, they leverage protocols that do not ensure communication encryption by default in order to intercept unencrypted traffic of the operators' clients. It is therefore necessary for operators to be particularly careful to stop using weak administration protocols, while their clients cannot assume there is security by default and must ensure end-to-end encryption is applied to communications passing, even partially, through unsecured protocols [1].

Strategic attackers usually try to remain stealthy[4] in order to carry out their espionage or pre-positioning campaigns[5]. Detecting them requires an excellent coordination between the French government services working on such threat. To that end, the French government set up the Cyber Crisis Coordination Centre (C4) as well as its operational subdivision called C4 TechOps [2]. This interministerial framework, steered by ANSSI, is responsible for cyber threat analysis sharing between experts from the Agency, the Directorate-General for Internal Security (DGSI[6]), the Directorate-General for External Security (DGSE[7]), the Cyber Command (COMCYBER[8]) and the Directorate-General of Armament (DGA[9]), whilst complying with the prerogatives of each entity [3]. It therefore directly contributes to the improvement of incident detection, anticipation and attribution capabilities. Through this framework, ANSSI regularly receives warnings about potential victims located in France.

[4] See *section 2.A.*
[5] See *section 1.C.*
[6] Direction générale de la sécurité intérieure.
[7] Direction générale de la sécurité extérieure.
[8] Commandement de la cyberdéfense.
[8] Direction générale de l'armement.

Even though the interest of malicious actors is generally focused on compromising organisations' networks, attackers nevertheless increasingly target equipment belonging to individuals, in particular mobile phones[10]. These operations are primarily directed against prominent figures or senior executives, but also against security teams. In 2023, attackers presumed to be associated with North Korea once again targeted security researchers with particularly advanced social engineering techniques [4], perhaps with the aim of collecting information and tools which could be reused in future attacks.

In 2023, just as in previous years, the Agency has dealt with incidents involving the presence of several groups of attackers on the network of a single victim (multi-compromise) as well as with the comeback of attackers kicked out only a few months before (re-compromise). These incidents bear testimony to the persistence of some actors, which will most probably keep on targeting French entities that are of high value for intelligence collection objectives. Despite the fact that their impacts remain difficult to evaluate, it is worth stressing that these long-lasting and low-key campaigns are aimed at collecting strategic information which will have major long-term consequences. ANSSI reiterates the importance of remediation actions and of maintaining efforts to rebuild and harden infrastructures after an incident has been addressed. ←

[10] See *section 2.C.*

↓

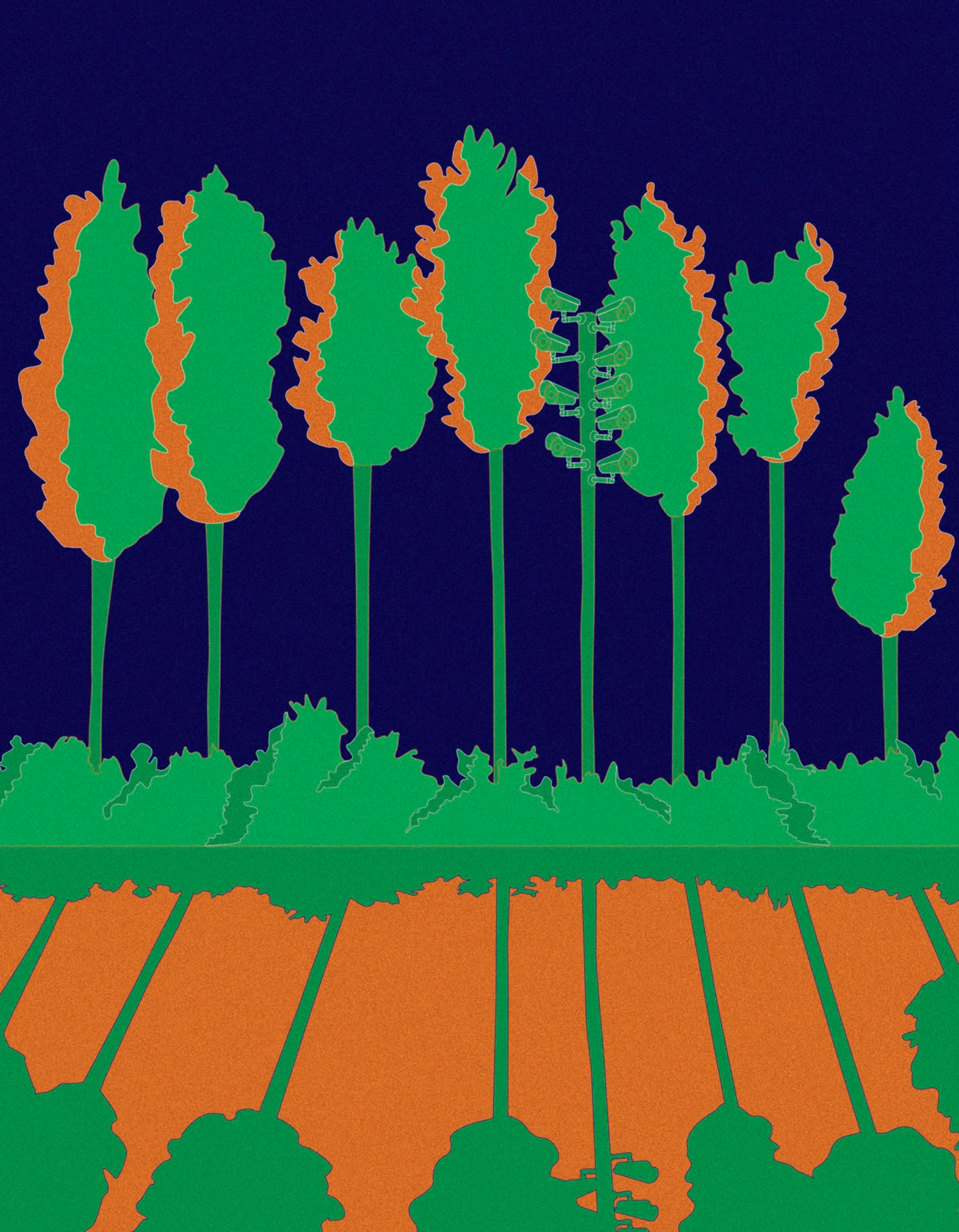
ANSSI's legal detection and anticipation capabilities

For threats likely to affect critical operators or defence capabilities or to harm national security, ANSSI benefits from legal provisions enabling it to enhance its knowledge of threats, to detect victims or even to hinder malicious activities. The military programming law 2024-2030[11] recently strengthened provisions related to cybersecurity by modifying the Posts and Electronic Communications Code (CPCE) as well as the Defence Code.

Thus, article L33-14 paragraph 2 of the CPCE authorises ANSSI to provide technical indicators to some electronic communications operators (OCE) for the purpose of detecting potential victims amongst their clients. For its part, article L2321-2-1 of the Defence Code can be used by the Agency with OCE, hosting providers and data centre operators in order to collect network or system data on equipment controlled by attackers. Finally, article 2321-2-3 of the Defence Code gives ANSSI the possibility to prescribe measures to DNS resolver providers, registrars or the registry operator for blocking or redirecting domain names. The use of these legal provisions is strictly regulated and controlled by the French electronic communications regulation authority (ARCEP[12]).

[10] Loi de programmation militaire (LPM).

[11] Autorité de régulation des communications électroniques, des postes et de la distribution de la presse.

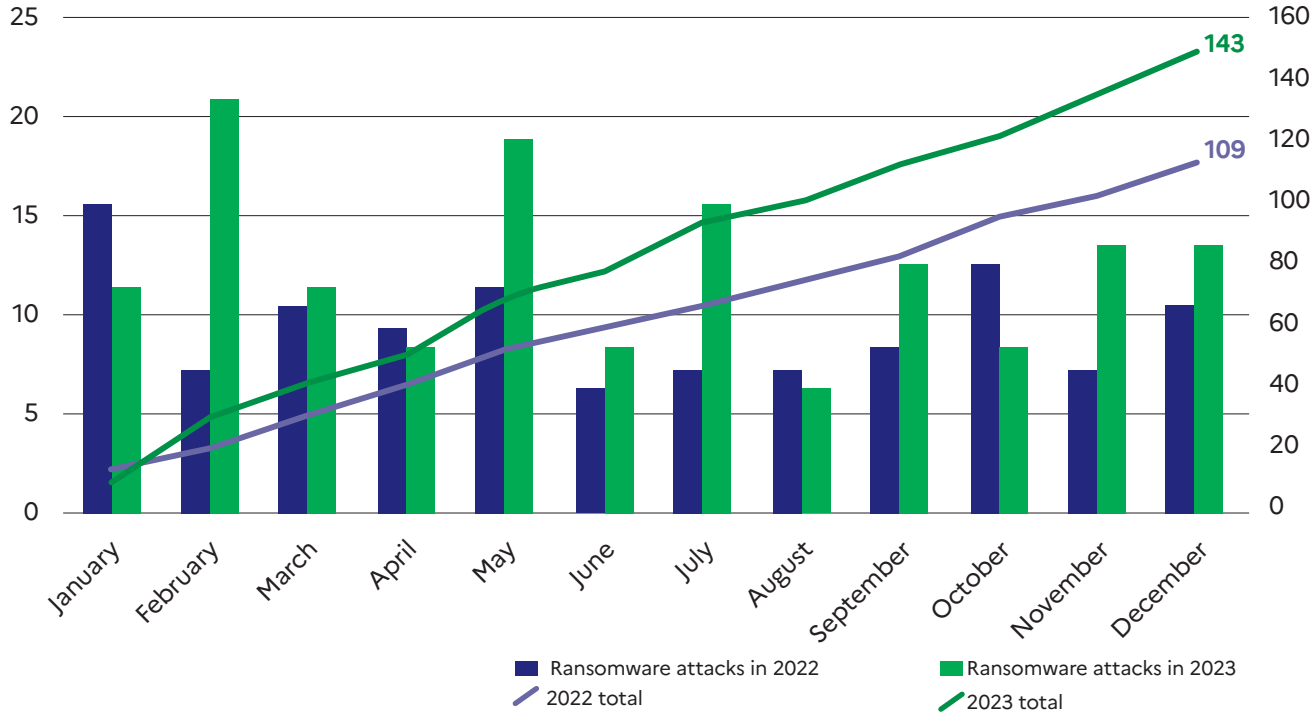


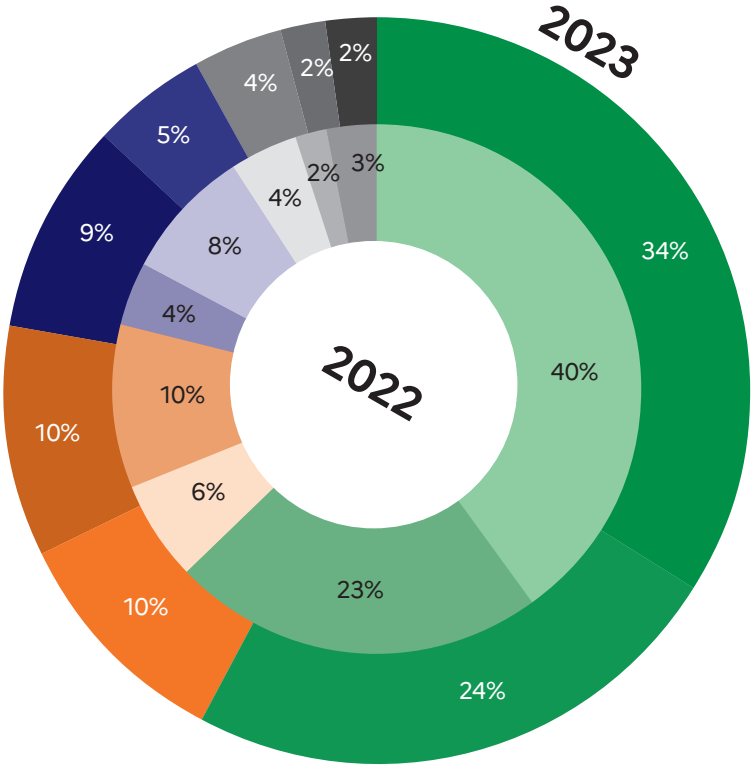
B **PROFIT-ORIENTED ATTACKS**

→ Financially motivated attacks also remained at a high level in 2023. The total number of ransomware attacks reported to ANSSI in 2023 is 30% higher than in 2022. This upsurge, which was also noted by the Paris Public Prosecutor's Office [5], contrasts with the decrease in the number of attacks observed by the Agency in its previous Cyber Threat Overview [6]. However, this trend is limited to the incidents reported to ANSSI or for which a complaint was filed, and thus does not constitute an exhaustive overview.

The increase of attacks was noticeable across all types of entities, and the three most targeted categories have remained identical since 2020 [7]. ANSSI noticed a rising number of incidents impacting several sectors, amongst which associations and local and regional authorities, which respectively accounted for 9% and 24% of ransomware victims in 2023. Moreover, the main strains used to carry out these attacks have evolved in 2023. The emergence of new strains is explained in particular by the identity change of former attackers' groups and

→ Comparison of ransomware attacks reported in 2022 and 2023





→ Breakdown of types of ransomware victims in 2022 and 2023

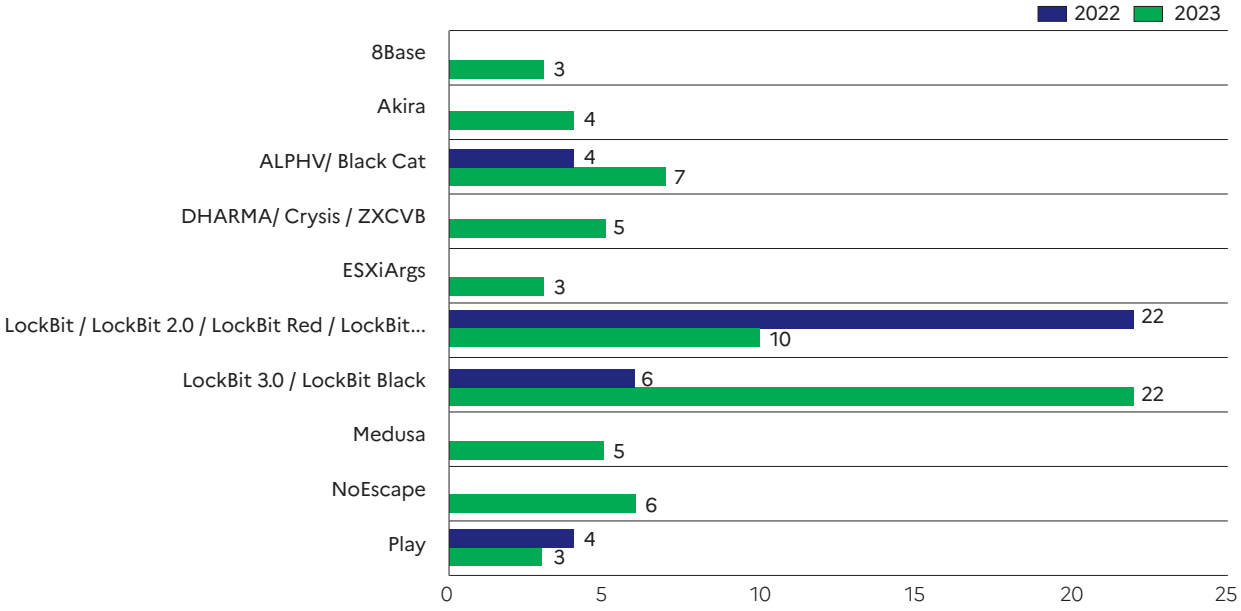
- Microenterprises, SMEs & intermediate-sized enterprises
- Local authorities
- Strategic businesses
- Public health sector
- Associations
- Higher education
- Administrative public establishments (EPA), industrial and commercial public establishments (EPIC)
- Ministries
- Other

by the appearance of new or restructured actors during the year[13]. The significant activity of the LockBit ransomware affiliates, already observed in 2022, continued in 2023.

In some cases, it remains challenging to identify with certainty the real motivations of the attackers who may use methods and tools traditionally linked to the cybercriminal ecosystem to conceal espionage or destabilisation efforts. The convergence

[13] See *section 2.B.*

Comparison of the main strains used in incidents reported to ANSSI in 2022 and 2023



Disclaimer: the above graph only includes strains which were positively identified, at least three times, during incidents handled by ANSSI or by a digital forensic service provider.

already observed last year between the tools and objectives of state and cybercriminal actors has accelerated since the invasion of Ukraine by Russia (see our focus hereunder). It now poses a threat to public entities and to some critical sectors, as well as a challenge to cybersecurity teams.

Malicious actors do not necessarily require a high level of sophistication to target entities of the most vulnerable sectors, such as health and local and regional authorities. Profit-oriented attacks can nevertheless have very serious impacts on the reputation and business continuity of those structures. As a reminder, ANSSI offers automated audit services to French regulated operators and, more generally, to entities within the public sector. In particular, the Active Directory Security (ADS) service helps them secure their Active Directory[14] while the SILENE service can be used to assess their level of exposure on the Internet [8]. ←

[14] Active Directory, the nerve centre of Microsoft information systems security, is a critical element that enables centralised management of accounts, resources and permissions. Obtaining elevated privileges on this directory results in instant and complete control of all resources managed through it.

The RomCom malware

The RomCom backdoor is publicly linked to the Tropical Scorpius cybercriminal group for profit-driven purposes since at least 2022. This group is also believed to have operated the Cuba ransomware since the end of 2019 [9] and is particularly notorious for claiming the compromise of the Montenegro government in August 2022 [10]. From October 2022 until July 2023, RomCom has been used in attacks that were seemingly carried out for espionage purposes within the context of the invasion of Ukraine by Russia. Numerous Ukrainian, European and American entities belonging to critical public and private sectors were reportedly targeted. These espionage operations borrowed tactics, techniques and procedures (TTP) usually associated with cybercriminal attacks [11, 12].

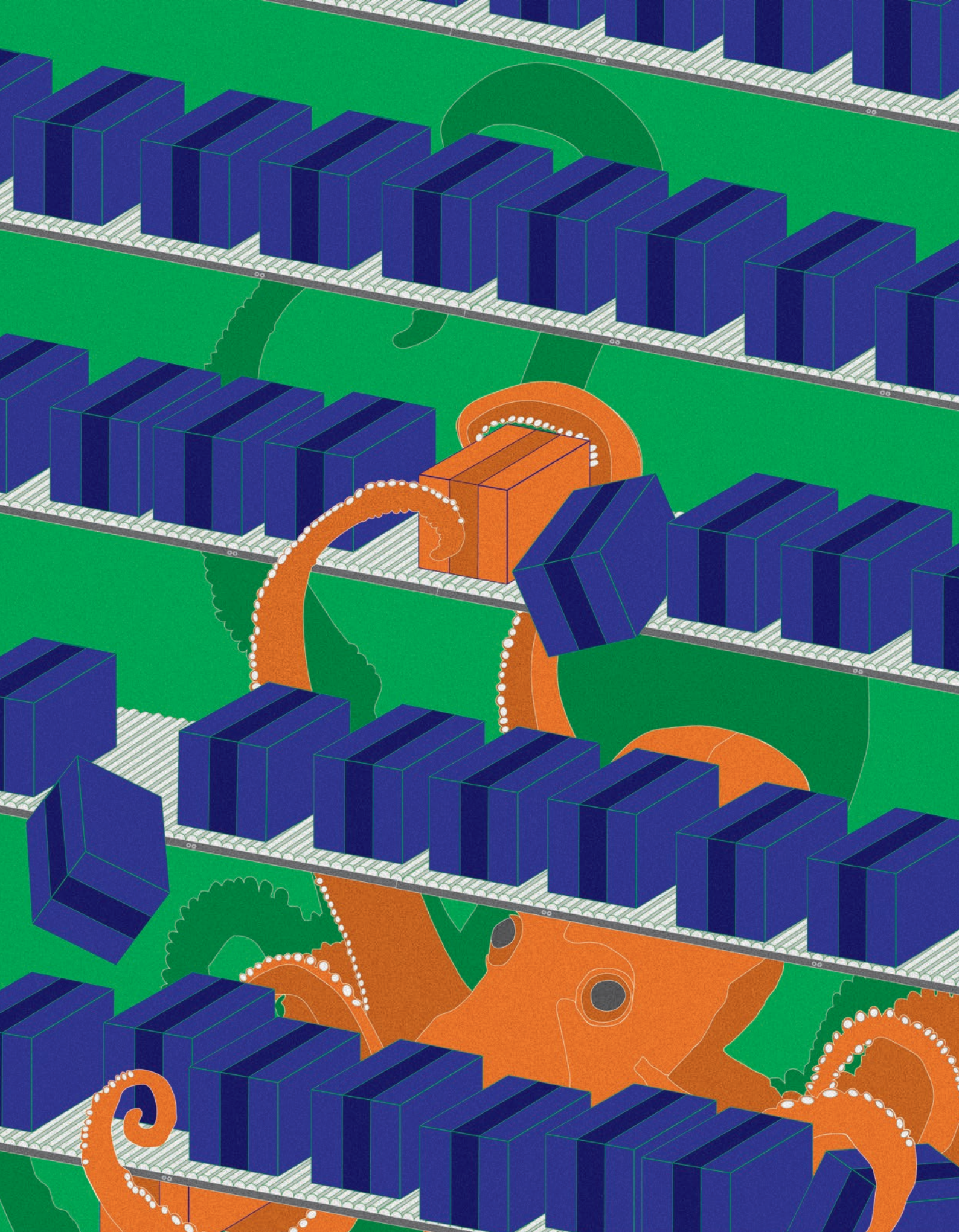
At the end of June 2023, prior to the NATO Vilnius Summit, espionage attacks had been conducted against countries of the Alliance. The operators tried to distribute a RomCom variant by exploiting a zero-day vulnerability[15] targeting Microsoft Office [13]. In the same time, an attack distributing similar malware is said to have targeted an entity in order to deploy a ransomware for profit but without exploiting the same vulnerability. To this day, ANSSI cannot confirm whether it was the same group of attackers or, on the contrary, if this was the work of several different groups. It does however illustrate the potential use of offensive cybercriminal capacities for the benefit of Russian strategic interests.

[15] CVE-2023-36684.

C DESTABILISATION OPERATIONS

→ In a tense geopolitical context, destabilisation threats have intensified this year. ANSSI observed new destabilisation operations using DDoS attacks [14], website defacement, hack-and-leak and sabotage. The most visible operations were DDoS attacks [15], which are most notably carried out by pro-Russian hacktivists who are quick to react to current events [16]. In August 2023, the Anonymous Sudan group thus threatened France with reprisals in case it would intervene against the coup in Niger [17], before redirecting its targeting against Israeli entities following the military offensive in the Gaza strip [18].

While the impact of DDoS attacks remains limited, attackers now exploit new techniques to circumvent existing protection mechanisms. In September 2023, the pro-Russian group NoName057(16) claimed responsibility for DDoS attacks against fifteen European CSIRT, including the CERT-FR, which is run by ANSSI. The campaign was carried out with DDoSia, a software developed by the group [19], and specifically targeted the



application layer of the targeted services [16] which is often not covered by anti-DDoS services. The CERT-FR website was attacked for five days, rendering it unavailable for three hours until a dedicated load balancer was deployed.

Besides these DDoS attacks, ANSSI was informed of destabilisation campaigns relying on intrusions followed by sabotage or the publishing of exfiltrated data (see our focus hereunder). Although no sabotage action against organisations in France was observed, this type of attack was once again conducted against Ukrainian media [20], governmental entities [21] and telecommunication companies [22, 23] in 2023. Some of these operations were likely coordinated with kinetic military action carried out by the Russian army in Ukraine [24].

It is worth remembering that the evolution of the geopolitical context might embolden malicious actors to gain access and maintain themselves on critical European networks, possibly with a view to carrying out subsequent sabotage operations. This year, potential pre-positioning activities were detected on information and operational systems of entities in the energy sector in Europe, in North America and in Asia [25, 26]. The energy, transport, logistics and telecommunications sectors are still considered particularly vulnerable to this threat. ←

[16] Which corresponds to layer 7 of the Open Systems Interconnection (OSI) model. The DDoSia malware executes HTTP requests.

Charlie Hebdo targeting

In December 2022, the French weekly satirical magazine *Charlie Hebdo* launched an international caricature competition depicting the Supreme Leader of Iran. This competition was intended in support of the protest movement sparked off by the death in custody of Mahsa Amini, an Iranian Kurd who was arrested for breaching the mandatory dress code applicable in the country. On 4 January 2023, *Charlie Hebdo* published those caricatures in a special edition [27]. On the same day, its online shop was defaced and data was exfiltrated from its customer database. A malicious actor, presenting himself under the avatar 'Holy Souls', claimed responsibility for both those incidents. This avatar then proceeded to sell the exfiltrated data, which gathered the personal data of 230,000 clients of the magazine, on several cybercriminal forums [28].

According to U.S. authorities, Holy Souls is operated by a shell company called Emennet Pasargad or Iliyanet [29], which carries out influence and interference efforts for the benefit of the Islamic Revolutionary Guard Corps and of the Iranian Ministry of Intelligence and Security [30]. The publication of caricatures had already exposed Charlie Hebdo to cyberattack plots: in June 2021, the Lab Dookhtegan hacktivist group, which presents itself as dissident, revealed on its Telegram channel the existence of a plan devised by Emennet Pasargad in 2020 to destabilise the magazine [29]. Like the January 2023 incident, this project was likely aimed at retaliating against and intimidating *Charlie Hebdo*.

→ 2

IMPROVEMENT OF OFFENSIVE CAPABILITIES

A A CONSTANT SEARCH FOR STEALTH

Malicious actors are constantly refining their techniques to reduce the risks of detection, characterisation and attribution of their activities. These evolutions apply to the infrastructure they use, the initial intrusion method, the persistence mechanisms and the tools used to carry out their attacks.

Attackers rely on increasingly complex anonymisation networks that they create by compromising, for instance, peripheral or shared equipment (see our focus hereunder). This quest for stealth is also reflected in the use of inconspicuous interception capacities: this year, ANSSI dealt with incidents where signals intelligence (SIGINT) was most probably employed. These capabilities were used to intercept authentication secrets which circulated unencrypted in order to connect to the victim's network.

Anonymisation networks

An anonymisation network is a network of compromised machines communicating between themselves which is used by malicious groups to make their operations stealthier. These networks are used both for reconnaissance and for command and control (C2) actions. The same anonymisation network is often used by multiple actors, which makes the distinction and characterisation of its operators more difficult. Although anonymisation networks are not specific to intrusion sets which are reputedly Chinese, intrusion sets such as APT31 and Ke3chang distinguish themselves by an increasingly frequent and large-scale use of such mechanisms [32, 33].

To set up these networks, attackers typically compromise home routers[17], smart devices and other edge devices exposed on the Internet with specific malware. The frequent poor security of those equipment makes their compromise easier. Indeed:

- the vulnerability management of these types of equipment is often lacking, especially when it comes to applying constructors' updates;
- they are seldom supervised, in particular through logs, antivirus software or EDR[18], which makes the detection of attackers more difficult;
- the default passwords of their administration interfaces are seldom modified.

For several years now, ANSSI has observed that routers belonging to individuals, small and medium-sized enterprises (SME) and local or regional authorities are compromised and then incorporated to these anonymisation networks [34]. The security of these devices is a collective issue since, unbeknownst to them, they become the active intermediaries of espionage and cybercriminal campaigns. The upcoming European Cyber Resilience Act (CRA[19]) shall help make safer this type of equipment, which can be made part of anonymisation networks [35, 36].

[17] Usually called SOHO (Small Office/Home Office).

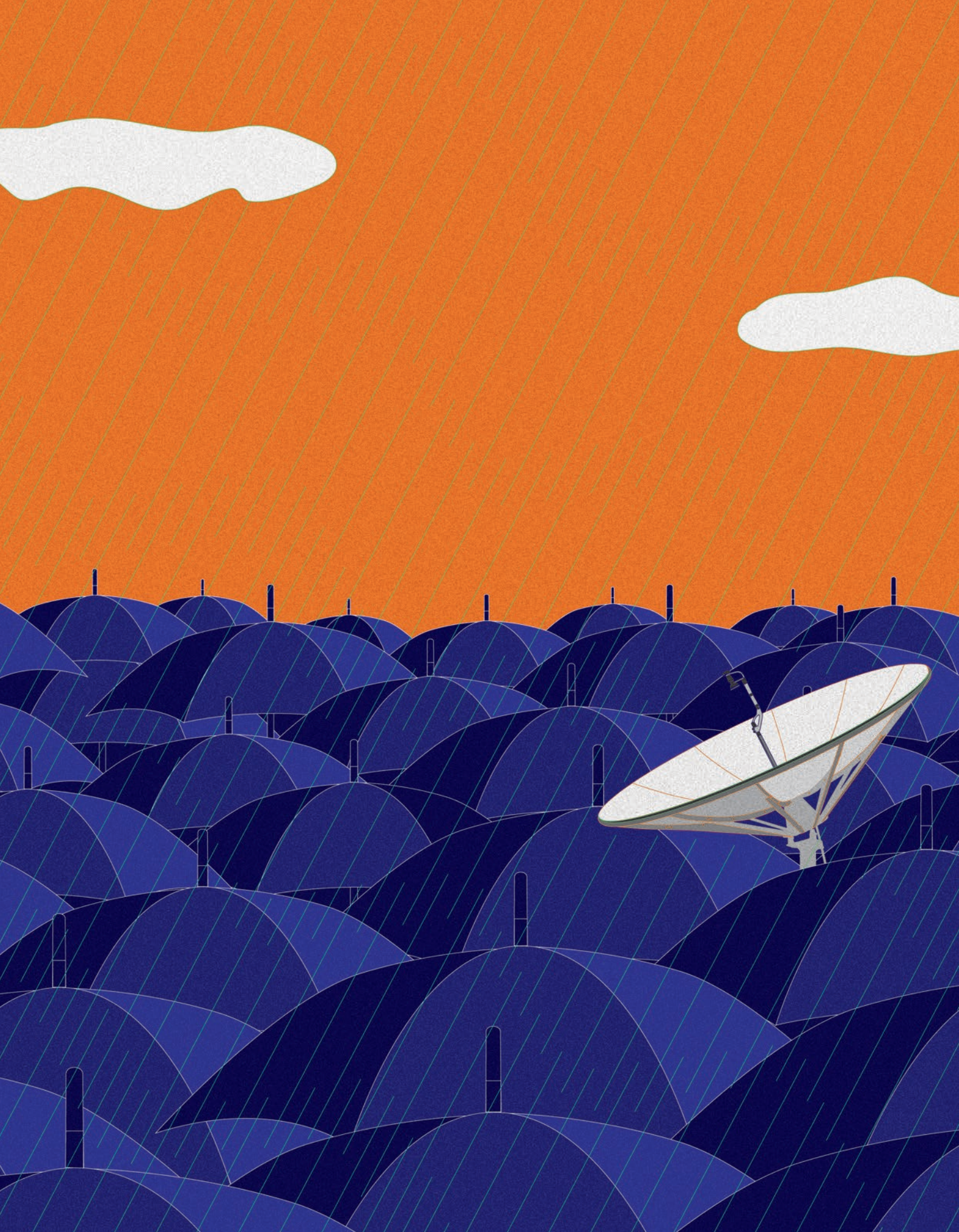
[18] Endpoint Detection & Response.

[19] Cyber Resilience Act.

After the initial intrusion, attackers pay particular attention to their stealth on the compromised network. In 2023, ANSSI dealt with incidents involving persistence mechanisms on edge devices (routers, email gateways, firewalls, etc.). In one of these incidents, attackers targeted an equipment which was not managed by the victim, thus drastically reducing the risk of detection by the latter. No malware was deployed, as the attackers simply set up redirection filters to exfiltrate emails of interest [37].

As regards tooling, ANSSI noticed an increasing use of so-called 'living-off-the-land' techniques, which involve using application and functionalities already existing on the compromised network[20] rather than specific tools deployed by the attacker, in order to avoid raising alerts. As a result of the confusion between the activities of the attacker and those of legitimate users, investigations are made more complex. This strategy was allegedly used by attackers deemed Russian or Chinese to target critical infrastructure in Ukraine [24] and in the United States [38, 39]. At last, attackers still take advantage of shared codes, adding to the complexity of monitoring and attributing malicious activities. The ShadowPad code, which has been employed since 2019 by different groups publicly linked to China [40, 41], was reportedly leveraged in 2023 to compromise a national power grid organisation in Asia [42]. ANSSI also noticed this malware in an incident impacting an entity with international reach located in France. ←

[20] For instance, legitimate system administration tools.



B **DIVERSIFICATION OF THE ECOSYSTEM AND OF CYBERCRIMINAL METHODS**

→ A number of factors contribute to the diversification of cybercriminal profiles observed over the past few years. The leak of builders and ransomware source codes such as LockBit, Babuk and Conti in 2021 and 2022 is encouraging the rise of groups and actors less experienced which build and then deploy their own ransomware [43, 44]. This trend is further reinforced by the growing availability of infostealers, which are marketed on forums and within private groups. Their increasing use has made it easier for cybercriminals with limited technical expertise to secure initial access [45, 46].

ANSSI also noted that attackers sometimes rely on intrusion guides sold or distributed on cybercriminal forums. These manuals detail the attack techniques that should be implemented to gain access to an information system, collect usernames and escalate privileges [47, 48], in particular with the aim of carrying out a ransomware attack. At the same time, ANSSI observed that the end of Conti's activities, which began in March 2022, followed by the dismantling of Qakbot in August 2023, led to the collapse and restructuring of the activities of some groups and affiliates [49].

Methods used by cybercriminals have also undergone significant changes. The trend towards ransoms based solely on data exfiltration (without deploying a ransomware), which had been observed since 2021 [7], was confirmed by massive campaigns in 2023 [50, 51]. This development leads to complications in the management of exfiltrated data volumes, which cybercriminal groups try to circumvent by using peer-to-peer transfer protocols (P2P) such as BitTorrent, or by forcing individuals who would like to receive the data to get in touch with the attackers [52]. Meanwhile, exploitation of several zero-day or one-day vulnerabilities by the CL0P cybercriminal group [21] demonstrates the ability of mature cybercriminal groups to lead large-scale attacks targeting commercial software likely to host sensitive data [53, 54]. ←

[21] Amongst which vulnerabilities in the GoAnywhere MFT, Papercut, MoveIT or SysAID solutions.

The dismantling of the Qakbot infrastructure

On 26 August 2023, an international operation involving the judicial and law enforcement authorities of the United States, Germany, Netherlands and France resulted in the dismantling of the command and control infrastructure of the Qakbot malicious network [55]. The anti-cybercrime section of the French national jurisdiction for the fight against organised crime (JUNALCO[22]) of the Paris Public Prosecutor's Office supervised the French part of this operation. Qakbot is a malware which had been active since 2008 and which was primarily used for the deployment of third-party malware such as offensive generic tools (Cobalt Strike) and ransomware (Royal, BlackBasta) on the victims' networks. The infected machines could be connected to each other and became part of a network of compromised machines (botnet).

ANSSI provided support to this dismantling by helping to identify and notify French victims. Although new Qakbot implants have been discovered in December 2023, the users of the botnet have been forced to stop their activities or to look for alternatives on the market, potentially investing in new malware [56, 57]. Dismantling actions therefore have direct consequences on the threat level as they significantly disturb the cybercriminal activities and force them to reorganise.

[22] Juridiction nationale de lutte contre la criminalité organisée.

Attack of a University Hospital by the BianLian group

On 21 June 2023, the Rennes University Hospital detected malicious activities on its information system and informed ANSSI, which deployed agents to support the hospital teams. The investigations highlighted the deep compromise of the information system as well as a data exfiltration carried out by the BianLian cybercriminal group.

Following the compromise, the hospital set up containment measures, including, in particular, a cut-off of Internet access, which was gradually restored over the following months. All medical activities were maintained but the impact of the attack on the organisation of the hospital and on the day-to-day tasks of the healthcare staff was significant. This incident shows the impacts that the compromise of an hospital information system can have, even without encryption actions. This type of incident requires a strong commitment as well as costly and long-term reconstruction and security work. However, the responsiveness of the teams meant that dearer consequences were avoided, the attack having been detected during its initial stage.

C INCREASED TARGETING OF MOBILE DEVICES FOR ESPIONAGE PURPOSES

→ ANSSI noticed an increase in the number of incidents involving the compromise of professional and personal mobile phones. The targeting of mobile devices usually requires substantial resources, in particular to identify and exploit vulnerabilities on phones with recent software versions and with no action required from the target[23]. Historically, these capabilities have been developed by governments with advanced offensive capabilities, but the private surveillance market keeps on expanding: some companies provide highly sophisticated malware not only to public actors, but also to private companies as well as to individuals with malicious motivations. The proliferation of commercial cyber intrusion capabilities significantly contributes to the global rise of the threat level.

This year, new information has been made public regarding malware specifically targeting mobile devices, amongst which BlastPass [58], Triangulation [59], Reign [60, 61] and Predator [62, 63]. Some of these publications have prompted the actors to cease their activities, such as Quadream, the company behind Reign [64]. Nevertheless, this ecosystem continues to reorganise itself.

This type of capacity is used both for targeting senior executives in administrations or strategic sector companies but also to spy on dissidents, journalists and human-rights activists who are present on the territory of the client or abroad [62]. Malware targeting mobile phones are also deployed in the context of armed conflicts, such as Infamous Chisel, a malware publicly linked to the Sandworm intrusion set, which was targeting mobile devices of the Ukrainian army [65, 66]. The Pegasus code, developed by the Israeli company NSO Group, is supposedly used since 2022 by Azerbaijani actors to spy on key-figures in Armenia [67, 68].

In 2023, France supported a Joint Statement on efforts to counter the proliferation and misuse of commercial spyware, which was adopted during the 2nd edition of the Summit for Democracy [69]. Along with the United Kingdom, and during the 2023 Paris Peace Forum, France also initiated consultations to counter the proliferation of commercial cyber intrusion capabilities [70]. ←

[23] Commonly known as 'zero-click' exploits.

→ 3

OPPORTUNITIES SEIZED BY ATTACKERS

A **EXPLOITATION OF NUMEROUS WEAKNESSES**

To compromise an information system, attackers can rely on numerous weaknesses, both technical and human: unsecured equipment exposed online, configuration errors, bad administration practices, bad management of access rights and of secrets, phishing, lack of hardening, 'zero-day' and 'one-day' vulnerabilities, etc. Amongst those weaknesses, exploitation of software vulnerabilities remains a prime gateway into numerous systems. Thanks to increasingly efficient and automated tools for reconnaissance and exploitation, attackers can, for instance, carry out scans and opportunistically obtain access for subsequent intrusions on an information system.

The use by publishers of software components developed by third parties also remain an important cause for concern. Whether it involves widely used libraries such as log4j [24], jackson-databind [25] or integrated solutions such as real-time operating systems [26], it is very difficult to ensure that all the products that use these components will be patched within a reasonable time, and national CSIRTs make considerable efforts to map them.

It should be noted that vulnerabilities affecting a component are not always exploitable, as it depends on how the component is used in each product. This detail makes the severity assessment of vulnerabilities even more complicated for all the actors involved (coordinators, users, systems integrators). The implementation of the SBOM [75] and VEX [76] standards by publishers provides a partial answer to this

[24] CVE-2021-44228, also known as Log4shell [71].

[25] CVE-2020-24616 [72], etc.

[26] CVE-2021-22156 targeting BlackBerry QNX [73].

CERT-FR scanning activities and vulnerability alerts

CERT-FR monitors vulnerabilities. For this purpose, it evaluates the severity of newly discovered vulnerabilities according to their exploitability, the prevalence of the impacted products and their online exposure. This allows preventive scanning actions to be carried out to determine entities likely to be targeted by attackers. Scans are conducted by CERT-FR with the aim of identifying and notifying exposed entities so that they can protect themselves or initiate searches for a potential breach [8]. In addition to this identification process, which may take time, other measures may be implemented. In particular, CERT-FR sends communications to its constituents, asking them to take the necessary measures according to their exposure to a given attack and issues alerts through telecommunication operators in accordance with article L33-14, paragraph 5, of the CPCE.

Actions carried out following the discovery of the ProxyLogon vulnerability (CVE-2021-26855) illustrate this approach. On 3 March 2021, one day after the vulnerability was disclosed, an alert was issued on the CERT-FR website [74]. A warning campaign was launched on 5 June. However, data from a scan performed on 9 March showed that around 70% of identified servers were running a version incompatible with the security updates provided by Microsoft. As a result, many entities had to apply the latest cumulative update before being able to patch the vulnerability. CERT-FR communicated several more times to encourage entities to apply the patch. Nevertheless, in June 2021, 5% of surveyed servers were still vulnerable. Even though it can be complex, keeping services up-to-date is paramount for the swift deployment of security patches.

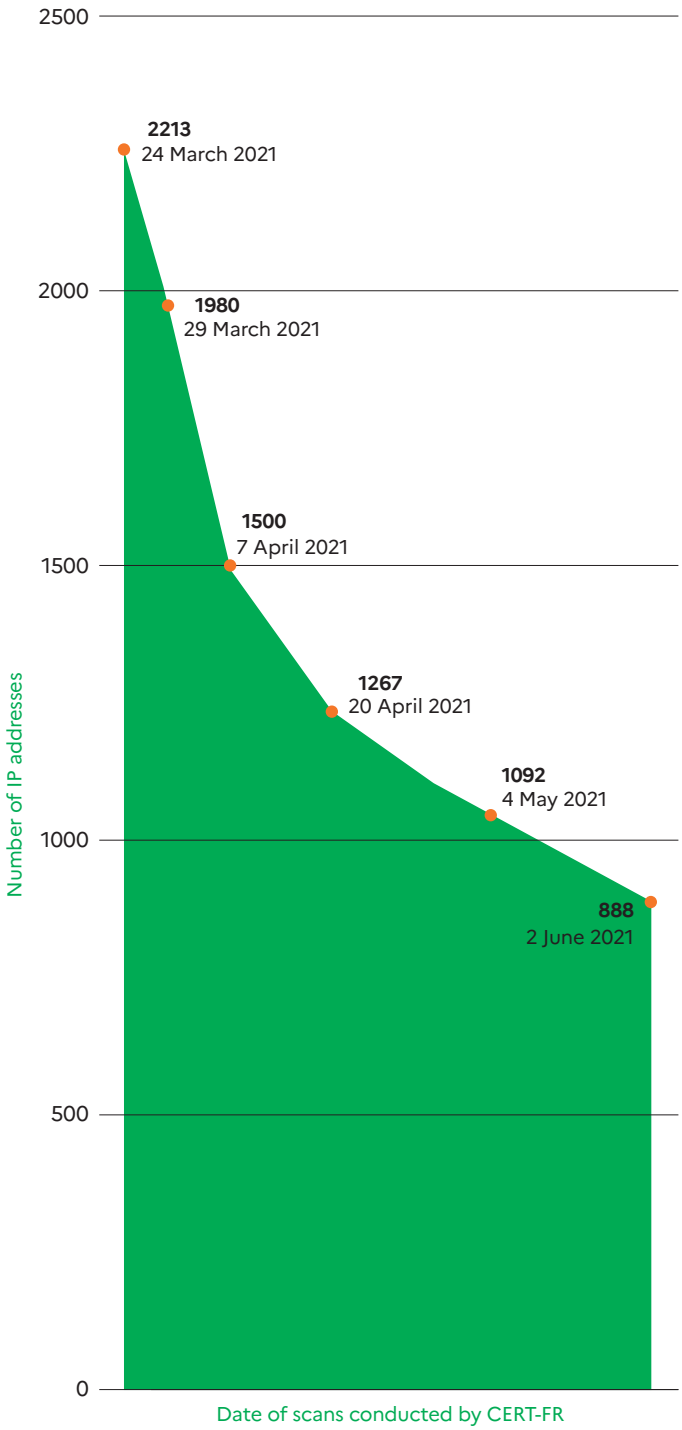
problem. The first one enables them to provide a list of components integrated in their products, while the second one enables them to inform their clients if a product is impacted by a newly discovered vulnerability in one of their components. Unfortunately, their use is still very limited.

The lack of security in development, test and integration environments can also be the source of another threat: the software supply chain attack. In this type of attack, malicious actors manage to tamper with a software in order to insert malicious code in it, which will subsequently enable them to gain access to the information systems of the users of this software. Some cases were treated by CERT-FR in the past, in particular the SolarWinds Orion supply chain attack in December 2020 [77] as well as the 3CX Desktop App supply chain attack in March 2023 [78].

Finally, ANSSI notices that a number of attackers take advantage of victims' lack of control over their own information systems. For this reason, subcontracting the whole or part of an information system to a managed service provider cannot be done without verifying the level of security of the services provided. Indeed, liability remains with the owner of the information system, especially when it is a strategic operator. ←

EXPLOITATION OF NUMERO
NESSES **A** EXPLOITATION O

→ French IP addresses vulnerable to CVE-2021-26855



B SOFTWARE VULNERABILITIES

In 2023, vulnerability exploitation was the source of numerous incidents handled by ANSSI. In a significant number of cases, patches were available when the vulnerability was exploited and a number of publications (notice, newsletter or security alert) were available on the CERT-FR website [79]. The five most exploited vulnerabilities of 2023 are listed in the table hereunder.

Warning: this ranking only considers events for which ANSSI or a service provider could confirm with a high degree of certainty that a given vulnerability was exploited.

CVE	VENDOR	CVSS SCORE [27]	CERT-FR REFERENCE
CVE-2021-21974	VMWARE	8.8	CERTFR-2023-ALE-015 CERTFR-2021-AVI-145
CVE-2023-20198	CISCO	10.0	CERTFR-2023-ALE-011 CERTFR-2023-AVI-0878
CVE-2023-3519	CITRIX	9.8	CERTFR-2023-ALE-008 CERTFR-2023-AVI-0568
CVE-2023-22518	ATLASSIAN	9.8	CERTFR-2023-AVI-0899 CERTFR-2023-ACT-048
CVE-2023-34362	PROGRESS SOFTWARE	9.8	CERTFR-2023-ALE-005

In addition, other vulnerabilities made public in 2023 were considered particularly significant due to their severity and because of the risk of exploitation and the potential consequences for ANSSI's constituents.

CVE	VENDOR	CVSS SCORE	CERT-FR REFERENCE
CVE-2023-23997	MICROSOFT	8.8	CERTFR-2023-ALE-002 CERTFR-2023-AVI-0231
CVE-2023-27997	FORTINET	9.8	CERTFR-2023-ALE-004 CERTFR-2023-AVI-0451
CVE-2023-35078	IVANTI	9.8	CERTFR-2023-ALE-009 CERTFR-2023-AVI-0584
CVE-2023-4966	CITRIX	9.4	CERTFR-2023-ALE-012 CERTFR-2023-AVI-0823
CVE-2023-36884	MICROSOFT	8.8	CERTFR-2023-ALE-006
CVE-2023-42117	EXIM	8.1	CERTFR-2023-ALE-010
CVE-2022-41328	FORTINET	6.7	CERTFR-2023-ALE-001 CERTFR-2023-AVI-0199
CVE-2023-37580	ZIMBRA	6.1	CERTFR-2023-ALE-007 CERTFR-2023-AVI-0546

[27] *Common Vulnerability Scoring System* (CVSS) is a standardised system for assessing the severity of vulnerabilities according to objective and measurable criteria. This assessment is based on three measurable metrics: base metrics, temporal metrics and environmental metrics. The score indicated above is the base metrics. It ranges between 0 and 10, 10 corresponding to the most critical vulnerabilities. More information is available on *www.first.org/cvss*.

Amongst vulnerabilities mentioned above, CVE-2021-21974, which targets VMWare ESXi [80] and CVE-2023-34362, which impacts the Progress Software MOVEit Secure Managed File Transfer solution [56], were the subject of financially motivated and opportunistic exploitation campaigns. The first one led to encryption of data on the hypervisor through the use of a ransomware called 'ESXiArgs', whereas in the second campaign, publicly attributed to the cybercriminal group CL0P, the attacker threatened victims with data exfiltration and offered it for sale. In the same way, CVE-2023-22518, which affected the Confluence product from Atlassian, may have been leveraged to deploy ransomware. In those examples, attackers took advantage of the fact that equipment hosting sensitive data was exposed online, as exploitation of the vulnerability was sufficient to access this data. It should be noted that the exploitation campaign of CVE-2021-21974 was observed in 2023, despite the fact that a patch had been released since February 2021 and that the exploitation code had been made public in May 2021.

As in previous years, several critical vulnerabilities published in 2023 target network devices (CVE-2023-20198, CVE-2023-27997, CVE-2023-3519, CVE-2023-4966, CVE-2022-41328). Amongst those some were security appliances, including Virtual Private Network (VPN) gateways. Those devices are prime targets for attackers as they offer persistent and stealthy access to the victim's information system whilst allowing for traffic interception.

Finally, email services were particularly targeted in 2023 by attackers trying either to access emails or simply to compromise desktops or user accounts. Vulnerabilities can, for instance, enable code execution in the victim's web browser (CVE-2023-37580 targeting a Zimbra product). They can also be exploited to leak authentication secrets (such as CVE-2023-23397 for Microsoft Outlook). Attackers target the whole email processing system, including externalised email security appliances (see focus hereunder).

IDENTIFIER	CVE-2021-21974	PUBLICATION DATE	24/02/2021
VENDOR	VMWARE	CVSS SCORE	8.8

On 3 February 2023, ANSSI was informed of a malicious campaign against VMware ESXi hypervisors for ransomware deployment. The SLP service, which was the subject of several patches over the last few years (CVE-2020-3992 and CVE-2021-21974) was once again targeted by this campaign. The first wave of attacks encrypted the configuration files of virtual machines. As a result, it was still possible to recover data from the storage. A second wave initiated on 8 February 2023 went further and encrypted more data in larger files, making their recovery more complicated, or even impossible. CVE-2021-21974 enables arbitrary remote code execution by the attacker. ESXi hypervisors from versions 6.x to 6.7 were targeted by this attack [80, 81].

IDENTIFIER	CVE-2023-20198	PUBLICATION DATE	16/10/2023
VENDOR	CISCO	CVSS SCORE	10.0

Between 16 and 22 October 2023, Cisco made public the existence of two vulnerabilities in its IOS XE administration Web interface (webui)[28]. These vulnerabilities allow an unauthenticated attacker to create a highly privileged user. Actively exploited by attackers, they were giving unlimited access as well as the possibility to modify configuration of the vulnerable system, which effectively means gaining full control of it. All devices which exposed the IOS XE administration web interface were considered compromised as patching was not sufficient to evict the attacker [82, 83].

[28] CVE-2023-20198 and CVE-2023-20273.

IDENTIFIER	CVE-2023-3519	PUBLICATION DATE	19/07/2023
VENDOR	CITRIX	CVSS SCORE	9.8

Multiple vulnerabilities were discovered in July 2023 in the Citrix NetScaler ADC and NetScaler Gateway products. The most critical one allowed arbitrary remote code execution by an unauthenticated attacker if the device was configured as a gateway [29] or as an AAA virtual server [30]. Clients were invited to migrate to a supported and fixed version. On 20 July 2023, CISA published indicators of compromise, guidance and tooling for detecting compromised equipment [84, 85, 86].

IDENTIFIER	CVE-2023-22518	PUBLICATION DATE	31/10/2023
VENDOR	ATLASSIAN	CVSS SCORE	9.8

In October 2023, a vulnerability was discovered in the Confluence collaboration platform (Data Centre and Server versions) developed by Atlassian. The exploitation of the vulnerability allows the attacker to tamper with the integrity of the data stored in the tool. The vendor reported incidents related to this vulnerability resulting in ransomware deployment [87, 88].

IDENTIFIER	CVE-2023-34362	PUBLICATION DATE	21/04/2022
VENDOR	PROGRESS SOFTWARE	CVSS SCORE	9.8

On 31 May 2023, a vulnerability was discovered in the Progress Software MOVEit file transfer solution. An SQL injection allows an unidentified attacker to access, extract and modify the application database. Depending on the database engine used (MySQL, Microsoft SQL Server or Azure SQL), the structure and content of the database may be deleted by an attacker. The exploitation of the vulnerability can also make data exfiltration possible through the deployment of webshells. The massive exploitation of this vulnerability was claimed by the CL0P cybercriminal group in June 2023. More than 80 potential victim names were published by the attackers for extortion purposes [53].

IDENTIFIER	CVE-2023-23997	PUBLICATION DATE	14/03/2023
VENDOR	MICROSOFT	CVSS SCORE	8.8

In March 2023, Microsoft provided information on a vulnerability targeting a number of versions of the Outlook product for Windows. This vulnerability, actively exploited in targeted attacks, enables an attacker to retrieve the NetNTLMv2 hash without any intervention from the legitimate user [89, 90]. A patch was also published in May for a second vulnerability (CVE-2023-29324) which made the exploitation of CVE-2023-23397 still possible if the March 2023 patch had not been applied [37].

[29] Gateway: VPN virtual server, ICA Proxy, CVPN, RDP Proxy.

[30] AAA virtual server.

IDENTIFIER	CVE-2023-27997	PUBLICATION DATE	13/06/2023
VENDOR	FORTINET	CVSS SCORE	9.8

A vulnerability, made public in June 2023, allows arbitrary remote code execution by an unauthenticated attacker on Fortinet products offering a VPN SSL feature. This vulnerability is exploitable only if the SSL VPN is activated. As the sole application of patches is not sufficient, CERT-FR recommends in its warning to analyse systems with the indicators of compromise provided by Fortinet and to apply the hardening measures specified by the vendor [91, 92].

IDENTIFIER	CVE-2023-35078	PUBLICATION DATE	25/07/2023
VENDOR	IVANTI	CVSS SCORE	9.8

A vulnerability targeting the Endpoint Manager Mobile (EPMM) product was discovered in June 2023. It enables an attacker to gain unauthenticated access to specific API paths in order to retrieve personal data from users. Through this vulnerability, an attacker can also modify the configuration of the EPMM product and create an administrator account.

Four days later, Ivanti made a second vulnerability public (CVE-2023-35081) which enables an attacker who has administrator rights to write arbitrary files on the server, ultimately leading to arbitrary remote code execution. This vulnerability was actively exploited in targeted attacks, in conjunction with CVE-2023-35078 to circumvent administrator authentication. On 1st August 2023, CISA, along with the Norwegian cybersecurity agency (NCSC-NO), published a notice about CVE-2023-35078 and CVE-2023-35081. The first one may have been exploited since at least April 2023 [93, 94, 95]. ←

↓

Vulnerability in the Barracuda Email Security Gateway solution

On 23 May 2023, Barracuda Networks, a U.S. company, announced that one of its email security products was affected by a critical security vulnerability (CVE-2023-2868). These devices, which filter and analyse emails, could be abused during the analysis of malicious attachments. Files designed to exploit the vulnerability allowed unrestricted arbitrary remote code execution, including the installation of backdoors. Compromise of such devices is enough to obtain all the emails of the target.

According to Mandiant [96, 97], this vulnerability had been exploited as early as October 2022 by attackers carrying out espionage operations on behalf of the Chinese government. Attackers were particularly careful about the stealth of this zero-day exploitation, in particular by crafting emails designed to be flagged by the anti-spam filter, downstream of the vulnerable device. This way, the malicious email and its attachment were analysed by the Barracuda solution without the recipient's knowledge. Attackers tried to compromise exclusively networks of interest to them[31], targeting primarily devices belonging to governmental entities.

Numerous exposed devices were the target of exploitation campaigns, whether public or not, over the last few years. The research and implementation efforts needed for such vulnerabilities suggest that attackers allocate substantial resources for compromising systems that are exposed and which usually do not benefit from security monitoring.

[25] Only 5% are thought to have been compromised, i.e. several thousand devices.

C ORGANISATION OF MAJOR EVENTS

Major events provide attackers with additional opportunities to act. They require the implementation of numerous information systems – often interconnected and sometimes created for the occasion – by a multitude of players with heterogeneous levels of security. Attackers can take advantage of this extensive exposure to gather information on or extort organisers and participants. They are also likely to exploit the media coverage to tarnish the image of the host country or even disrupt the event. In addition to the aforementioned espionage campaigns in the run-up to the NATO summit in Vilnius, attackers have reportedly carried out DDoS attacks and a hack-and-leak operation during the event [98, 99].

The Paris 2024 Olympic and Paralympic Games could be targeted by such attacks. The 2023 Rugby World Cup in France has paved the way for France to host major events [100]. ANSSI did not notice any significant change in the threat before or during the competition, and no large-scale computer attack was detected. The event also provided an opportunity to test a strengthened detection, warning and incident response system ahead of the 2024 Olympic Games.

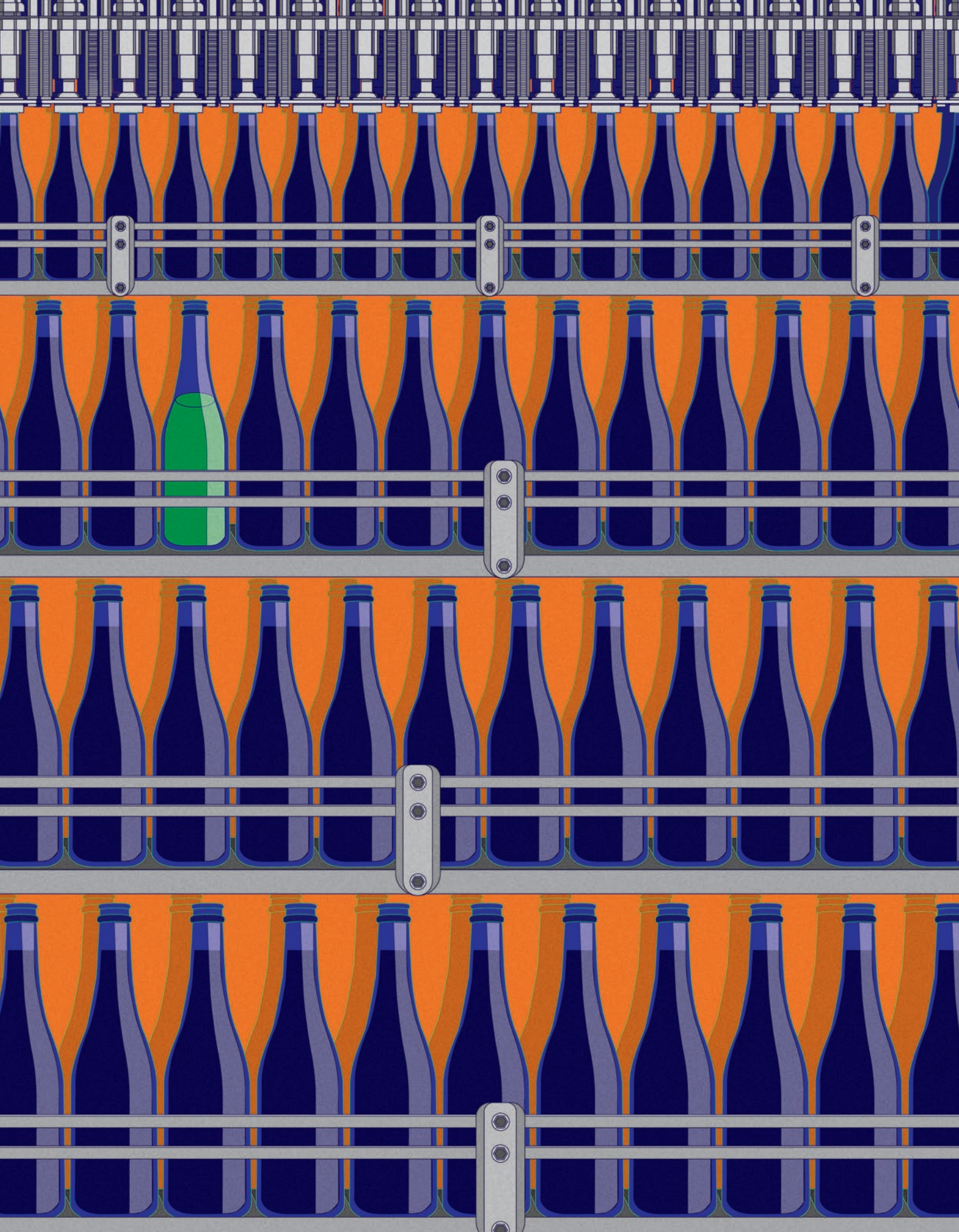
ANSSI's role during the 2024 Olympic and Paralympic Games

The steering of cyberattacks prevention strategy for the 2024 Olympic and Paralympic games has been assigned to ANSSI by the French Prime Minister. The measures taken by ANSSI, in close collaboration with the various entities involved in the organisation of the Games – and in particular the Inter-ministerial Delegation to the Olympic and Paralympic Games (DIJOP[32]), the Interior and Overseas Ministry (MIOM[33]) and the organisation committee of the Olympic and Paralympic Games (Paris 2024) – are articulated around five main axes:

- improving the knowledge of the threats faced by the Games;
- securing critical information systems;
- protecting sensitive data;
- increasing awareness of the Games' ecosystem;
- getting ready to intervene in the event of an attack during the Games.

The security actions are tailored according to the needs of the various entities involved. They include security audits and technical guidance for critical entities, a specific program for sensitive entities and access to tools and services, in particular for estimating security levels and crisis management. An awareness campaign is also underway for several hundred players in the Games ecosystem. It provides information about the threats against major sporting events and helps spreading best practices. To this end, in August 2023, CERT-FR published a first assessment of the threat against major sporting events along with recommendations [100].

At last, ANSSI has defined, in cooperation with the various government services involved in the preparation of the Games, a reinforced monitoring and alerting system for IT incidents. It includes specific measures designed to withstand an increased operational activity. Several crisis exercises have also been organised in 2023 to prepare for a collective response in the event of an attack during the Games.



CONCLUSION

In 2023, ANSSI observed significant changes in the structure and methods of attackers. Strategic and industrial espionage operations remain at a high level and are increasingly focused on individuals and non-governmental entities that create, host or transmit sensitive data. To achieve their objectives, threat actors fine-tune their techniques to avoid detection and monitoring, or even identification. Financially motivated attacks also remain at a high level, fuelled by actors with increasingly diverse profiles. Widely available tools and techniques are leveraged by the cybercriminal ecosystem to target particularly vulnerable targets, with sometimes dire consequences.

In a context of international tensions, there has been a resurgence of destabilisation activities. DDoS attacks, which have a limited impact, remain the most common but the threat of operations against critical sectors on a European Union scale, such as coordinated disclosure of exfiltrated data and sabotage, cannot be excluded. Despite the efforts undertaken to improve the security of some sectors, attackers keep on taking advantage of the same weaknesses to gain access to networks, in particular through the exploitation of unpatched vulnerabilities and as result of the victims' lack of control over their own information systems. These tendencies contribute to the overall increase of the cyber threat level.

The regulatory framework in which ANSSI operates is also evolving. The Network and Information System Security directive (also known as 'NIS2'), which was published on 27 December 2022 in the Official Journal of the European Union, must be transposed into national law before the end of 2024. For ANSSI, the challenge will be to deploy an efficient and sustainable scheme, enabling thousands of new regulated operators to be included within the Agency's scope, whilst adapting the tools and services available to them. This transposition into national law will also have to be coordinated with other schemes such as the REC [34] and DORA [35] European legislations.

The attackers' structure and methods will undoubtedly undergo changes in 2024, as France prepares to host the Olympic and Paralympic Games. To meet these challenges, ANSSI calls for security to be considered right from the design stage of projects, for dedicated administration workstations and network to be set up, for information systems to be made more robust, in particular through regular use of the automated audit services of ANSSI [36], and for the development of detection capabilities. The Agency also recommends the rigorous application of vulnerability management and operational readiness policies, the implementation of an information system backup strategy and elaboration of business continuity and resiliency plans. ANSSI and CERT-FR will continue sharing threat assessments and useful resources on their websites to protect oneself against the most prevalent threats and vulnerabilities.

[34] Directive (UE) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities.

[35] Regulation (UE) 2022/2554 Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector.

[36] Available for regulated operators and the public sector, these services can be used to assess Active Directory security and for mapping online exposure.

APPENDIX
BIBLIOGRAPHY

[1]
CERT-FR
État de la menace ciblant le secteur des télécommunications.
18 December 2023.
https://www.cert.ssi.gouv.fr/cti/CERTFR-2023-CTI-010/

[2]
SÉNAT
Pour une coordination de la cyberdéfense plus offensive dans la loi de programmation militaire 2024-2030.
24 May 2023.
https://www.senat.fr/rap/r22-638/r22-6384.html

[3]
DGSI
La DGSI au cœur de l'organisation française de cyberdéfense.
23 June 2021.
https://www.dgsi.interieur.gouv.fr/decouvrir-la-dgsi/nos-missions/cyberdefense/la-dgsi-au-coeur-de-lorganisation-francaise-de

[4]
GOOGLE
Active North Korean campaign targeting security researchers.
31 October 2023.
https://blog.google/threat-analysis-group/active-north-korean-campaign-targeting-security-researchers/

[5]
ZDNET
Les attaques par rançongiciel repartent à la hausse en France.
19 December 2023.
https://www.zdnet.fr/actualites/exclusif-les-attaques-par-rancongiciel-repartent-a-la-hausse-en-france-39963068.htm

[6]
ANSSI
Cyber Threat Overview 2022.
10 February 2023.
https://www.cert.ssi.gouv.fr/cti/CERTFR-2023-CTI-002/

[7]
CERT-FR
Cyber Threat Overview 2021.
9 March 2022.
https://www.cert.ssi.gouv.fr/cti/CERTFR-2022-CTI-004.pdf

[8]
CERT-FR
Scans et services.
https://www.cert.ssi.gouv.fr/scans

[9]
PALO ALTO
Novel News on Cuba Ransomware: Greetings From Tropical Scorpius.
9 August 2022.
https://unit42.paloaltonetworks.com/cuba-ransomware-tropical-scorpius/

[10]
TREND MICRO
Void Rabisu's Use of RomCom Backdoor Shows a Growing Shift in Threat Actors' Goals.
30 May 2023.
https://www.trendmicro.com/en_us/research/23/e/void-rabisu-s-use-of-romcom-backdoor-shows-a-growing-shift-in-th.html

[11]
MICROSOFT
Storm-0978 attacks reveal financial and espionage motives.
11 July 2023.
https://www.microsoft.com/en-us/security/blog/2023/07/11/storm-0978-attacks-reveal-financial-and-espionage-motives/

[12]
CERT-UA
Cyberattack on DELTA system users using RomCom/FateGrab/StealDeal malware.
18 December 2022.
https://cert.gov.ua/article/3349703

[13]
BLACKBERRY
RomCom Threat Actor Suspected of Targeting Ukraine's NATO Membership Talks at the NATO Summit.
8 July 2023.
https://blogs.blackberry.com/en/2023/07/romcom-targets-ukraine-nato-membership-talks-at-nato-summit

[14]
ANSSI
Les dénis de service distribués (DDOS).
5 September 2023.
https://cyber.gouv.fr/publications/les-denis-de-service-distribues-ddos

[15]
ANSSI
Comprendre et anticiper les attaques DDoS.
20 March 2015.
https://cyber.gouv.fr/publications/comprendre-et-anticiper-les-attaques-ddos

[16]
MANDIANT
Hacktivists Collaborate with GRU-sponsored APT28.
23 September 2022.
https://www.mandiant.com/resources/blog/gru-rise-telegram-minions

[17]
LE PARISIEN
Niger : les hackers d'Anonymous Sudan menacent la France de représailles en cas d'intervention militaire.
1 August 2023.
https://www.leparisien.fr/high-tech/niger-les-hackers-danonymous-sudan-menacent-la-france-de-represailles-en-cas-dintervention-militaire-01-08-2023-P3YNIDEVEFEDFDXLUUN65WMSTQ.php

[18]
POLITICO
How hackers piled onto the Israeli-Hamas conflict. 15 October 2023.
https://www.politico.eu/article/israel-hamas-war-hackers-cyberattacks/

[19]
SEKOIA
Following NoName057(16) DDoSia Project's Targets.
23 June 2023.
https://blog.sekoia.io/following-noname05716-ddosia-projects-targets/

[20]
CERT-UA
Cyberattack on the Ukrinform information and communication system.
27 January 2023.
https://cert.gov.ua/article/3718487

[21]
CERT-UA
WinRAR as a "cyber weapon". UAC-0165 (probably Sandworm) destructive cyberattack on Ukraine's public sector using RoarBat.
29 April 2023.
https://cert.gov.ua/article/4501891

[22]
CERT-UA
Peculiarities of destructive cyberattacks against Ukrainian providers.
15 October 2023.
https://cert.gov.ua/article/6123309

[23]
REUTERS
Russian hackers were inside Ukraine telecoms giant for months.
5 January 2024.
https://www.reuters.com/world/europe/russian-hackers-were-inside-ukraine-telecoms-giant-months-cyber-spy-chief-2024-01-04/

[24]
MANDIANT
Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology.
9 November 2023.
https://www.mandiant.com/resources/blog/sandworm-disrupts-power-ukraine-operational-technology

[25]
SEKTORCERT
The attack against Danish, critical infrastructure.
November 2023.
https://sektorcert.dk/wp-content/uploads/2023/11/SektorCERT-The-attack-against-Danish-critical-infrastructure-TLP-CLEAR.pdf

[26]
CANADIAN CENTRE FOR CYBER SECURITY
The cyber threat to Canada's oil and gas sector.
21 June 2023.
https://www.cyber.gc.ca/en/guidance/cyber-threat-canadas-oil-and-gas-sector

[27]
FRANCE INFO
Iran : « La cariture est une arme politique utilisée par les mollahs donc on l'a utilisée contre eux » dans *Charlie Hebdo*, explique Riss.
3 January 2023.
https://www.francetvinfo.fr/economie/medias/charlie-hebdo/iran-la-caricature-est-une-arme-politique-utilisee-par-les-mollahs-donc-on-l-a-utilisee-contre-eux-dans-charlie-hebdo-explique-riss_5577969.html

[28]
MICROSOFT
Iran responsible for *Charlie Hebdo* attacks.
3 February 2023.
https://blogs.microsoft.com/on-the-issues/2023/02/03/dtac-charlie-hebdo-hack-iran-neptunium/

[29]
FBI
Context and Recommendations to Protect Against Malicious Activity by Iranian Cyber Group Emennet Pasargad.
26 January 2022.
https://www.ic3.gov/Media/News/2022/220126.pdf

[30]
U.S. DEPARTMENT OF THE TREASURY
Treasury Sanctions Iran Cyber Actors for Attempting to Influence the 2020 U.S. Presidential Election.
18 November 2021.
https://home.treasury.gov/news/press-releases/jy0494

[31]
LAB DOOKHTEGAN
https://t.me/lab_dookhtegan

[32]
CERT-FR
Campagne d'attaque du mode opératoire APT31 : description, contre-mesures et code.
15 December 2021.
https://www.cert.ssi.gouv.fr/cti/CERTFR-2021-CTI-012/

[33]
BUNDESAMT FÜR VERFASSUNGSSCHUTZ
Cyber-Brief Nr. 02/2023.
31 August 2023.
https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/cyberabwehr/2023-02-bfv-cyber-brief.pdf

[34]
CERT-FR
Synthèse de la menace ciblant les collectivités territoriales.
23 October 2023.
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-008.pdf

[35]
EUROPEAN COMMISSION
Cyber Resilience Act.
15 September 2022.
https://digital-strategy.ec.europa.eu/fr/library/cyber-resilience-act

[36]
EUROPEAN COUNCIL
Cyber resilience act: Council and Parliament strike a deal on security requirements for digital products.
30 November 2023.
https://www.consilium.europa.eu/en/press/press-releases/2023/11/30/cyber-resilience-act-council-and-parliament-strike-a-deal-on-security-requirements-for-digital-products/

[37]
CERT-FR
Campagnes d'attaques du mode opératoire APT28 depuis 2021.
26 October 2023.
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-009.pdf

[38]
CISA
People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection.
24 May 2023.
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a

[39]
MICROSOFT
Volt Typhoon targets US critical infrastructure with living-off-the-land techniques.
24 May 2023.
https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/

[40]
SENTINELONE
ShadowPad. A Masterpiece of Privately Sold Malware in Chinese Espionage.
19 August 2021.
https://www.sentinelone.com/labs/shadowpad-a-masterpiece-of-privately-sold-malware-in-chinese-espionage/

[41]
SECUREWORKS
ShadowPad Malware Analysis.
15 February 2022.
https://www.secureworks.com/research/shadowpad-malware-analysis

[42]
SYMANTEC
Redfly: Espionage Actors Continue to Target Critical Infrastructure.
12 September 2023.
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/critical-infrastructure-attacks

[43]
TALOS
Code leaks are causing an influx of new ransomware actors.
7 August 2023.
https://blog.talosintelligence.com/code-leaks-new-ransomware-actors/

[44]
BANKINFOSECURITY
Why Criminals Keep Reusing Leaked Ransomware Builders.
30 August 2023.
https://www.bankinfosecurity.com/blogs/criminals-keep-reusing-leaked-ransomware-builders-p-3503

[45]
SEKOIA
Overview of the Russian-speaking infostealer ecosystem: the distribution.
11 April 2023.
https://blog.sekoia.io/overview-of-the-russian-speaking-infostealer-ecosystem-the-distribution/

[46]
SEKOIA
Overview of the Russian-speaking infostealer ecosystem: the logs.
11 May 2023.
https://blog.sekoia.io/overview-of-the-russian-speaking-infostealer-ecosystem-the-logs/

[47]
ANALYST1
The Ransomware Diaries: Volume 2.
25 April 2023.
https://analyst1.com/wp-content/uploads/2023/04/Ransomware-diaries-vol2-v2.pdf

[48]
BLEEPING COMPUTER
Angry Conti ransomware affiliate leaks gang's attack playbook.
5 August 2021.
https://www.bleepingcomputer.com/news/security/angry-conti-ransomware-affiliate-leaks-gangs-attack-playbook/

[49]
CERT-FR
FIN12 : Un groupe cybercriminel aux multiples rançongiciels.
18 September 2023.
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-007.pdf

[50]
NCC GROUP
NCC Group Monthly Threat Pulse – June 2023.
20 July 2023.
https://www.nccgroup.com/ae/newsroom/ncc-group-monthly-threat-pulse-june-2023/

[51]
LOGPOINT
Emerging Threat: BianLian Ransomware's Shapeshift to Encryption-less Extortion.
22 June 2023.
https://www.logpoint.com/en/blog/emerging-threat/bianlian-ransomware/

[52]
UNIT 42
CL0P Seeds ^_- Gotta Catch Em All!
29 September 2023.
https://unit42.paloaltonetworks.com/cl0p-group-distributes-ransomware-data-with-torrents/

[53]
CERT-FR
Synthèse sur l'exploitation d'une vulnérabilité dans MOVEit Transfer.
5 July 2023.
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-ALE-005.pdf

[54]
MICROSOFT
Microsoft has discovered exploitation of a 0-day vulnerability in the SysAid IT support software.
9 November 2023.
https://twitter.com/MsftSecIntel/status/1722444141081076219

[55]
CERT-FR
Démantèlement du botnet Qakbot.
18 September 2023.
https://www.cert.ssi.gouv.fr/cti/CERTFR-2023-CTI-006/

[56]
MICROSOFT
Microsoft has identified new Qakbot phishing campaigns.
16 December 2023.
https://twitter.com/MsftSecIntel/status/1735856754427047985

[57]
COFENSE
Are DarkGate and PikaBot the new QakBot?
20 November 2023.
https://cofense.com/blog/are-darkgate-and-pikabot-the-new-qakbot/

[58]
THE CITIZEN LAB
BLASTPASS. NSO Group iPhone Zero-Click, Zero-Day Exploit Captured in the Wild.
7 September 2023.
https://citizenlab.ca/2023/09/blastpass-nso-group-iphone-zero-click-zero-day-exploit-captured-in-the-wild/

[59]
KASPERSKY
Operation Triangulation.
1 June 2023.
https://securelist.com/trng-2023/

[60]
THE CITIZEN LAB
Sweet QuaDreams. A First Look at Spyware Vendor QuaDream's Exploits, Victims, and Customers.
11 April 2023.
https://citizenlab.ca/2023/04/spyware-vendor-quadream-exploits-victims-customers/

[61]
MICROSOFT
DEV-0196: QuaDream's "KingsPawn" malware used to target civil society in Europe, North America, the Middle East, and Southeast Asia.
11 April 2023.
https://www.microsoft.com/en-us/security/blog/2023/04/11/dev-0196-quadreams-kingspawn-malware-used-to-target-civil-society-in-europe-north-america-the-middle-east-and-southeast-asia/

[62] AMNESTY
Dans les mailles de Predator. La menace mondiale d'un logiciel espion « réglementé par l'Union européenne ».
9 October 2023.
https://www.amnesty.org/fr/documents/act10/7246/2023/fr/

[63]
EUROPEAN INVESTIGATIVE COLLABORATIONS
Predator Files. October 2023.
https://eic.network/projects/predator-files.html

[64]
CALCALIST
Offensive cyber company QuaDream shutting down amidst spyware accusations.
16 April 2023.
https://www.calcalistech.com/ctechnews/article/hy78kiym2

[65]
NCSC-UK
Infamous Chisel
Malware Analysis Report.
31 August 2023.
https://www.ncsc.gov.uk/static-assets/documents/malware-analysis-reports/infamous-chisel/NCSC-MAR-Infamous-Chisel.pdf

[66]
CISA
Infamous Chisel Malware Analysis Report.
31 August 2023.
https://www.cisa.gov/news-events/analysis-reports/ar23-243a

[67]
ACCESS NOW
Hacking in a war zone: Pegasus spyware in the Azerbaijan-Armenia conflict.
25 May 2023.
https://www.accessnow.org/publication/armenia-spyware-victims-pegasus-hacking-in-war/

[68]
THE CITIZEN LAB
Armenia-Azerbaijan Conflict. Pegasus infections – Technical Brief.
25 May 2023.
https://citizenlab.ca/2023/05/cr1-armenia-pegasus

[69]
FRANCE DIPLOMATIE
Cyber sécurité – Lutte contre la prolifération de la vente de logiciels espions.
31 March 2023.
https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/securite-desarmement-et-non-proliferation/actualites-et-evenements-lies-a-la-securite-au-desarmement-et-a-la-non/2023/article/cyber-securite-lutte-contre-la-proliferation-de-la-vente-de-logiciels-espions

[70]
LE MONDE
Cybersécurité : la France à l'initiative d'un nouveau texte sur les logiciels commerciaux « offensifs ».
10 November 2023.
https://www.lemonde.fr/pixels/article/2023/11/10/cybersecurite-la-france-a-l-initiative-d-un-nouveau-texte-sur-les-logiciels-commerciaux-offensifs_6199348_4408996.html

[71]
CERT-FR
Vulnérabilité dans Apache Log4j.
10 décembre 2021.
https://www.cert.ssi.gouv.fr/alerte/CERTFR-2021-ALE-022/

[72]
CERT-FR
Bulletin d'actualité CERTFR-2021-ACT-053.
20 December 2021.
https://www.cert.ssi.gouv.fr/actualite/CERTFR-2021-ACT-053/

[73]
CERT-FR
Multiples vulnérabilités dans des systèmes d'exploitation temps réel.
18 August 2021.
https://www.cert.ssi.gouv.fr/avis/CERTFR-2021-AVI-639/

[74]
CERT-FR
Multiples vulnérabilités dans Microsoft Exchange Server.
3 March 2021.
https://cert.ssi.gouv.fr/alerte/CERTFR-2021-ALE-004/

[75]
CISA
Software Bill of Material (SBOM).
https://www.cisa.gov/sbom

[76]
CISA
Vulnerability Exploitability eXchange (VEX) - Use Cases.
April 2022.
https://www.cisa.gov/sites/default/files/2023-01/VEX_Use_Cases_Aprill2022.pdf

[77]
CERT-FR
Présence d'un code malveillant dans SolarWinds Orion.
14 December 2022.
https://www.cert.ssi.gouv.fr/alerte/CERTFR-2020-ALE-026/

[78]
CERT-FR
Compromission de l'application 3CX Desktop App.
31 March 2023.
https://www.cert.ssi.gouv.fr/alerte/CERTFR-2023-ALE-003/

[79]
CERT-FR
https://www.cert.ssi.gouv.fr

[80]
CERT-FR
Multiples vulnérabilités dans les produits VMWare.
24 February 2021.
https://www.cert.ssi.gouv.fr/avis/CERTFR-2021-AVI-145/

[81]
CERT-FR
Campagne d'exploitation d'une vulnérabilité affectant VMware ESXi.
3 February 2023.
https://www.cert.ssi.gouv.fr/alerte/CERTFR-2023-ALE-015/

[82]
CERT-FR
Multiples vulnérabilités dans Cisco IOS XE.
17 October 2023.
https://www.cert.ssi.gouv.fr/alerte/CERTFR-2023-ALE-011/

[83]
CERT-FR
Multiples vulnérabilités dans Cisco IOS XE.
23 October 2023.
https://www.cert.ssi.gouv.fr/avis/CERTFR-2023-AVI-0878/

[84]
CERT-FR
Vulnérabilité dans Citrix NetScaler ADC et NetScaler Gateway.
19 July 2023.
https://www.cert.ssi.gouv.fr/alerte/CERTFR-2023-ALE-008/

[85]
CERT-FR
Multiples vulnérabilités dans Citrix NetScaler ADC et NetScaler Gateway.
19 July 2023.
https://www.cert.ssi.gouv.fr/avis/CERTFR-2023-AVI-0568/

[86]
CISA
Threat Actors Exploiting Citrix CVE-2023-3519 to Implant Webshells.
20 July 2023.
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-201a

[87]
CERT-FR
Vulnérabilité dans Atlassian Confluence Data Center et Server.
31 October 2023.
https://www.cert.ssi.gouv.fr/avis/CERTFR-2023-AVI-0899/

[88]
CERT-FR
Bulletin d'actualité CERTFR-2023-ACT-048.
6 November 2023.
https://www.cert.ssi.gouv.fr/actualite/CERTFR-2023-ACT-048/

[89]
CERT-FR
Vulnérabilité dans Microsoft Outlook.
15 March 2023.
https://www.cert.ssi.gouv.fr/alerte/CERTFR-2023-ALE-002/

[90]
CERT-FR
Multiples vulnérabilités dans Microsoft Office.
15 March 2023.
https://www.cert.ssi.gouv.fr/avis/CERTFR-2023-AVI-0231/

[91]
CERT-FR
Vulnérabilité dans les produits Fortinet.
13 June 2023.
https://www.cert.ssi.gouv.fr/alerte/CERTFR-2023-ALE-004/

[92]
CERT-FR
Multiples vulnérabilités dans les produits Fortinet.
13 June 2023.
https://www.cert.ssi.gouv.fr/avis/CERTFR-2023-AVI-0451/

[93]
CERT-FR
Multiples vulnérabilités dans Ivanti Endpoint Manager Mobile.
26 July 2023.
https://www.cert.ssi.gouv.fr/alerte/CERTFR-2023-ALE-009/

[94]
CERT-FR
Vulnérabilité dans Ivanti Endpoint Manager Mobile.
25 July 2023.
https://www.cert.ssi.gouv.fr/avis/CERTFR-2023-AVI-0584/

[95]
CISA
Threat Actors Exploiting Ivanti EPMM Vulnerabilities.
1 August 2023.
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-213a

[96]
MANDIANT
Barracuda ESG Zero-Day Vulnerability (CVE-2023-2868) Exploited Globally by Aggressive and Skilled Actor, Suspected Links to China.
15 June 2023.
https://www.mandiant.com/resources/blog/barracuda-esg-exploited-globally

[97]
MANDIANT
Diving Deep into UNC4841 Operations Following Barracuda ESG Zero-Day Remediation (CVE-2023-2868).
29 August 2023.
https://www.mandiant.com/resources/blog/unc4841-post-barracuda-zero-day-remediation

[98]
LRT
Hackers stream anti-NATO broadcasts in Lithuania after cyber attacks.
10 July 2023.
https://www.lrt.lt/en/news-in-english/19/2031082/hackers-stream-anti-nato-broadcasts-in-lithuania-after-cyber-attacks

[99]
LRT
NATO summit leak linked to cyber attack on Lithuanian government – official.
20 July 2023.
https://www.lrt.lt/en/news-in-english/19/2039842/nato-summit-leak-linked-to-cyber-attack-on-lithuanian-government-official

[100]
CERT-FR
Grands évènements sportifs – Évaluation de la menace 2023. 30 August 2023.
https://www.cert.ssi.gouv.fr/cti/CERTFR-2023-CTI-005/

CYBER THREAT OVERVIEW

RESOURCES

→ **The 'Cyber Crisis Management' collection**

In a context of growing and ever changing cyber threat, improving digital resilience through cyber crisis management training is no longer an opportunity, but a necessity for all organizations. ANSSI's 'Cyber Crisis Management' collection is designed to help organisations prepare for and manage a cyber crisis. This collection is composed of three volumes: Organising a cyber crisis management exercise, Crisis of cyber origin, the keys to operational and strategic management and Anticipating and managing your cyber crisis communication. This collection aims to provide a cross-sectoral expertise on all aspects of cyber crisis management.

CYBER THREAT OVERVIEW 2023

Published by Agence nationale de la sécurité des systèmes d'information (ANSSI)

Art direction, layout and illustrations:
Cercle Studio (*www.cerclestudio.com*)

LEGAL DEPOSIT

February 2024
Published under open license/
Open Licence (Etalab — VXX)

ISSN: 2999-5612

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI
51 boulevard de la Tour-Maubourg
75700 PARIS 07 SP
www.cyber.gouv.fr
www.cert.ssi.gouv.fr
cert-fr@ssi.gouv.fr