RÉPUBLIQUE
FRANÇAISE

Liberté
Égalité
Fraternité

CYBER THREAT OVERVIEW 2025

CERT-FR

2025

CYBER THREAT OVERVIEW

A MESSAGE FROM ANSSI'S DIRECTOR GENERAL

The year 2025 ended on a concerning note when Poland's electrical infrastructure was systematically targeted by a series of coordinated cyberattacks. A first for any a European Union Member State, this kind of high intensity event has now become a common occurrence in Ukraine. Even though the worst has been successfully averted, the intentions behind these attacks were clear: provoke power and heating outages to affect a substantial part of the Polish population. France is preparing for a similar scenario where a massive increase in hybrid attacks relying heavily on cyberattacks would wreak lasting damage on the nation's most critical infrastructure; all the while overlapping with major military engagements outside the French borders.

Following the end of the successfully hosted 2024 Paris Olympic and Paralympic Games, the high threat level accompanying the event's exceptional nature might have been expected to ease in the year 2025. It was never the case, as the threat level faced by the French Cybersecurity Agency (ANSSI) has remained high during the entire year 2025, sparing no one and relying on attackers ever more difficult to monitor. The line dividing State-sponsored and cybercriminal actors is progressively blurring, while increasingly specialised threat actors share their attack tools and methods, exploit weaknesses in poorly-supervised devices, noisily (but not always truthfully) claim responsibility for cyberattacks, and surreptitiously wait for their time, preparing future cyberattacks whose unknown objectives should concern us all. In short, even though imputing a cyberattack to a known intrusion set or attacker has always been a difficult task, nowadays even detecting and analysing the clues left behind and actively concealed by attackers has become an increasingly complex task.

It is precisely this complexity that this year's edition of ANSSI's Cyber Threat Overview offers to untangle and explain, as much as is feasible, while unveiling some of the work accomplished by ANSSI cyberthreat intelligence analysts, producing knowledge essential for the cyberdefence community, helping prevent attacks, orienting cybersecurity audits, supplying both detection systems and incident response teams with actionable knowledge.

This edition does not, however, constitute an exhaustive overview of all of the various cyberthreats targeting France, highlighting some of the challenges faced and contributing to the corpus of work already published by other cybersecurity actors: specialised vendors, cyber incident response centres, InterCERT France, ACYMA - *Action contre la Cybermalveillance* Public Interest Group (GOP ACYMA), cyber campuses, and trusted service providers. Effective coordination between these actors is an essential component in France's 2026-2030 national cybersecurity strategy, whose priorities include strengthening the country's resilience. ANSSI does not – and cannot – act alone when cyberthreats have become systemic and impact the nation's entire social and economic fabric.

Establishing a yearly threat review must however not be seen as a daunting task, as a better understanding and anticipation of current cyberthreats help us develop more effective tools to counteract their impact. Implementation of recent French and European legislations, such as the NIS2 Directive and the Cyber Resilience Act Regulation, are essential in this context, creating and enforcing a common security framework and helping increase the nation's security as a whole.

France has the means to counteract, discourage and at the very least hinder attackers' efforts.

Vincent Strubel
Director General of ANSSI

INTRODUCTION

The Cyber Threat Overview is an annual document established by the French National Cybersecurity Agency (ANSSI) presenting the most prevalent cyberthreats observed by ANSSI. It does not pretend to be exhaustive but rather to offer a perspective shaped by the most serious incidents treated by or reported to ANSSI.

Marked by a strengthening legal framework, particularly with the national transposition of the NIS 2 Directive[1], this year's edition sets out to raise awareness as well as to add to the considerations of those interested in the current cybersecurity challenges.

In 2025, the borders between state and cybercriminal actors have continued to be blurred. The technological and organisational confusion already addressed in the previous edition of the Threat Overview is now well-established as state and cybercriminal actors increasingly share capabilities and common practices, some of which used to specifically characterise an actor.

Exploiting legitimate applications and services for malicious purposes used to be typically favoured by reputedly state-backed actors and is now on the rise again amongst cybercriminal ones. This evolution may muddy the waters to some degree, while some attackers strive to evade detection by hiding their activity within legitimate traffic.

1
Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive)

This tendency, in addition to the division of labour between different actors specialised in distinct phases of the attack, complicates the imputation process. This context creates a smokescreen through which ANSSI must operate, however the recent data leaks affecting reputedly state-sponsored intrusion sets as well as offensive security companies and cybercriminal groups have provided a helpful insight into their functioning.

In a context of mounting international tensions, ANSSI has also observed continuous efforts by reputedly state actors striving to collect strategic intelligence from the diplomatic networks they compromised. Critical infrastructures remain a target of choice for such attackers, much like the telecommunications and energy sectors. Targeting this type of infrastructure allows them to obtain valuable information to be reused in future attack campaigns.

As already noted in previous editions of the Cyber Threat Overview, ANSSI has again observed malicious activities affecting a wide array of French organisations associated with intrusion sets widely reported to show links with Russian and Chinese State interests.

On the cybercriminal side, ANSSI has noted a slight decline in the number of ransomware attacks compared to 2024, while data exfiltration-related incidents have significatively increased in 2025. Data exfiltration can occur following the compromise of the networks of a third-party provider, which may in itself result from an exfiltration and disclosure of credentials on cybercriminal forums.

More generally, as a result of the growing use of cloud services by a large variety of organisations, ANSSI has observed an increase in cases of compromise impacting these environments, which can lead to the encryption of resources and result in the temporary unavailability of services employed by both professional clients and the broader French public. In at least one of these cases, the attacker exploited a vulnerability affecting an edge security device.

When they were not affected by technical weaknesses inherent to their design, edge devices were affected by various vulnerabilities, as already noted in the previous years. The recurrent compromise of these devices heavily mobilised incident response teams, highlighting the multiple challenges associated with vulnerability treatment.

Lastly, the targeting of mobile environments has been addressed in several publications – including some produced by ANSSI for awareness-raising purposes. These attacks, conducted against both personal and professional-use devices, are indicative of sophisticated research capabilities and of a will to impact a wider range of users. Private companies developing these specialised offensive capabilities are likely to supply them to numerous customers, increasing the risk of their proliferation and thereby elevating the global threat level. ←

STATISTICAL ELEMENTS

Comparison of the number of incidents and reports in 2024 and 2025

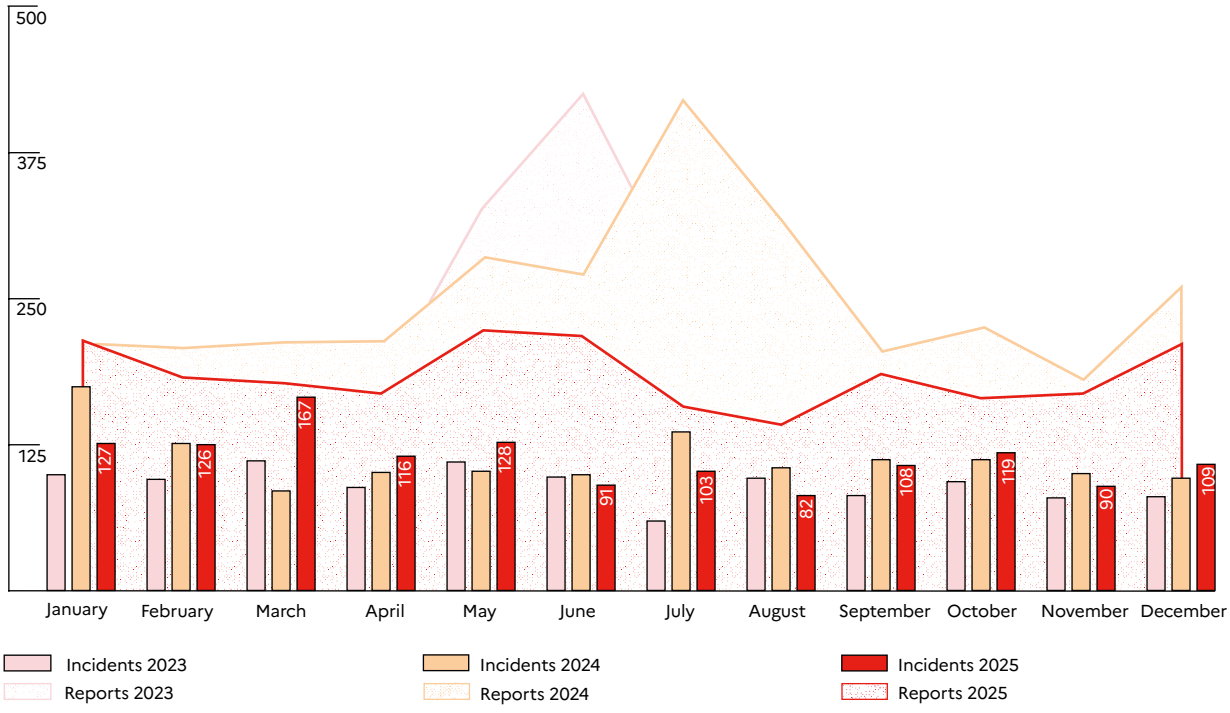
In 2025, ANSSI treated – with a varying degree of engagement – 3,586 security events[2], representing an 18% decrease compared to 2024. This decrease may be attributed the hosting of the Olympic and Paralympic Games in Paris in 2024, as suggested by the upsurge in reports between May and August of the same year.

Of all the 2025 security events, 1,366 incidents[3] were reported to ANSSI. This number remains relatively unchanged compared to 2024 (1,361), following the increase observed between 2022 (831) and 2023 (1,112).

Breakdown of incidents treated in 2025

In 2025, four industries experienced 76% of the 1,366 incidents reported to ANSSI: education and research (34%), ministries and local government (24%), healthcare (10%), and telecommunications (9%). The overrepresentation of these four sectors confirms the trend already observed for several years by ANSSI. This trend can be explained by the significant number of organisations – including public entities – operating in these sectors. These figures correspond to ANSSI's knowledge, consolidated by its constituents' reports, and are not necessarily representative of all of the security events impacting France's various industries.

Progression of the number of reports and incidents



2
Events reported to ANSSI for which incident response teams were mobilised.

3
An incident is a security event for which ANSSI is able to confirm a malicious actor's successful attack on the victim's information system.

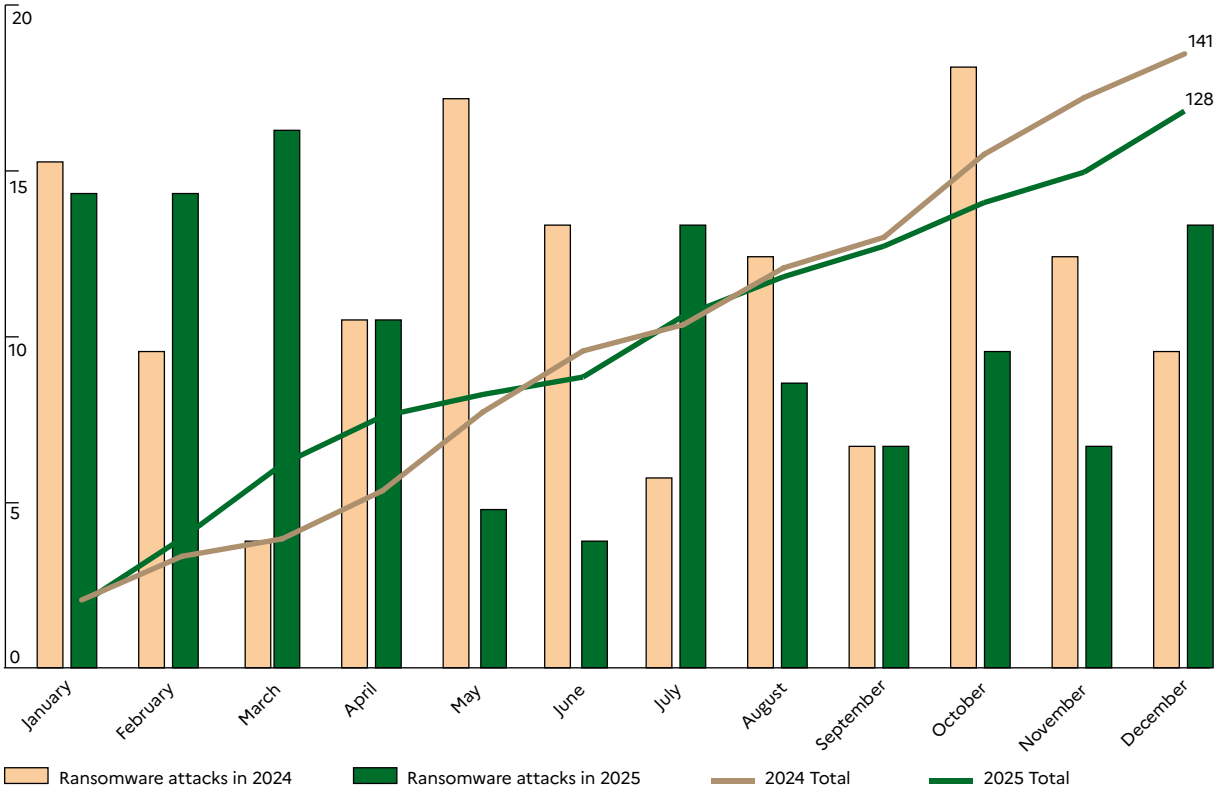
1

ATTACK OBJECTIVES: EXTORTION, ESPIONAGE, AND DESTABILISATION

A
EXTORTION

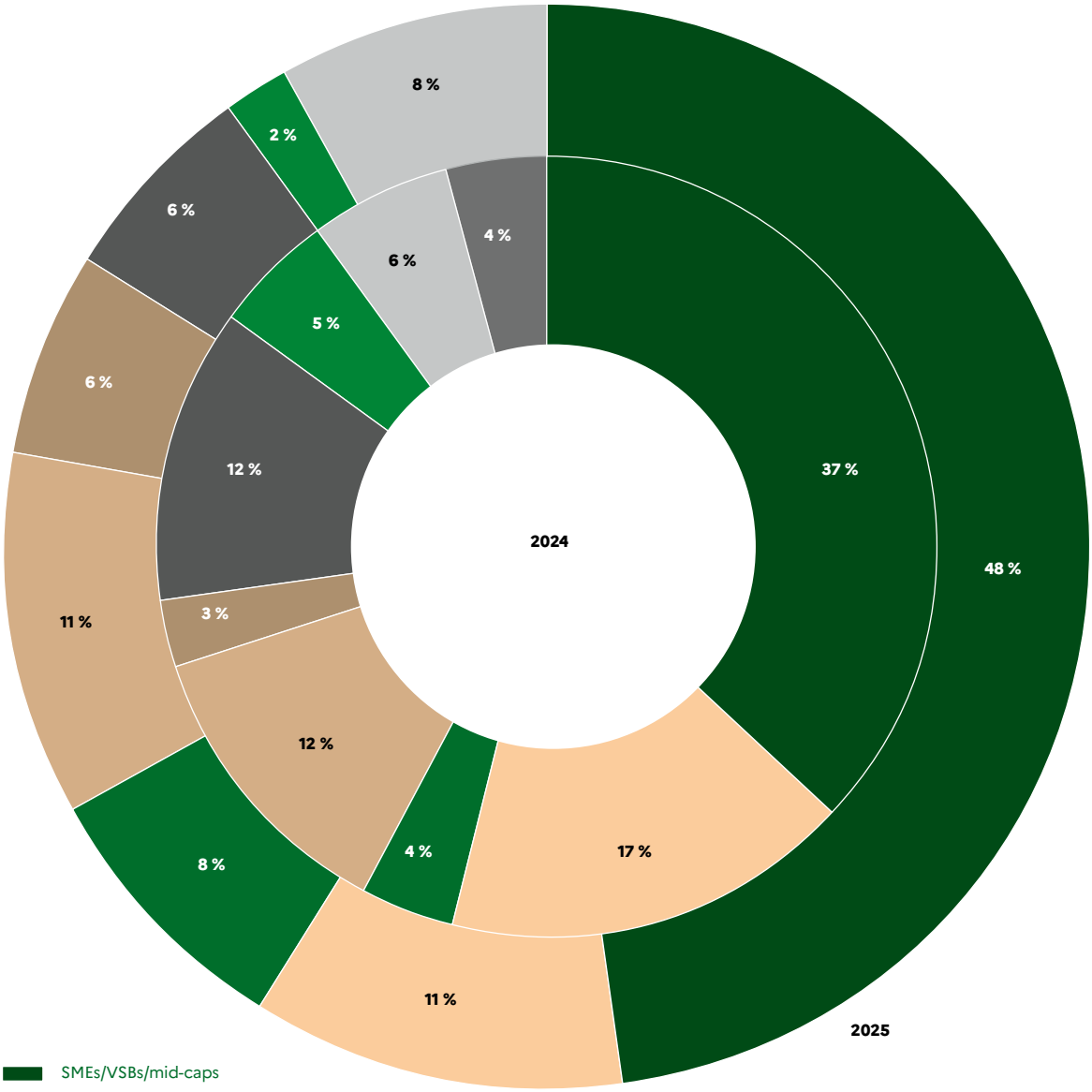
Different types of attackers may carry out financially-motivated attacks. Cybercriminals continue to conduct ransomware attacks relying on double and even triple extortion[4] methods against small and medium enterprises, local governments, and healthcare and educational institutions. Some cybercriminal groups and actors however also favour extortion relying on data exfiltration without encryption. State-sponsored attackers usually known to carry out attacks aimed at espionage have also been involved in activities intended to extort funds from their victims.

Yearly comparison of the number of incidents and reports



4
Double extortion consists in exerting pressure on the victim by exfiltrating and encrypting the data found on their information system, then threatening to divulge it. This dual approach may be complemented by other pressure tactics, such as distributed denial-of-service attacks (DDoS), or by targeting the victim's partners and clients in a so-called "triple extortion" attempt.

Breakdown of ransomware victims



1/BY CYBERCRIMINAL ACTORS

Security vendors and ANSSI's partners have noted a rise in the practice of extortion without the deployment of ransomware across the cybercriminal ecosystem. However, this trend remains limited amongst the incidents treated by ANSSI in 2025.

Ransomware[5]

In 2025, 128 cases of compromise resulting from ransomware attacks were reported to ANSSI – a little less than the previous year. Ransomware attacks nonetheless remain a significant threat, making up a significant part of the cybercriminal operations observed by ANSSI.

While SMEs/VSBs/mid-caps remain the primary victims of ransomware attacks, the proportion of incidents of this type impacting healthcare institutions (8%) has been on the rise again since 2024. Several hospitals have experienced disruptions in the reception and treatment of patients. Small healthcare structures such as nursing homes and clinics have also been affected by this type of incident. The share of local authorities (11%) targeted by such attacks has however slightly decreased.

Educational establishments – including primary and secondary schools – were particularly impacted in 2025. These incidents had significant consequences, notably resulting in difficulties when accessing internal resources and sometimes disrupting operations over the course of several weeks.

Cybercriminal actors deploy ransomware to indiscriminately target all sectors and geographical areas. These opportunistic attacks can have major consequences and lead, amongst other things, to severe operational disruptions on the victim's services and production chains.

In October of 2025, an attack against Collins Aerospace, whose responsibility was claimed by the cybercriminal group Everest, thus disrupted the proper functioning of a number of European airports – resulting in significant delays and the cancellation of flights over several days [01].

The most common types of ransomware observed in 2025 were Qilin (21%), Akira (9%), and Lockbit 3.0/Lockbit Black (5%). Over a dozen other codes were also observed for the first time in the context of at least one incident. Some older ransomware-as-a-service[6] (RaaS) groups – such as Akira, Inc Ransom, and Qilin – also managed to foster their affiliates' loyalty and thus maintain high levels of activity. Qilin was in fact the most broadly used RaaS code in 2025, with over 700 claimed victims – including 185 in the month of October alone [02].

5
Ransomware is a type of malware used to extort money by preventing victims from accessing their files, usually through encryption, and offering up the means to decrypt or recover the data in exchange for the payment of a ransom.

6
Refers to the economic model under which a service and resources are provided by a group or an individual dubbed "operator" to attackers known as "affiliates", to be used in their attacks in exchange for a percentage of the ransoms obtained.

→ Launched in May of 2024, the joint action by international law enforcement agencies and judicial authorities named "Operation ENDGAME" has dismantled various infrastructure associated with cybercriminal malware. Two phases of the Operation took place 6 months apart in 2025. The most recent one took place in November of 2025 and led to the dismantlement of infrastructure associated with the malware Rhadamantys. The first one had targeted other malware in May of 2025, including Lumma Stealer [03]. Operation ENDGAME involves German, American, Australian, British, Danish, French (coordinated by the judicial police's cybercrime office - OFAC), and Dutch law enforcement agencies and judicial authorities. In this context, and in collaboration with OFAC, ANSSI has assisted in identifying and notifying victims as well as disseminating security recommendations.

This operation highlights the importance of international cooperation when addressing malicious infrastructure scattered across national border. Operation ENDGAME furthermore demonstrated, at the national level, that a collaboration with complementary resource from law enforcement agencies and the judicial ecosystem allowed for a successful disruption of cybercriminal activity, at least for a time. A broader collaboration, particularly with the CERT[7] ecosystems, could further enhance the effectiveness of this type of operation, notably in relation to victim support. ←

Cybersecurity incident containment

A hasty implementation of containment measures can have significant consequences for some entities. In 2025, for example, ANSSI handled a case in which the large-scale compromise of an entity had been detected prior to the encryption of its information system. The hasty decisions taken by the entity – which included unplugging its data centre – halted its operations and further led to a long-term disruption of its activities. These containment measures may have prevented an aggravation of the incident, but need to be closely managed in order to avoid edge effects:

- One of the first adverse effects of any remedial action is that a return to normal is not always guaranteed when restarting complex systems. Indeed, the sudden shutdown of electronic devices and applications can affect how they reboot and further function. The effects on business continuity must also be taken into account as some systems have high availability requirements and cannot be easily shutdown;
- Interactions with compromised systems and their shutdown may alter or even erase evidence, thus compromising the understanding of the incident. Prematurely neutralising a known access into the compromised network may actually limit the victim's visibility of the attacker's actions and hinder a future identification of the access paths used by the latter;
- Lastly, any action carried out on a compromised system can be observed and interpreted by the attacker. In the event of an incident, a common reaction is shutting down and isolating compromised systems and revoking credentials. When facing an imminent destructive threat, priority should be given to effectively hinder the attacker's actions. These immediate actions can however provoke both expected and edge effects. Each measure must then be assessed by the crisis management team prior to their implementation. Preparedness in incident-related decision-making processes is thus fundamental to guaranty the victim's capacity to handle cybersecurity incidents. Business continuity plan (BCP) and business recovery plan (BRP) are essential tools for an effective incident response effort [04].

7
CERT: A Computer Emergency Response Team (CERT) or Computer Security Incident Response Team (CSIRT) is a cyberattack alert and response centre.

Data exfiltration

Some cybercriminal actors exfiltrate data without ransomware and monetise the product of their attacks by reselling the stolen data to other, downstream actors who reuse it to support further attacks – as with the already established Initial Access Brokers ecosystem, or when directly extorting future victims. Some data exfiltration attacks are also carried out by hacktivists as part of broader destabilisation operations.

In 2025, 196 incidents involving data exfiltration, with or without ransomware, were reported to ANSSI. In comparison, 130 incidents of this type were treated by ANSSI in 2024. These malicious operations are often publicly claimed on cybercriminal forums or social media platforms such as Telegram, often including already public or previously leaked data. As such, ANSSI was only able to confirm the authenticity of 80 of these data exfiltration claims.

Some cybercriminal actors, such as the cybercriminal group Cl0p, exfiltrate data without deploying ransomware. Active since 2019, Cl0p regularly exploits vulnerabilities found in secure file transfer solutions. In August of 2025, for example, the cybercriminal group exploited the zero-day vulnerability CVE-2025-6182 impacting the Oracle E-Business Suite solution to exfiltrate data belonging to hundreds of companies from across the globe, including France [05]. ANSSI has observed a trend for several years where attackers threaten to publish their victims' exfiltrated data to force the latter into paying ransoms. Increasingly common, this threat nevertheless remains a limited occurrence for now.

Other malicious actors such as Initial Access Brokers (IAB) monetise their attacks by reselling the exfiltrated data to other actors who reuse it to support future attacks. IABs and traffic distribution systems (TDS) are essential upstream actors of the infection chain who act as intermediaries within the cybercriminal ecosystem and particularly the ransomware ecosystem.

ANSSI noted at the same time the regular use of infostealer malware[8] in attacks where data was exfiltrated. In February of 2025, several companies from the agri-food sector detected the presence of EpoBrowser infostealer on several company endpoints, infected following the download and deployment of a malicious software posing as Chromium browser. Once installed, the software redirected searches, displayed malicious advertisements, and collected the victim's credentials. Handling this type of attack can be delicate for victim organisations for a lack of control over the infection vector, especially where professional and personal uses are not clearly separated.

8
An infostealer is a type of malware designed to collect information on the victim's workstation, including any login credentials saved on Web browsers, cryptoasset wallet addresses, session cookies, etc.

Data leaks

Elements that are not individually considered to be sensitive can become much more critical when they are aggregated together. It is however important to differentiate between personal user data leaks and business data leaks, whose level of importance may vary from victim to victim. Whatever their nature, these data exfiltration cases and their subsequent mediatisation pose a significant reputational risk, as they may lead to a loss of trust amongst users and even threaten the entity's economic survival.

Moreover, handling data exfiltration claims requires an active participation of the victims – whether or not the compromise has been confirmed, and whatever the level of sophistication of their attackers' methods. Any alleged data exfiltration must be assessed in order to identify its source and subsequently assess the impact of the exfiltration.

The data published by attackers may also have been extracted from older leaks, or from multiple different sources. Once exfiltration has been confirmed, the victims must, in addition to incident response measures, inform any potentially impacted entities and comply with their regulatory obligations. This includes reporting the incident to the CNIL. Media coverage of these claims – both by the press and by social media influencers – may generate additional pressure on the victims.

ANSSI assists its constituents in the management of such incidents, simultaneously working towards their prevention. Towards that end, recommendations have been published on the CERT-FR's website [06].

2/BY STATE ACTORS

For several years now, ANSSI has observed attacks by state actors seeking financial gain – such, for instance, as the reputedly North Korean intrusion sets which typically target cryptoassets. In 2025, reputedly State-sponsored intrusion sets were observed on multiple occasions deploying ransomware including ransomware usually distributed following a RaaS model. For example, the intrusion set known as Moonstone Sleet, reportedly linked to North Korea, was used to deploy Qilin RaaS as part of a limited number of attacks conducted in 2025 [07]. While intrusion sets associated with North Korea are known to regularly deploy ransomware code – such as Maui, between May of 2021 and July of 2022 [08] – the use of RaaS-distributed code usually employed by cybercriminals is a recent development.

The use of ransomware codes for extortion purposes by reputedly Chinese intrusion sets also appears to be a recent development, observed in open source by ANSSI on several occasions in 2025. These profit-driven attacks are however not new: in 2012, operators of the reputedly Chinese intrusion set APT41 were already targeting the video game industry to this end [09].

From the second half of 2024, a campaign of attacks combining espionage and the deployment of NailaoLocker ransomware was documented in open source [10][11][12]. The intrusion set associated with this campaign by security vendors had been on ANSSI's radar since 2016 for strategic intelligence-gathering operations which notably involved attacks on supply chains [13]. However, the use of ransomware codes represented a significant change in its known techniques, tactics, and procedures (TTP).

Similarly, the RA World ransomware was reportedly observed in compromise chains alongside other tools which are typically associated with reputedly Chinese intrusion sets such as PlugX. Since July of 2024, this same malware has been used in both espionage and extortion operations against victims located across Asia. During these attacks, a ransom request was issued and a negotiation was conducted between the victim and attacker [14]. ←


DONNÉES
DONNÉES

B
TARGETING FOR INTELLIGENCE-GATHERING PURPOSES BY REPUTEDLY RUSSIAN AND CHINESE ATTACKERS

→ Cyberattacks aimed at espionage are most often conducted against entities associated with the governmental sphere or providing essential services, or against individuals considered to be targets of strategic interest for adversary states. In 2025, this type of attack continued to mobilise ANSSI's operational teams.

1/TARGETING AIMED AT STRATEGIC ESPIONAGE

Espionage operations by intrusion sets reputedly linked to Russian or Chinese intelligence services are regularly documented by various sources, not only against a number of targets from the governmental spheres, but also against members of non-governmental organisations (NGOs), media outlets and journalists, entities operating in the field of cybersecurity, and the defence technological and industrial base (DTIB).

In March of 2025, members of the French NGO *Reporters Sans Frontière* (RSF) were reportedly targeted by a phishing campaign. The investigations conducted by the NGO and the security vendor Sekoia made it possible to trace this campaign back to the reputedly Russian intrusion set Callisto[9]. This intrusion set has been used to target entities involved in the governmental, academic, and defence sectors, think tanks, journalists, as well as non-governmental organisations in Europe, North America, and the Caucasus [15][16][17].

In a publication from May of 2025, two Dutch government agencies (AIVD and MIVD) [18] identified a new intrusion set, dubbed Laundry Bear, believed to be aligned with Russian state interests. This intrusion set had been used since 2024 during cyberattacks aimed at espionage, against governmental, non-governmental and military entities, DTIB and aerospace companies, social, cultural and educational organisations, the media and, to a lesser extent, critical infrastructure and digital service providers in EU and NATO member states.

In connection with this publication, between 2023 and 2024, ANSSI handled incidents impacting French entities operating in the media and governmental sphere which – according to the investigations led by ANSSI – might have been linked to the Laundry Bear intrusion set. These incidents involved password spraying attacks against email accounts authentication panels. The infrastructure associated with these attacks notably relied on commercial proxies, VPN services and TOR network. In an effort to limit the risks of detection, operators of the intrusion set also exfiltrated email accounts during working days and working hours.

9
Active since at least 2015, the Callisto intrusion set has been attributed to the Russian Federal Security Service (FSB) by different sources.

In 2024 and 2025, several security vendors and government agencies also observed the targeting of critical infrastructure by intrusion sets reputedly linked to China. On the 28th of May 2025, the Czech Ministry of Foreign Affairs attributed a cyberattack against one of the country's critical infrastructures to operators of the reputedly Chinese intrusion set APT31, publicly associated [19] to a contractor for the Ministry of State Security [20]. The security vendor Talos also observed the compromise, for espionage purposes, of critical Taiwanese infrastructure by operators of the UAT-5918 intrusion set, which had been active since at least 2023. This attack involved the exploitation of vulnerabilities present on exposed web services, notably relying on open-source tools [21].

The compromise, between March and December of 2024, of the US army's federal network by operators of the reputedly Chinese intrusion set Salt Typhoon was a continuation of the actions led against the telecommunications sector in 2024. Attackers may have obtained personal information, administrator access credentials, and network architecture diagrams which could be used in subsequent campaigns. In addition to the telecommunications sector, a dozen other sectors were reportedly targeted by Salt Typhoon in 2024: energy, communications, transportation, and water treatment. At least one exfiltrated configuration file was subsequently used to support an attack against another US government agency [22]. ANSSI has also noted the expansion of the victimology associated with the Salt Typhoon intrusion set, and further observed the use of a compromised device in the conduct of a rebound attack. Such methods complexify the analysis of the attack and the associated objectives. ANSSI is unable to determine whether Salt Typhoon is still strategically used to target the telecommunications sector, or to conduct opportunistic attacks on devices broadly used by operators of electronic communications.

2/THE TARGETING OF DIPLOMATIC ENTITIES

ANSSI has noted continuous attempts by state actors to compromise diplomatic networks with the intention of gathering strategic intelligence amid escalating international tensions. In 2025, ANSSI assisted a French diplomacy-oriented entity whose information system had been compromised. The state-sponsored attacker had gained a foothold on the information system through the exploitation of vulnerabilities on edge devices and achieving privilege escalation for espionage purposes.

A report published in July of 2025 by the security vendor Microsoft revealed a Turla[10] espionage campaign targeting Moscow-based embassies since at least 2024. As part of this cam-paign, an Adversary-in-the-middle[11] technique was used to deploy a compromise chain cul-minating with the dissemination of the ApolloShadow malware. This malware could enable privilege escalation and be used as a persistence mechanism, and potentially

10
Active since at least 2004, the Turla intrusion set has been attributed to the 16th Centre of the Russian Federal Security Service (FSB) by several different sources. This intrusion set is used to target governmental sectors, including the diplomatic and defence sectors in Europe, most particularly in Ukraine, and across North America (sources: US, UK, Estonia, Czechia, Kaspersky, Trend Micro).

11
An *Adversary-in-the-middle* attack is an advanced form of Man-in-the-Middle attack. This type of attack goes beyond the passive interception of communications between two parties, to collect and manipulate data which may then be used to perform additional offensive actions.

allow attack-ers to exfiltrate data from the compromised systems. According to the security vendor, this campaign creates notable risks for diplomatic personnel living in Moscow and using local Internet providers and telecommunications service providers. Indeed, these attacks were reportedly facilitated by the System for Operative Investigative Activities (SORM) – the legal-ly-operated system for interception of telecommunications in Russia controlled by the Rus-sian Federal Security Service (FSB), which may have been used to monitor political opponents [23].

This case bore similarities to another incident treated by ANSSI in 2022, involving an attack against a diplomatic network. Ostensibly conducted for espionage purposes, this attack involved the use of a reputedly Russian intrusion set. As they sought to exfiltrate communications, the attackers developed a thorough understanding of the compromised communication network which may be used to support future attacks.

Intrusion sets reputedly linked to China are regularly used to target diplomatic entities. In March of 2025, the reputedly Chinese intrusion set UNC6384 was reportedly used against diplomatic entities in South-East Asia and Europe. Operators of the intrusion set targeted Hungary, Belgium, Italy, and Serbia with phishing emails whose contents pertained to NATO or the European Commission. Google Threat Intelligence Group (GTIG) believes this intrusion set to be linked to the reputedly Chinese intrusion set Mustang Panda, given the similarities in the victimology of their attacks, the tools and techniques, tactics, and procedures (TTP) used, and the common features observed in the command and control (C2[12]) servers employed. The operators notably distributed StaticPlugin, CanonStager, and PlugX malware [24] [25].

In September of 2025, ANSSI also observed a campaign associated with the RedDelta cluster – linked to the Mustang Panda intrusion set – against several European diplomatic entities, including France. RedDelta was hitherto notoriously used to target diplomatic entities in central and eastern Europe, as well as across Asia. ←

12
C2 (or Command & Control) refers to the server and software infrastructure used by a given attacker to remotely control compromised services.

C
DESTABILISATION: SABOTAGE OPERATIONS AND DENIAL OF SERVICE ATTACKS

→ While espionage may allow attackers to latently and durably pre-position themselves, it can also be a preliminary step towards future sabotage operations.

1/THE CONTINUATION OF RUSSIAN SABOTAGE OPERATIONS IN UKRAINE.

ANSSI has been monitoring cyberattacks suspected to be linked or are formally attributed to Russia with the intention of anticipating any threats of destabilisation which might target France, not only for its support of Ukraine but also in the context of major events taking place in 2026 and 2027 (elections, G7 presidency, etc.).

In Ukraine, these attacks were still carried out in 2025 for the purpose of sabotage and destruction, as a continuation of a strategy adopted at the beginning of Russia's war against Ukraine in 2022. These attacks notably involved the use of wiper codes against critical infrastructures. Security vendors have traced some of these wipers back to Russian attackers in possession of advanced capabilities, and identified similarities with other wipers used during the large-scale invasion of Ukraine in 2022 and associated with the Sandworm intrusion set (reputedly linked to the Russian military intelligence agency).[13]

The continuation, in Ukraine, of cyberattacks aimed at sabotage is indicative of real persistent efforts by offensive actors reputedly linked to strategic Russian interests, to develop sabotage capabilities which might also be used outside of Ukraine. The security vendor Microsoft indeed documented a campaign dubbed BadPilot, associated with a subgroup of the Sandworm intrusion set and active since at least 2021 [26]. This campaign involved the targeting of entities across Ukraine, Europe, the United States, Central Asia, and the Middle East, operating in critical sectors (energy, agriculture, railway, etc.). Attackers would conduct internet scans in search of vulnerable edge devices, to gain initial access, implement means of persistence, and facilitate their lateralisation across the victim's network. In at least three cases, the initial access gained enabled the conduct of destructive attacks later attributed to the reputedly Russian intrusion set Sandworm. In late 2025, Poland was also targeted by coordinated attacks aimed at destabilising its energy infrastructure, which it attributed to actors linked to Russia [27].

2/DENIAL-OF-SERVICE ATTACKS AND SABOTAGE OF SMALL INDUSTRIAL FACILITIES BY HACKTIVIST GROUPS

Hacktivists no longer limit themselves to the simple conduct of distributed denial-of-service (DDoS) attacks, to website defacements, or to data exfiltration. In 2025, ANSSI noted a continuation of the sabotage operations already reported in last year's report against small industrial facilities – such as small-scale renewable energy facilities – exposing poorly secured control interfaces.

Distributed denial of service attacks (DDoS)

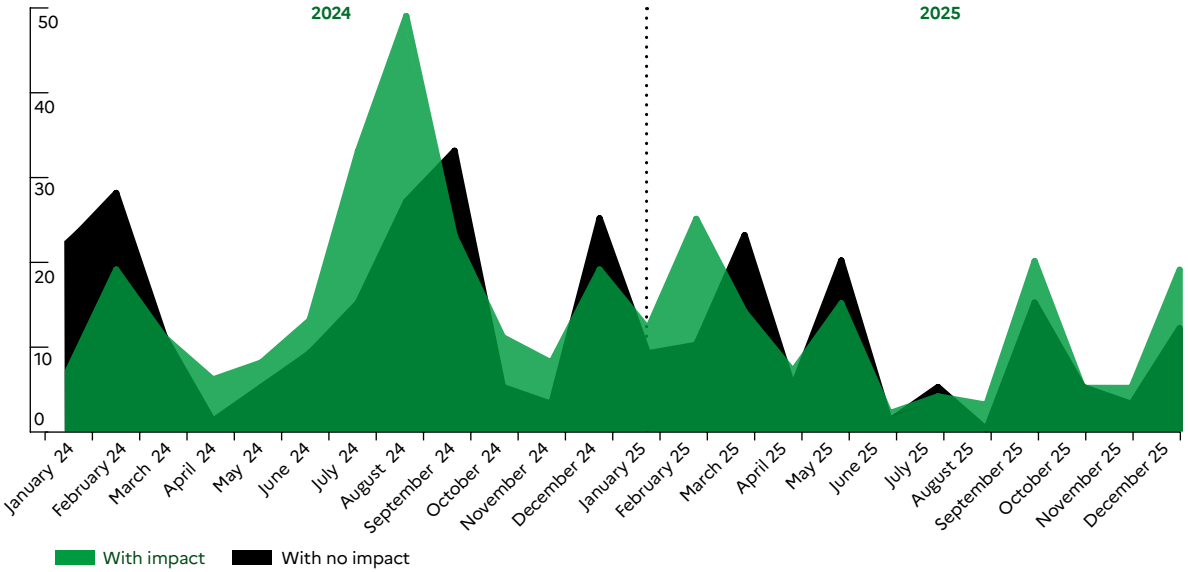
In 2025, ANSSI found that DDoS attacks aimed at destabilisation were the most common type of attack. Despite the notable decline observed in comparison to 2024 – a year which had been marked by a dense geopolitical context and, in France, by a number of large-scale events – several DDoS attacks were conducted in 2025, benefiting from a relentless stream of news as well as a persistent background noise ensuring from malicious actors.

While these attacks are traditionally led by hacktivists who may sometimes be aligned with strategic state interests, they appear to also be increasingly favoured by cybercriminal actors.

Less technically sophisticated, compared to the efforts required to develop malware or to achieve lat-

13
Sandworm, also known as APT44, is an intrusion set reputedly linked to the Russian military intelligence agency, GRU. It has been associated with espionage and sabotage operations against several entities from critical sectors across the world, including Ukraine and the countries which have been supporting it throughout of the war of aggression started by Russia in 2022.

Progression of denial-of-service attacks reported to ANSSI in 2024 and 2025, and their impact



eralisation on a compromised system, DDoS attacks reported to ANSSI were primarily intended to undermine the reputation of victims via the mediatisation of incidents which predominantly impacted the availability of their services. In 2025, however, targeted entities faced increasingly large-scale attacks, over short time frames, which hindered their qualification and the limitation of their effects. In spite of their sheer scale, these attacks did not lead to in-depth compromise. In order to more effectively counter them, ANSSI provides emergency guidelines on the CERT-FR's website to assist entities for the assessment and containment of this type of attack [28] [29].

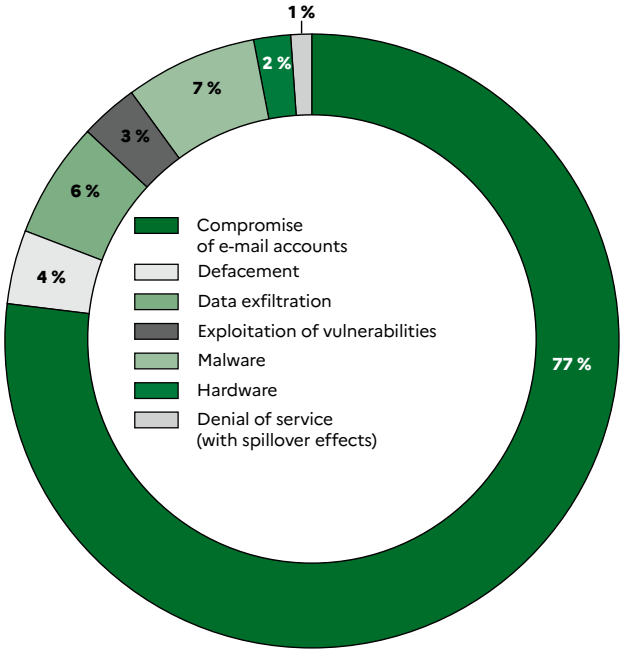
Sabotage of small industrial facilities

Poorly-secured industrial control systems exposed to the internet also also offer easy targets for hacktivists.

Since 2024, ANSSI has been receiving numerous reports regarding the targeting, by hacktivist groups, of entities operating in the sector of renewable energy production. Attackers have targeted industrial systems exposing administration interface on the Internet without authentication or using default credentials. An exposed administration interface may allow attackers to take control of the connected valves and turbines.

In 2025, pro-Russian hacktivist groups claimed more attacks on systems used by the water sector in France and across Europe, conducted for destabilisation purposes. However, the attacks handled by ANSSI over this past year did not result in any significant physical impact. In only one of these cases, malicious actions on the valves led to an increase in the flow of water –which was actually hampered by the facility's limited water supply. While these attacks are not usually

Types of incidents impacting Research and Education



very technically advanced, their heavy mediatisation by the attackers often amplify their effects.

Indeed, pro-Russian hacktivist groups such as Z-Pentest Alliance have claimed responsibility for their attacks *via* Telegram, maximising their media coverage by publishing various videos in which they exhibit their actions on industrial system administration interfaces and regularly exaggerate their impact on victim entities.

ANSSI recently published security guidelines specifically addressed to the water and energy sector actors [30].

The compromise of similar devices was also documented across Europe: in August of 2025, the Norwegian domestic intelligence agency (Politiets Sikkerhetstjeneste) formally attributed to Russian attackers a cyberattack during which a dam on the eastern side of the country was remotely hijacked in April of 2025 [31]. ←

Targeting of the Research and Education sectors

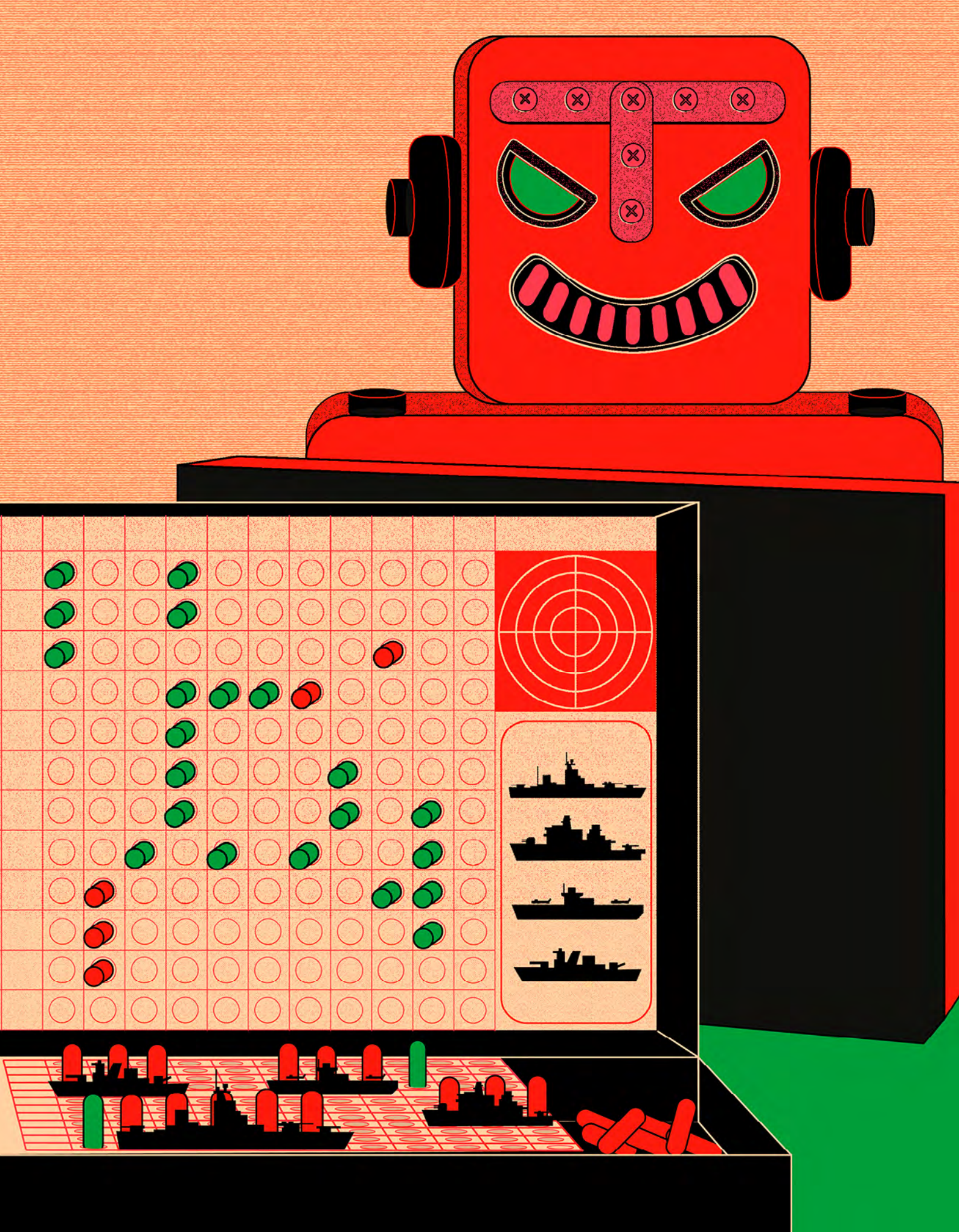
In 2025, education and research were the sectors most impacted by the incidents treated by ANSSI, representing 34% of cases alone. These figures should be put into perspective by taking into account the significant number of public entities operating in these sectors, which are typically more susceptible to report security incidents to ANSSI, even the less critical ones.

A significant portion of these attacks has been conducted opportunistically by cybercriminal actors. Higher education establishments regularly have to handle staff and student e-mail accounts compromise used by attackers to carry out phishing campaigns. Several entities from the education sector also suffered website compromise resulting in a visible modification of their content (defacement). These attacks relied on preliminary exploitation of vulnerabilities and administrator account compromise. Ransomware threat is also a prevalent threat for these sectors. This type of incidents can have significant and visible impacts on business continuity. In February of 2025, a higher educational establishment had for instance to remotely deliver lectures when their network was forced offline as a consequence of such an attack.

In 2025, ANSSI also handled several attacks launched against secondary educational establishments by attackers exploiting their target's low security levels to successfully compromise them, despite their limited technical skills.

Education and higher education organisations fostering more sensitive activities have also been targeted. For example, ANSSI learned of the compromise of resources of interest belonging to a French research institute. While the intentions behind these attacks are difficult to ascertain, this targeting is indicative of attackers' interest in the research sector, for espionage or for prepositioning purposes[14].

14
Pre-positioning refers to the strategy implemented by a cyberattacker to penetrate and remain on critical systems, potentially with the intention of performing further actions at a later date.



2

EVOLUTION AND MONITORING OF ATTACKERS' CAPABILITIES

A
THE EVOLUTION OF ATTACKERS' TOOLS: THE USE OF LEGITIMATE SERVICES AND CAPABILITIES DRAWN FROM ARTIFICIAL INTELLIGENCE

→ The growing use of legitimate components and services by attackers allows them to conceal their activities within legitimate traffic and to reduce the cost of maintaining attack infrastructure. The use of capabilities drawn from artificial intelligence also allows them to significantly increase the level, quantity, diversity, and efficiency of their attacks. ANSSI has observed the use of such practices amongst all types of offensive actors, whether state-sponsored or cybercriminal.

1/THE USE OF LEGITIMATE SERVICES TO COMPROMISE SYSTEMS AND MAINTAIN ATTACK INFRASTRUCTURE

In 2025, ANSSI observed the hijacking of legitimate IT applications and services for malicious purposes. This practice is not a new one for actors reputedly linked to China and Russia, but is on the rise amongst cybercriminal actors.

These applications and services can be remote monitoring and management tools (RMM[15]), online and Cloud storage tools, and even online development or integration support services.

Widely available and easy to deploy, these tools are also difficult to detect when hijacked to support malicious activities, explaining their still growing use by attackers. Legitimate applications and services are used by attackers at all stages of the compromise chain to collect and exfiltrate data, download malware, ensure persistence on a compromised system to prepare for ransomware attacks, or achieve lateralisation. Attackers can reap several benefits from the use of such tools: on the one hand, this technique reduces the cost of maintaining command and control infrastructure; on the other, it complicates identification of a compromise, as it can be difficult for victims and cyberdefensive teams to distinguish between legitimate and malicious communications. Indeed, hijacking legitimate services allows attackers to effectively conceal their own traffic from monitoring solutions while circumventing potential counter-measures. In this context mapping the use of such services is critical to identify the presence of unexpected services or services whose uses do not correspond to what was initially planned.

Within the cybercriminal ecosystem, the increasingly common use of legitimate tools in the

15
Remote monitoring and management: IS remote access and supervision solutions, also known as remote management tools.

early stages of the compromise chain coincides with the declining use of loaders and botnets by initial access brokers (IAB). For example, several IABs – such as TA577, TA571, and TA544 – have reduced or completely stopped using malware in favour of RMM tools or LOLBins techniques[16] [32]. The Scattered Spider intrusion set, for instance, rarely uses malware and almost always gains access to an information system via the compromise of legitimate accesses [33]. ANSSI has observed the use, by cybercriminal attackers, of commercial open-source applications and services available in to target French entities. These tools are employed in a variety of ways: through social engineering techniques deployed to collect credentials, via vishing attacks used to convince the victim to directly download a tool, or after having obtained initial access to the targeted device – relying, for example, on the deployment of a backdoor following a successful phishing e-mail attack.

Operators of reputedly Russian intrusion sets regularly hijack legitimate Web services to conduct cyberattacks. Already observed in 2023 and 2024[17], these attacks continued in 2025 [34] [35] [36]. In September of 2025, the IT security vendor Sekoia for instance documented the use, by operators of the Russian intrusion set APT28, of Koofr, Icedrive, and Filen.io online file storage tools at different stages of their attack [37]. These services were reportedly used to store malicious payloads, loaded through codes used by APT28 operators, such as Covenant and BeardShell [38].

Lastly, operators of the reputedly Iranian intrusion set MuddyWater have also hijacked RMM tools to support their offensive operations, such as AteraAgent [39], SimpleHelp, and ScreenConnect [40].

16
LOLBins, or Living Off the Land Binaries, are the legitimate binaries of an operating system, misused to furtively execute malicious actions.

17
In 2023 and 2024, attacks conducted with the APT28 intrusion set, attributed to the GRU, thus exploited tools such as webhook[.]site, run.mocky[.]io, and Pipedream.

Legitimate applications and services observed by ANSSI during incidents

Listed below are some commercial open-source tools most commonly hijacked by attackers, as observed by ANSSI over the last six months:

NON-EXHAUSTIVE LIST	**LEGITIMATE APPLICATIONS AND SERVICES USED BY REPUTEDLY STATE-BACKED INTRUSION SETS**	**LEGITIMATE APPLICATIONS AND SERVICES USED BY CYBERCRIMINAL ACTORS**
REMOTE MONITORING AND MANAGEMENT TOOLS	• AteraAgent • SimpleHelp • ScreenConnect	• AnyDesk • TeamViewer • VNC (UltraVNC, TightVNC...) • Atera • LogMeIn
LEGITIMATE STORAGE/ SHARING SERVICES	• Google Calendar • Google Drive • Google SpreadSheet • Google Docs • Open Drive • DropBox • Koofr • Icedrive • Filen[.]io	• MEGA
ONLINE DEVELOPMENT AND INTEGRATION SUPPORT SERVICES	• WebHook.site • Mocky.io • Pipedream • Cloudflare Workers • AWS Lambda URL	

The majority of recorded incidents involved the Anydesk software. The download and deployment of this solution was notably observed among attackers linked to the Inc Ransom group, as part of a ransomware attack which impacted a hospital in October of 2025. Open-source RMM solutions have also been used by some cybercriminal groups – like the MeshAgent, employed in cyberattacks involving the Nova ransomware strain this year.

2/ARTIFICIAL INTELLIGENCE: A TECHNOLOGICAL DEVELOPMENT PROVIDING ATTACKERS WITH VARIOUS OPPORTUNITIES

Generative AI and the rapid evolution of its applications may represent a potential accelerator of offensive capabilities associated with current cyberthreats, requiring regular reassessment of the threat landscape. However, adoption of generative AI by attackers depends on their objectives and, above all, on their level of maturity.

Generative AI services may also be targeted by attackers seeking to alter their training data. The proliferation of AI-generated misleading content on the Internet may pollute the training data of chatbot models such as ChatGPT, and may contribute to the large-scale dissemination of false information.

The evolving use of generative AI services – particularly in professional settings – and their integration into workflows are likely to broaden attack surfaces wherever different types of uses are not physically partitioned. The compromise of an AI system may therefore undermine the confidentiality of the data processed and the integrity of the information systems with which it is connected. In terms of software development, the compromise of an AI system specialised in computer code generation could represent a new type of supply chain attack. An overview of the threats associated with generative AI and a guide have been written and published by ANSSI and offer security recommendations for the implementation of generative AI relying on LLMs within public and private entities. The documents are available respectively on the CERT-FR and ANSSI [41] websites. ←

→ In the context of its investigations into private cyberwarfare, ANSSI identified several websites which appeared to have been created using generative AI systems. Though they may seem legitimate, these websites are used to host malicious payloads or for user profiling purposes[18]. The use of AI tools was notable through the abnormal presence, in the middle of paragraphs, of text which was completely unrelated to the rest of the content. ←

18
User profiling consists in collecting the technical data of a webpage user in order to identify targets before compromising their systems.


7

B
THE SUSTAINED EXPLOITATION OF DIVERSE SOCIAL ENGINEERING TECHNIQUES

→ Without the need for high technicality levels, attackers have been able to continue their exploitation of the biases inherent to human nature – taking advantage, for example, of the goodwill of their targets.

1/ADVANCED SOCIAL ENGINEERING TECHNIQUES

In 2025, ANSSI observed the use, by cybercriminal actors, of advanced social engineering techniques such as SIM-Swapping[19], MFA Fatigue[20], identity theft, and vishing[21]. These techniques consist in luring users into performing tasks they consider to be legitimate but which in reality compromise their systems. ANSSI observed several instances of tech support scams inciting employees to download RMM solutions as initial vectors of compromise. Once these tools had been installed, the cybercriminals could circumvent firewall rules or modify registry keys by adding the legitimate programme's launch feature during a clean boot – all to avoid detection by antiviruses and EDRs.

The Scattered Spider intrusion set has also stood out with its mastery of techniques used to deploy ransomware and/or exfiltrate data. The effectiveness of these techniques is largely owed to the attacker's knowledge of internal company processes, but also to the reconnaissance phase during which personal data associated with the targeted employees was collected to prepare the attack. This also stands as a testament to the ability of these attackers to adapt to and circumvent security measures – particularly those pertaining to multi-factor authentication [42][43]. Several French entities, including some from the luxury goods industry, were compromised via Scattered Spider in 2025. In at least one of these cases, attackers reportedly usurped the IT department to obtain access details from a customer relationship management application.

Furthermore, in June of 2025, the security vendor Google Threat Intelligence Group (GTIG) and the academic research group Citizen Lab simultaneously issued publications on the targeting, between April and June of 2025, of Russia experts – including British researcher Keir Giles – as part of phishing campaigns associated with the UNC6293 intrusion set. According to GTIG, UNC6293 may be linked to the reputedly Russian intrusion set Nobelium[22]. Over the course of several weeks, UNC6293 operators used personalised social engineering techniques to incite Keir Giles to create and share an application password linked to his Google account. This password subsequently allowed the attackers to access the victim's accounts [44][45].

In February of 2025, French researchers – some of whom were experts on Russia – received phish-

19
A social engineering technique which consists in transferring a victim's phone number to a SIM card controlled by the attacker. This technique makes it possible to circumvent authentication mechanisms based on text messages or voice calls.

20
In which the attacker bombards their victim with multi-factor authentication (MFA) requests until said victim inadvertently accepts the request.

21
Technique whereby the attacker uses phone calls to encourage their victims to share sensitive information or to perform actions which may lead to their compromise, often by posing as a trusted authority (tech support, bank, etc.).

22
The Nobelium intrusion set is reputedly linked to the Russian foreign intelligence service. According to the security vendor Microsoft, the activities associated with this intrusion set can be traced back to 2018. It has notably been used against government entities, diplomatic bodies, and entities from the industry of technology in North America and Europe (Acteurs émanant d'un État-nation Midnight Blizzard, 2024).

ing messages via the instant messaging applications Signal and WhatsApp. These mes-sages usurped the identities of American and Ukrainian political figures. This targeting may have been part of broader phishing campaigns exploiting mobile environments to collect the pairing codes associated with Microsoft accounts and services. The TTPs implemented during these attacks correspond to those employed by intrusion sets potentially linked to Russia and documented by several security vendors [46][47].

2/IMPLEMENTATION OF THE "CLICKFIX" TECHNIQUE

Since autumn of 2024, cybercriminal actors have been increasingly relying on the "Clickfix" technique – which consists in encouraging victims to execute commands to download and execute malware. According to several vendors, this technique has been on the rise in 2025. Numerous RATs and infostealers, such as Lumma Stealer, Rhadamanthys, XWorm, and AmadeyLoader, were deployed via such means [48][49]. At least one attack campaign relying on this technique has been reported to ANSSI.

In 2025, operators of reputedly state-sponsored intrusion sets have also been known to rely on this technique. In a report published on the 25th of October 2024, for example, the CERT-UA identified a phishing campaign by the Russian intrusion set APT28, targeting Ukrainian government entities. This campaign notably relied on the use of a fake captcha to convince the victim to copy a malicious command to their clipboard, open a command line interface (CLI) and then paste and execute it on the CLI, potentially allowing attackers to compromise the victim's device [50].

More recently, in September of 2025, Callisto[23]operators also employed this technique as part of campaigns targeting members of civil society in Russia and non-governmental organi-sations involved in Ukraine [51][52]. ←

23
Active since at least 2015, the intrusion set known as Callisto has been attributed by different sources to the Russian Federal Security Service (FSB).

C
MONITORING ATTACKER CAPABILITIES

1/TOOLS AND PRACTICES WHICH COMPLEXIFY THE IMPUTATION PROCESS

Over the course of its investigations, ANSSI was faced with various difficulties linked to the use, by intrusion set operators, of anonymisation chains, non-discriminating or shared tools and of false flag techniques, which complexified threat monitoring and the imputation process.

For several years, ANSSI has for instance observed a growing use of offensive security tools developed and publicly shared by well-known companies and individuals in the ecosystem of Chinese offensive security companies, which could be reused by the operators of various intrusion sets. These tools – whose types can vary depending on the kill chain stage in which they are used – are almost exclusively used as part of attack campaigns led by intrusion sets reputedly linked to Chinese strategic interests, and most notably by offensive security companies (such as the company I-SOON). Only a fraction of these tools is more broadly used by other attackers outside of the Chinese offensive security ecosystem. The FRP and aspxspy tools, for instance, were respectively used by operators of reputedly Iranian intrusion sets Charming Kitten and APT39 [53] [54].

Simultaneously, ANSSI has also noted the extensive use of reconnaissance and tunnelling[24] tools, employed not only for the purpose of intrusion but also to administer the anonymisa-tion networks used by the operators of several different reputedly Chinese intrusion sets. Between 2024 and 2025, the use of the vShell (whose Github repository was deleted in 2024), Asset Reconnaissance Lighthouse, fscan, Neo-Regeorg, Rakshasa, and Stowaway tools was documented in open source on a number of occasions. Meanwhile, ANSSI was also ob-serving the use of tools such as Ladon, NPS, and iox [55] [56] [57].

The public availability of these tools indeed complexifies the imputation of cyberattacks to specific intrusion sets, and must be considered in conjunction to the increasingly common occurrence of non-public codes sharing between Chinese offensive actors (PlugX, ShadowPad and KeyPlug) and the deployment of attack infrastructures shared between several intrusion set operators (including reputedly Chinese anonymisation networks).

The use across the infection chain of malicious resources associated with different intrusion sets may also complicate the imputation of cyberattacks. In late 2024 for example, ANSSI observed the use of the reputedly Chinese intrusion set Houken against French government entities operating in the telecommunications sectors, media, finance, and transportation. The attackers exploited several zero-day vulnerabilities affecting Ivanti devices to achieve their initial compromise, subsequently lateralising themselves on the systems with the use of generic tools and leaving many traces in the process. The difference in sophistication observed between the initial exploitation of vulnerabilities and the rest of the attack suggests that Houken is being used by an initial access broker (IAB), and

24
Tunnelling is a method used to transport data on a network *via* protocols which are not supported by the network in question. Tunnels encapsulate network packets – meaning that they wrap packets in other packets.

that other reputedly Chinese intrusion sets are then used for the remainder of the attack. This division of labour between intrusion sets may further complexify the imputation process and the monitoring of malicious actors [58].

In a similar vein, on the 5th and 6th of June 2025, the security vendor ESET observed the de-ployment of the Kazuar v2 malware, associated with the intrusion set Turla, on two devices belonging to non-identified organisations in Ukraine, relying on a malicious code associated with the Gamaredon intrusion set. These observations suggest a collaboration between op-erators of the Turla and Gamaredon intrusion sets[25], both of which are reputedly linked to the Russian Federal Security Service (FSB) but to different centres, which further blurs the boundaries between the different intrusion sets reputedly linked to the FSB [59].

ANSSI has also noted that cybercriminals usurping the identity of other known cybercriminal groups to claim responsibility for cyberattacks –underlining the issue of false flag attacks and the importance, for cybercriminal groups, of mediatising their attacks. In March of 2025, for example, attackers usurped the identity of the Cl0p group by sending out fake e-mails claiming to have exfiltrated the data of their recipients through the exploitation of a vulnerability affecting Cleo [60]. The attack campaign against Salesforces[26] claimed in August of 2025 by a group posing as an alliance between Scattered Spider, Lapsus$, and ShinyHunters also raised issues concerning the imputation process. Indeed, while the operators of these three intrusion sets did evolve within the same community (TheCom), their involvement in this campaign could not be confirmed as the TTPs employed in this case were not sufficiently discriminating [61].

Lastly, connections between cybercriminal actors and the Russian state are regularly highlighted in open-source reporting by public figures. These relations are however not systemat-ic; rather, they appear to be largely born out of temporary opportunities, blackmail, or in-terpersonal relationships. BlackBasta's data leaks, published in February of 2025, shone a light on these complex connections by exposing the personal ties between cybercriminal actors and Russian service employees. Hence, while the complexity of the geopolitical con-text has prompted Russian authorities to tacitly protect cybercriminals from extradition, it is highly likely that the majority of these groups are autonomous and do not generally act fol-lowing orders from the Russian state.

2/A TECHNOLOGICAL AND ORGANISATIONAL FOG WHICH CAN HINDER THE DIFFERENTIATION OF OFFENSIVE CYBERCRIMINAL ACTORS

The monitoring of offensive capabilities may also be further complexified by the volatile nature of some threats, or by their organisation and development. This is, for example, the case with off-the-shelf cybercriminal codes and the groups which operate them.

25
The Gamaredon intrusion set has been publicly attributed by the Security Service of Ukraine (SSU) to the Russian Federal Security Service (FSB). Active since at least 2014, this intrusion set is primarily used to target strategic sectors in Ukraine such as the government, energy, and defence sectors, particularly in the context of espionage operations (*SSU identifies FSB hackers responsible for over 5,000 cyber attacks against Ukraine* (video), 2021).

26
American vendor specialised in Customer Relationship Management (CRM) software. .

Ransomware-as-a-service groups are volatile and made up of particularly heterogeneous affiliates. This type of ransomware has a relatively short life span and is used by a vast number of cybercriminals. In 2023, the average lifespan of a ransomware group was estimated to be 262 days [62]. In addition to the monitoring of these franchises, it is also necessary to identify long-term affiliates relying on technical markers. Most of the time, these groups of affiliates deploy different types of ransomwares simultaneously or over the course of a few years. In 2022, the EvilCorp group was reportedly affiliated to LockBit, a major group in charge of 60 different versions of the ransomware and responsible for extorting over 100 million euros. It is notably being monitored through its malware SocGolish (FakeUpdates). Between July of 2024 and early 2025, it reportedly deployed the ransomware RansomHub [63].

Malware-as-a-service (MaaS) cases also be challenging to monitor, given the complexity of cybercriminal code and the massive scale on which it is deployed by a number of affiliates. Sold as MaaS on Russian-speaking forums since at least August of 2022, Lumma Stealer offers data exfiltrations capabilities (targeting crypto wallets and credentials), code execution on the infected devices, and deployment of additional payloads. ANSSI faced several challenges during its analysis:

- **Massiveness**: Tens of thousands of samples requiring processing, and a significant number of infection chains;
- **Code complexity and update**: code is regularly updated and evolves with each new variant. It presents sophisticated code obfuscation techniques, adapted to the malware and used across the cybercriminal ecosystem, such as control flow flattening[27];
- **Resilience**: the resurgence of the code's activity after the dismantlement of its infrastructure on the 21st of May 2025 highlights the resilience of the actors responsible for developing Lumma Stealer;
- **Instability**: command and control domains are changed several times a week, and a single sample can contain up to a dozen domain names whether or not they are active when the malware is deployed. Moreover, a substantial part of these domain names is managed by – legitimate, but rented by cybercriminals – Content Delivering Network infrastructure. The use of this type of infrastructure, such as Cloudflare, allows for the partial anonymisation of command and control domains by concealing the server's real IP address with the CDN and therefore hindering analysis and detection. These difficulties are felt in the monitoring of numerous threats, including threats associated with private cyberwarfare.

The case of Lumma Stealer therefore illustrates the various issues which mark the study and monitoring of cybercriminal code.

3/DATA LEAKS PROVIDE A BETTER UNDERSTANDING OF OFFENSIVE ACTORS

In 2025, as with the previous year, several data leaks affecting operators of state-backed intrusion sets, cyberwarfare companies, and cybercriminal groups were published in open source – which provided insight into the inner workings of these diverse groups. On the one hand, they shed light – over the short term – on the organisation of these entities, on some of the tools and codes which might have

27
Control flow flattening is a technique used to transform code structure to conceal the logic of its execution.

been used during the attacks (*via* internal documentation, for example), and on their potential or confirmed targets. On the other hand, these leaks can lead to the dissolution, the suspension, and even the reorganisation of the identified attackers' activities. Over the longer term, this could lead to a loss of visibility amongst the entities involved in monitoring their work.

This past year, major ransomware groups faced data leaks and internal dissent which ultimately led to their dissolution. In late March of 2025, the activities of the RansomHub group – responsible for 239 attacks in 2024 [64] – were brought to an end as a result of conflict with other cybercriminal groups [65]. Around the same time, the BlackBasta group, active since 2022 [66], then the LockBit group [67], faced major data leaks. These sources of information are crucial to understanding the innerworkings of these groups, their internal organisation, the connections between different actors, and the codes and attack campaigns. While its authenticity can never be completely ascertained, the information leaked is credible and can correspond with the results of prior investigations.

Furthermore, data leaks exposing Chinese offensive security companies had already been observed during previous years [68], and in that re-gard 2025 was no exception. In May of 2025, for example, two data bases related to opera-tors of Salt Typhoon and the company VenuTech were put up for sale on the English-speaking cybercriminal forum DARKFORUMS. The case was documented in an article pub-lished by the American cybersecurity company SPYCLOUD on the 1st of July 2025 [69].

→ For several years now, data leaks affecting major cybercriminal groups have been multiplying. For the members of powerful groups, these leaks appear to represent an effective means to denounce actions (exitscams, non-payment of ransoms) or to obtain retribution. They have become an integral part of the ecosystem's dynamics and of its main restructuring plans. ←

A large part of the information contained in these documents is corroborated by publicly available sources, which suggests it may be authentic. These internal documents are undeniably useful when it comes to developing a better understanding of the Chinese cyberthreat. They specify the intentions and capabilities of attackers, in view of the targeting of foreign organisations and of the type of information sought by the operators (such as the contents of e-mail servers). They also shed light on the organisation of these offensive actors by identifying government client names, the offensive services they provide, commercial relations between providers, and the prices listed for these services – which makes it possible to estimate their value on the Chinese market. In this way, a discrepancy may be observed between the limited means allotted to this type of offensive service in China, and the significant resources allocated by targeted entities and countries to defence. More recently, in November of 2025, the Chinese company Knownsec[28] suffered a data leak. This leak reportedly included internal doc-umentation on malware, along with lists of potential victims from over twenty different countries, including Japan, Vietnam, India, and South Korea [70].

The attributions made as part of these public data disclosures should however be approached with caution. As a case in point, a data leak allegedly associated with North-Korean operators was, following its presentation during the Las Vegas DEF CON 33, brought into question in several publications by security vendors revisiting the initial attribution hypothesis and reorienting analyses towards potential Chinese operators. ←

28
Known for activities linked to the Chinese intelligence services.

3

ACCESS OPPORTUNITIES AND TARGETING

A
OPPORTUNITIES BORN OUT OF A SPECIFIC CONTEXT

Attackers seek or take advantage of opportunities to carry out their attacks. Some of these opportunities are born out of the global context within which their targets operate (hosting of events, electoral deadlines, conflict, etc.), while others are derived from their administrative environment (legal framework which facilitates the collection of data or vulnerabilities). The security level of targeted entities may also create a favourable context for attacks, in cases where technical weaknesses and bad practices are structural.

1/ATTACK OPPORTUNITIES GENERATED BY INADEQUATE SECURITY STRATEGIES

As part of its missions, ANSSI conducts security audits for government bodies, critical infrastructure operators, essential service providers, and victims of incidents. These audits often demonstrate that inadequate security strategies provide fertile ground for attack opportunities to arise, given the range of techniques, tactics, and procedures employed by attackers. Several observations may be made in this regard, notably on the IT networks of organisations whose infrastructure is made up of dozens, hundreds, or even thousands of workstations.

Firstly, few global audits are conducted, though they can provide a global overview of the information system's security level. Audit perimeters should indeed not be too restricted, lest their relevance be diminished. The following cases were for instance observed:

- The auditing of an application, in which the authentication provider used (such as the Active Directory) was not included;
- The auditing of an application, without the underlying server which exposed a non-updated IPMI[29] interface, itself exposed to the entire IT network.

The audits may furthermore be "redteam" audits, whereby a significant part of the assessment is dedicated to remotely gaining initial access to an information system (IS) connected to the Internet. Relatively common, this approach is intended to simulate an intrusion set's attack on the information system. While IS audits are, generally-speaking, rarely comprehensive, "redteam" assessments tend to be particularly fragmented. Indeed, since their primary aim is to gain access to the system to either obtain the information sought after or demonstrate its permeability, these audits do not involve a comprehensive analysis of all possible attack paths or potential existing vulnerabilities.

ANSSI therefore recommends that extensive audits be conducted, to develop a solid global overview of the environment's security level and to identify as many means of compromise as possible.

29
The Intelligent Platform Management Interface (IPMI) is a set of interface specifications for standalone components of computer servers.

These audits may be supplemented with a redteam approach or with an assessment of the intrusion detection mechanism in place – but they represent, by themselves, an essential building block of realistic and effective security strategies.

The following initial access points may be provided to auditors:

- Access to the company IT network, without privilege, to simulate the compromise of one of the network's physical access points;
- Access to the IT network (possibly through a VPN), alongside a user account, to simulate the compromise of a workstation;
- Access to resources such as a container, a virtual device, or a physical server, to simulate the compromise of an application.

The team in charge of intrusion detection (SOC, Security Operations Centre) should refrain from blocking access gained by the audit team – even when detected-, given that the audit is not intended to assess the SOC's reactivity. However, towards the end of the audit, the different compromise paths identified by the auditors should be presented to the SOC, to allow for:

- The promotion of the detection scenarios implemented which successfully detected the actions performed by the auditors;
- The implementation of new detection scenarios, for the actions which were not detected by the SOC.

Lastly, ANSSI's teams sometimes come across organisations whose security strategies are entirely reliant on their products. Such an approach is not sufficient; while EDRs, multi-factor authentication (MFA) mechanisms, and bastion hosts can indeed elevate an information system's security level, they also possess limitations:

- EDR: attackers often face these tools and are forced to adapt their own in order to avoid detection;
- MFA and bastion hosts: if a user's workstation is compromised, these mechanisms cannot stop the attacker. Indeed, once workstations have been compromised, attackers may inject themselves into user sessions and use the same channels as the legitimate users.

2/CYBER LAWFARE: OPPORTUNITIES MOULDED BY A FAVOURABLE LEGAL CONTEXT

Worldwide, several states have used their legal framework to facilitate or to conduct attacks against French interests, without limiting themselves to this scope. In some cases, the regulatory frameworks in place within these countries may impose the use of specific software on any companies and entities established on their territory. Most notably, ANSSI has, for several years now, been observing cases of imposed software in China [71].

In 2025, following the implementation of new legislation in China, companies operating in the same industry were required to install software allegedly only intended to be used for the registration of companies exporting their goods out of China. The analysis of the source code detected malicious features on this programme: it provided extensive access to the information systems of targeted entities, via enumeration capabilities and the surveillance of USB ports, coupled with autonomous update capabilities.

Similarly, a French pharmaceutical group reported the presence of malware on the information system of one of its subsidiaries located in China. Local authorities threated and exerted pressure on an employee to circumvent the company's cybersecurity policies and accomplish their goals.

While such software may contain malicious features intentionally included by its publisher, it may also be impacted by supply chain attacks intended to compromise the end users. Attackers may indeed target specific software whose usage is circumscribed to a given geographical area, to reach companies in a particular country.

To limit the impact of these threats, ANSSI recommends – wherever it is possible – that the software be installed on an isolated and dedicated workstation. Otherwise, the implementation of measures to mitigate the risks of data leaks and compromise should be considered, such as isolating the software – which should be considered to create an unmanaged risk – to the furthest possible extent. Additionally, it may be useful to monitor the information exchanges in which this software component is involved.

3/OPPORTUNITIES GENERATED BY CURRENT EVENTS

Political and geopolitical events such as elections, visits from government officials, and diplomatic negotiations create opportunities for espionage and influence operations. In 2025, ANSSI continued to observe offensive activity linked to reputedly Russian or Chinese intrusion set, brought on by such political and geopolitical opportunities. The security vendor Recorded Future for instance observed the coinciding launch of mass reconnaissance activities against Panamanian entities, via the reputedly Chinese intrusion set RedNovember[30], during the US Secretary of Defence Pete Hegseth's visit of Panama between the 22nd and the 24th of April 2025.

In Europe, the various elections which took place in 2025 and late 2024 provided numerous opportunities for cyberattacks and influence operations. ANSSI and VIGINUM[31] are particu-larly watchful of campaigns targeting European contexts and of any threats which might impact France. VIGINUM notably documented cases of information manipulation targeting the 2024 Romanian presidential elections, during which informational intrusion sets artifi-cially promoted specific Tiktok content [72]. Documentation declassified by the Romanian Presidency also mentioned cyberattacks against Romanian entities involved in the electoral process which might have been linked to state attackers [73]. The Romanian Presidency fur-thermore reiterated that Romania has been regularly targeted by Russian hybrid attacks.

In November of 2025, during local elections in Denmark, the official websites of multiple political parties and of the Danish parliament were targeted by DDoS attacks claimed by the pro-Russian hacktivist group NoName057 [74] [75].←

30
The intrusion set RedNovember, also known as Storm-2077, has reportedly been employed for espionage purposes and, according to Microsoft, is associated with China (Microsoft shares latest intelligence on North Korean and Chinese threat actors at CYBERWARCON, 2024).

31
Created on the 13th of July 2021 and associated with the General-Secretariat for National Defence and Security (SGDSN), VIGINUM is the technical and operational service implemented by the state to reinforce the country's framework to counter information manipulation. Intended to protect public debate on fundamental national interests, VIGINUM's mission is defensive: to detect and characterise digital foreign interference.


ANSSI

B
OPPORTUNITIES CREATED BY VULNERABILITIES

→ The exploitation of vulnerabilities remains one of the main vectors of compromise used by cyber-attackers, who have notably been targeting edge devices such as firewalls, proxy servers, and anti-spam gateways. It is therefore crucial to understand their lifecycle and the various issues associated with it.

1/ISSUES ASSOCIATED WITH THE LIFECYCLE OF VULNERABILITIES

Vulnerabilities may be identified by vendors, researchers, third-party entities, or attackers. Once discovered – and depending on their discoverer – they may be disclosed in a public, sometimes in a coordinated manner, or become the subject of a first exploit. The lifecycle of a vulnerability begins with its identification and ends when all security patches have been applied. When a vendor is involved in the early stages of this process, the associated risk may be contained. Indeed, vendors can produce and distribute the appropriate security patch for a given vulnerability, allowing users to deploy it as soon as it is received. The threat is however amplified when it is the attacker who takes the lead on researching, developing, exploiting, and distributing a vulnerability's exploit.

The more knowledge one possesses on a given vulnerability, the less skills are required to exploit it. Indeed, the differential analysis of patches and the publication of technical documentation allows less technically-skilled attackers to develop or obtain reliable and interoperable exploits. Exposed and vulnerable devices will always be targeted. Defenders who possess a solid understanding of their own information system and an effective strategy for the systematic application of security patches may anticipate the gradual democratisation of this threat.

The issues at stake are all the more pressing given that vulnerabilities are being published increasingly frequently, with an average increase of 18% per year since 2020. While only 6% of vulnerabilities are exploited (A Visual Exploration of Exploitation in the Wild), this volume poses a daily challenge for network security maintenance. To prevent – or at the very least limit – the consequences of these disclosures, it is therefore increasingly necessary to define risk-based priorities. Two key criteria might be considered: the severity of the vulnerability, evaluated according to its CVSS[32] score, and the criticality of the affected server, measured on the basis of the business stakes.

Servers exposed on the Internet, above all, require enhanced monitoring and greater reactiveness. These servers – edge and security devices most particularly – are ideal targets and have, as such, been the subject of several alerts by the CERT-FR.

Exploitations and exploit publications should also be permanently monitored, drawing on the alerts issued by the CERT-FR. Depending on the sources and perimeters considered, around 8% of exploited vulnerabilities are exploited prior to their publication or to the publication of a patch [76] and, in 2025, approximately 29% were exploited on the day of or before their publication [77]. These vulnerabilities must therefore be dealt with swiftly and efficiently, to limit any potential opportunities for attackers.

It is however important to note that such practices have not yet been completely generalised. Indeed, even when the number of exposed vulnerable assets drastically drops following an alert, a significant portion usually remains durably vulnerable. In late 2025, over 6,200 assets were still being affected by the same main vulnerabilities which had been exploited since 2023 and 2024 in France [78].

32
The Common Vulnerability Scoring System is a standardised system used to assess the criticality of vulnerabilities on the basis of objective and measurable criteria (Vulnerability Metrics, s.d.).

→ In addition to the various vulnerabilities published in 2025 and rapidly exploited thereafter, attackers have also been using older, unpatched vulnerabilities.

In 2025, for example, ANSSI treated an incident which involved the major compromise, via the CVE-2024-55591 vulnerability published several months prior, of a French entity. The exploitation of this vulnerability allowed the attacker to circumvent the authentication mechanism in place on the administration interface of a Fortinet device, and to achieve privilege escalation. Once administrator of the firewall, the attacker restricted the rights of legitimate administrators and prevented the constituent from accessing the device.

This case serves as a reminder of the fact that administration interfaces are prime targets whose exposure on the Internet, still frequently observed, should be proscribed. When this single vulnerability was reported to the affected entities, the CERT-FR found that 3,700 administration interfaces were exposed in France. ←

→ The vulnerabilities affecting an information system can only be effectively managed when the products they affect are themselves effectively managed by their manufacturers. Accordingly, the Cyber Resilience Act (CRA) will, from the 11th of September 2026, require vendors of digital products distributed in Europe to report any actively exploited vulnerabilities or significant incidents impacting the security of their products to national CSIRTs such as ANSSI's CERT-FR. It is already possible to submit reports on the CERT-FR website [ClubSSI – Assistance et déclarations règlementaires].

From the 11th of December 2027, the CRA will impose a number of additional requirements which vendors will need to meet in order to ensure the cybersecurity of the products they supply on the European market:

- Identifying and documenting product components and vulnerabilities;
- Promptly managing and patching any vulnerabilities affecting their products;
- Regularly assessing products containing digital components through effective security tests and reviews;
- From the very publication of a security update, communicating on the patched vulnerabilities;
- Implementing and applying a coordinated vulnerability disclosure policy;
- Adopting measures to facilitate the sharing of information on their products' potential vulnerabilities;
- Providing for secure update distribution mechanisms;
- Ensuring that security updates and patches are distributed without delay;

The ANFR (the National Frequency Agency) – designated as the authority for market supervision – will, in cooperation with ANSSI, be responsible for monitoring providers' compliance with these requirements. ←

2/NOTABLE VULNERABILITIES IN 2025, AND OTHER WEAKNESSES IN EDGE DEVICES

Despite the growing number of vulnerabilities identified and disclosed each year, ANSSI's incident response information for 2025 showed that specific vulnerabilities remained exploited recurrently and at scale.

Edge devices remain the prime targets of cyberattacks, given that their widespread use allows attackers to conduct opportunistic, large-scale operations and to gain initial access or turn them into hosts for anonymisation infrastructures.

Some vulnerabilities may also be more discretely exploited, to preserve the capabilities they provide and to enhance the attacker's stealth. In one of the cases observed by ANSSI, for example, an attacker patched the CVE-2024-8190, CVE-2024-8963, and CVE-2024-9380[33] vulnerabilities after exploiting them, to then lateralise themself on the victim entity's inter-nal network. During internal vulnerability scans, the affected devices therefore appeared to be up-to-date. This example demonstrates the importance of meticulously monitoring the implementation of security patches.

Since the beginning of 2025, ANSSI has been notified of the compromise of several Connect Secure VPN appliances – commercialised by Ivanti – by attackers exploiting the CVE-2025-0282 and CVE-2025-0283 vulnerabilities [79][80]. In at least two of these cases, the attacker was able to lateralise themself on the information system to reach internal resources. On the 8th of January 2025, when the patch was published, the security vendor Mandiant published a report on the ex-ploitation of the CVE-2025-0282 vulnerability, since at least mid-December of 2024, by the reputedly Chinese intrusion set UNC5221. This intrusion set had already been employed at least thrice between December of 2023 and March of 2025, during the exploitation of zero-day vulnerabilities affecting Ivanti security devices. These attack campaigns led to the compromise of multiple Ivanti devices across the world, including some belonging to public and private entities in France (sources: GTIG, Volexity, GTIG, justice.gov). This targeting indicates that some actors are particularly interested in this type of devices.

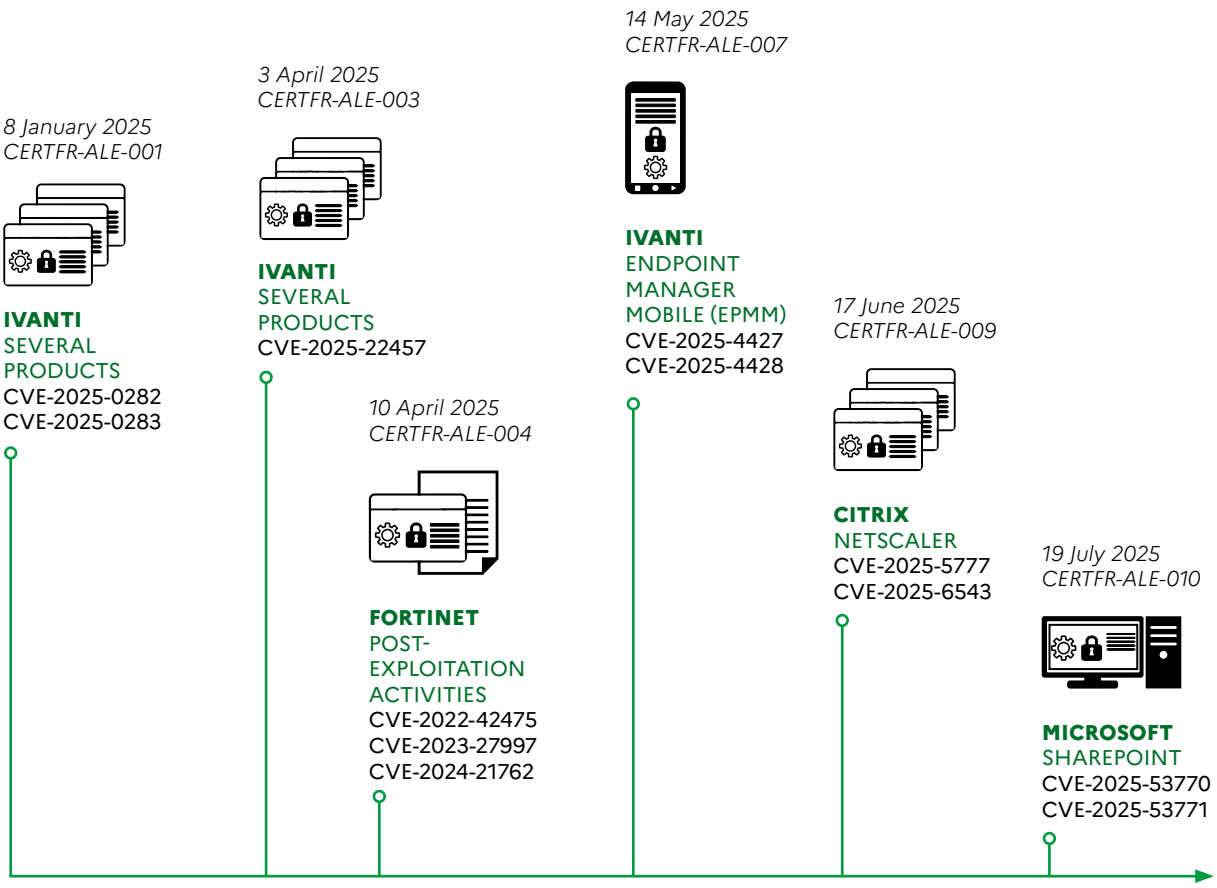
Server and IT environments have also been subjected to the exploitation of significant vulnerabilities. This indicates a certain interest, on the part of attackers, in data which is directly accessible from compromised devices, for both espionage and extortion purposes.

During the summer of 2025, Microsoft Sharepoint solution was affected by multiple exploited vulnerabilities. Both patched with the publication of their respective updates on the 8th and 20th of July 2025, the CVE-2025-49704, CVE-2025-49706, then CVE-2025-53771 and CVE-2025-53770 vulnerabilities were indeed subjected to multiple waves of exploitation. Though the large-scale exploitation of the first two vulnerabilities – dubbed "toolshell" – was first publicly reported by Eye Security on the 18th of July [81], ANSSI observed their zero-day exploitation from the end of June 2025. Several exploit proof-of-concepts were then published from the 21st of July, allowing an even greater number of malicious actors to utilise them.

Among the numerous cases of compromise which impacted SharePoint servers, the ransomware group WarLock used these vulnerabilities to gain a foothold on the internal servers of French entities and subsequently encrypt their resources. Other attackers were seen exploiting these vulnerabilities to access business data of interest, though their intentions have not been precisely defined. Amongst the actions performed by the attackers, the recovery of Machine Keys – notably used to encrypt sensitive data – was observed. This practice is a reminder that, in addition to applying security patches and ousting potential attackers, responses to exploited vulnerabilities should also involve the renewal of secrets associated with the affected equipment – in this instance, Machine Keys.

33 Vulnerabilities affecting Ivanti CSA devices.

Vulnerabilities most exploited in the incidents processed by ANSSI in 2025



Furthermore, the compromise of several other Ivanti Connect Secure VPN devices was reported to ANSSI following the exploitation of the CVE-2025-22457 vulnerability, which could allow for the remote execution of arbitrary code. Once again, the timeframe between the publication of the alert and the detailed analysis of the vulnerability was particularly short.

In addition to these vulnerabilities, edge devices are also affected by weaknesses which do not possess a CVE identifier[34]. ANSSI for instance handled an attack campaign against Cisco devices during which the attacker took advantage of weaknesses in a protocol devoid of authentication mechanisms and exposed on the Internet: Cisco Smart Install (SMI). During the first stage of the campaign, the attacker performed mass untargeted actions aimed at exposing the configuration of devices on the Internet. More targeted actions against certain entities were then observed. ANSSI suspects that these undocumented features may have been used in combination with other vulnerabilities to allow the attacker to lateralise themself on their victims' information systems. Over 50 different devices were compromised during this campaign.

Amongst the numerous incidents treated in 2025, attackers also compromised VPN accounts – devoid of any strong authentication mechanisms – to penetrate their targets' internal networks. Though this is not a new practice, this method remains one of the primary vectors of intrusion used by attackers seeking to take advantage of poorly protected gateways. ANSSI intervened in a number of cases of ransomware infections, impacting both single user and service provider accounts, where this technical weakness was exploited.

34
Common Vulnerabilities and Exposures, or CVE, catalogues all known cybersecurity vulnerabilities on a global scale.

3/WEBMAIL, VIRTUALISATION, AND MOBILE DEVICES REMAIN PRIME TARGETS

The exploitation of XSS[35] zero-day vulnerabilities against webmail clients was a major trend in 2025, as in previous years. While the offensive potential of this type of vulnerability re-mains limited, partly due to the impossibility of ensuring persistence on victim devices, the possibilities it can unlock may still interest attackers: theft of e-mails or contact lists, recov-ery of login credentials via fake login pages, or implementation of e-mail redirection filters. Such attacks have notably been associated with intrusion sets reputedly linked to the Rus-sian and potentially Belarussian threat – such, for instance, as UNC1151 [82] and APT28 [83][84] in 2025, or Winter Vivern from 2023 [85].

Given their unwavering success, virtualisation solutions have, once again in 2025, also been targeted and compromised via zero-day vulnerabilities. On the 6th of March 2025, three critical vulnerabilities (CVE-2025-22224, CVE-2025-22225, CVE-2025-22226) affecting VMware ESXi, Workstation and Fusion were published simultaneously with the revelation of their zero-day exploitation [86].

This type of solution is particularly targeted by operators of reputedly Chinese intrusion sets. In 2025, the UNC5221 and UNC5174 intrusion sets (also referred to as Houken by ANSSI) targeted and compromised such environments [87][88]. The attackers behind UNC5221 furthermore exhibited a solid understanding of these environments as they injected a Servlet filter into memory to position a backdoor on a VMware vCenter server. ←

The targeting of mobile devices

Mobile phones are now part of everyday life. Their growing use in both personal and professional settings have made them prime targets for cyberattacks, particularly given the information they may hold. Vulnerabilities on wireless interfaces (mobile network, Wi-Fi, Bluetooth) or on the operating system itself are therefore regularly exploited, much like some applications, by virtue of the sensitivity of the data they contain. Like any other IT devices, mobile phones provide opportunities for attackers with varying motivations.

Among these threats, ANSSI has mainly observed cases of compromise achieved for espionage and surveillance purposes, via capabilities developed internally or obtained through private companies specialised in cyberwarfare. These companies provide access to sophisticated technologies, allowing new offensive actors to emerge and consequently elevating the associated level of threat. In addition to espionage, mobile phones have also been targeted by cybercriminals seeking financial gain or, more rarely, diverted for private surveillance or destabilisation operations.

Advanced vulnerabilities in components and applications are regularly being patched. In August and September of 2025, Apple, Samsung, and Meta published updates regarding actively exploited vulnerabilities (CVE-2025-43300, CVE-2025-21043, and CVE-2025-55177), respectively) whose combined use allowed attackers to compromise Apple and Samsung mobile phones remotely, without the need for user interaction. One vulnerability, affecting WhatsApp, was chained with another vulnerability in the operating system's DNG image-processing component (iOS or Android). The chained exploitation of vulnerabilities targeting the same format on both iOS and Samsung combined with a zero-day vulnerability in a popular messaging application is indicative of sophisticated research capabilities and of an intent to target a broad range of users.

Since 2021, Apple has been sending out batches of "threat notifications" to victims whose mobile devices have been targeted by spyware such as Pegasus, Predator, and Triangulation[36]. ANSSI chose to communicate on these alerts as a way to increase awareness of this threat among the high authorities, company executive committees, and civil society. Ad-ditionally, ANSSI published a more in-depth document detailing the different technical vectors used by attackers to compromise mobile phones. It presents an overview of the threats facing mobile phone users, providing concrete examples of attacks conducted in France or abroad. This threat overview also contains security recommendations for users [89].

35
Cross site scripting (XSS) vulnerabilities, or indirect code injections, consist in injecting arbitrary data in HTML webpage code, for example to redirect a user towards a different website.

36
When receiving reports (e-mails, text messages) from solution vendors alerting to the potential compromise of an account or device, it is recommended to stop handling the mobile phone and to contact the CERT-FR

- by e-mail at → cert-fr@ssi.gouv.fr or
- by phone at → 3218 (free service + cost of a call) → or +33 (0) 9 70 83 32 18.

C
THE TARGETING OF SUBCONTRACTORS AS A VECTOR OF COMPROMISE

→ Supply-chain attacks consist in compromising a third party, such as a software supplier or service provider, to target the intended victim. This technique has been tried-and-tested by several cybercriminal and state actors since at least 2016. This type of attack can spread quickly and sometimes impact entire industries or specific geographical areas, particularly when attackers are targeting widespread software providers, local digital service providers (DSPs), or companies operating in a specific industry [90]. The attackers responsible for these attacks may seek to exfiltrate information through a third party, to conduct lucrative attacks, or to temporarily or durably paralyse a sector or group of entities.

With the development of subcontracting, and the delegation of capabilities within some industries, companies may lose control over some of the devices connected to their networks. Such circumstances undermine the overall security of these environments, and attackers may take advantage of this development to achieve their compromise.

Several reputedly Russian, Chinese, and Iranian state actors have led supply-chain attacks over the past few years.

Supply-chain attacks are however not the prerogative of reputedly state-backed intrusion sets. Between January and June of 2025, ANSSI observed the compromise *via* ransomware of several industrial entities involved in the supply chain of the French Defence Technological and Industrial Base (DTIB). Responsible for designing and manufacturing systems, parts, and software linked to the armaments and aeronautics industries, these companies can have access to sensitive information which runs the risk of being exposed during attacks. While ANSSI does not consider these attacks to have been coordinated (the companies were compromised by different ransomware operators), this kind of security event highlights the importance of identifying essential subcontractors and helping them to improve their cybersecurity. In 2025, the defence industry was also subjected to reconnaissance activities, compromise attempts, and cases of compromise achieved *via* reputedly state-backed intrusion sets for the purpose of strategic espionage and intelligence-gathering.

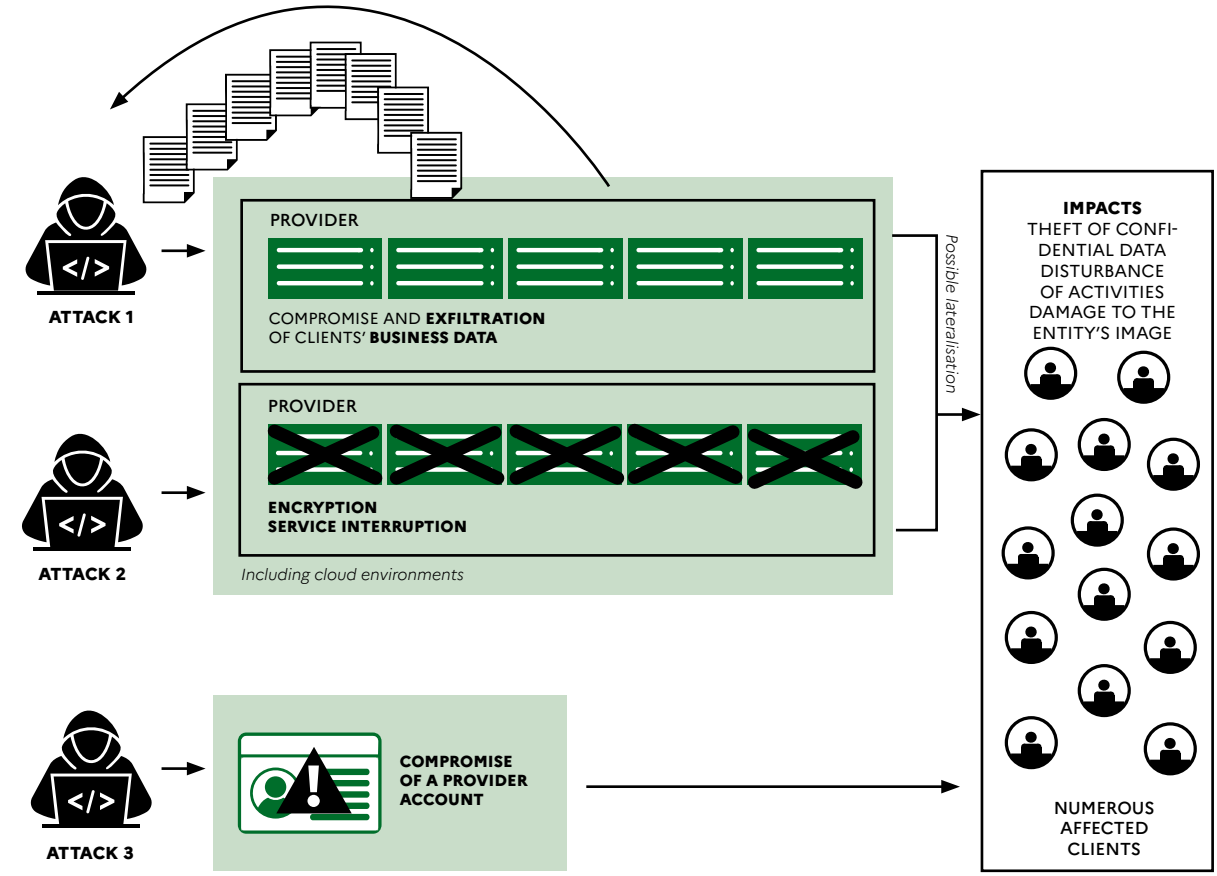
In 2025, ANSSI witnessed the compromise of several entities by attackers capable of lateralising themselves from service providers' information systems to their clients. For example, an attacker compromised and exfiltrated client resources from a service provider working alongside numerous French entities. Taking advantage of the interconnections which linked the provider to its clients' information systems and using stolen login credentials, the attackers were able to lateralise themself on the information systems of several clients.

In other cases observed by ANSSI, attackers performed rebound attacks by compromising an initial victim – who did not necessarily need to be a subcontractor – and using their resources to target other entities. The internal resources taken from the first compromised entity could be used to forge or obtain credible components which facilitated the targeting of a second entity [91] [92].

ANSSI also witnessed cases whereby the compromise of service providers via ransomware generated significant impacts on their clients. In one of these cases, the compromise of a French entity's resources disrupted its clients' access to the application provided. This incident caused major disruptions in the activities of several actors operating in the same industry.

The containment measures implemented during this type of attack may also have a significant impact on clients who might lose access to some resources. ←

Supply chain



The compromise of cloud environments

As a result of the growing use of cloud services amongst many organisations, cases of compromise affecting the data hosted within these environments are regularly observed. Several cases of ransomware attacks involving the encryption of data hosted on cloud resources were notably reported to ANSSI in 2025, which suggests that numerous malicious actors are conscious of this development. The generalisation of cloud-hosted solutions represents an opportunity for these actors to acquire the data of several different entities by compromising a single service provider. In October of 2025, ANSSI was informed of a ransomware attack which resulted in the encryption of resources linked to a French vendor's Software-as-a-Service solution which had been hosted on an Amazon Web Services cloud environment.

The client's lack of control over this type of environment can sometimes hinder analyses during incident response. In a major compromise case observed in 2025, doubt removals performed by the victim with ANSSI's support proved inconclusive due to the difficulties faced when attempting to retrieve the logs associated with the potentially compromised cloud resources.

It should also be noted that incidents involving cloud service providers, now critical links of supply chains in most industries, can affect a large number of entities. In July of 2025, the compromise and encryption of an important French entity's cloud resources was observed, engendering the momentary unavailability of services for both professional clients and the general public in France.

ANSSI was informed by one of its constituents of the compromise of a development platform hosted in the Cloud. The attacker exploited a vulnerability affecting an edge device, triggering service interruptions. The victim's reactivity during the remediation process put a stop to the attack.

These attacks can also affect the confidentiality of hosted data – as was the case with the cyberattack led against the company RedHat, which had observed the compromise of one of its GitLab instances in October of 2025, leading to an exfiltration of data linked to thousands of private code repositories belonging to numerous organisations across the world, including French entities.

The deployment of crypto-mining software has also been regularly observed. In June of 2025, ANSSI was informed of the compromise of a public entity's cloud instances by a malicious actor who subsequently attempted to exploit the available computational resources and mine for cryptocurrency.

In 2025, ANSSI published an Overview of the threats targeting Cloud Computing, which includes recommendations for Cloud service providers and their clients [93].


SECURITY
PANORAMA
DEFENSE
CYBERMENACE

BIBLIOGRAPHY

[01] SUSPECTED COLLINS AEROSPACE HACKER ARRESTED IN UK.
24 09 2025.
https://www.bankinfosecurity.com/suspected-collins-aerospace-hacker-arrested-in-uk-a-29531

[02] NEWS, RECORDED FUTURES. RESEARCHERS WARN OF QILIN RANSOMWARE GANG AFTER GROUP HIT HUNDREDS OF ORGS THIS YEAR.
28 10 2025.
https://therecord.media/qilin-ransomware-gang-hits-hundreds-of-orgs-2025

[03] OPÉRATION ENDGAME 2025.
23 05 2025.
https://www.cert.ssi.gouv.fr/cti/CERTFR-2025-CTI-008/

[04] PRÉPARER LA REMÉDIATION.
16 01 2026.
https://messervices.cyber.gouv.fr/guides/cyberattaques-et-remediation-preparer-la-remedation

[05] ORACLE E-BUSINESS SUITE ZERO-DAY EXPLOITED IN WIDESPREAD EXTORTION CAMPAIGN.
10 09 2025.
https://cloud.google.com/blog/topics/threat-intelligence/oracle-ebusiness-suite-zero-day-exploitation

[06] EXFILTRATION DE DONNÉES DU SECTEUR SOCIAL: RETOUR D'EXPÉRIENCE DU CERT-FR.
18 09 2024.
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2024-CTI-009.pdf

[07] EXTORTION AND RANSOMWARE TRENDS JANUARY-MARCH 2025.
23 04 2025.
https://unit42.paloaltonetworks.com/2025-ransomware-extortion-trends/

[08] #STOPRANSOMWARE: RANSOMWARE ATTACKS ON CRITICAL INFRASTRUCTURE FUND DPRK MALICIOUS CYBER ACTIVITIES.
09 02 2023.
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-040a

[09] APT41: A DUAL ESPIONAGE AND CYBER CRIME OPERATION.
07 08 2019.
https://cloud.google.com/blog/topics/threat-intelligence/apt41-dual-espionage-and-cyber-crime-operation?hl=en

[10] MEET NAILAOLOCKER: A RANSOMWARE DISTRIBUTED IN EUROPE BY SHADOWPAD AND PLUGX BACKDOORS.
18 02 2025.
https://www.orangecyberdefense.com/global/blog/cert-news/meet-nailaolocker-a-ransomware-distributed-in-europe-by-shadowpad-and-plugx-backdoors

[11] NAILAOLOCKER RANSOMWARE'S "CHEESE".
18 07 2025.
https://www.fortinet.com/blog/threat-research/nailaolocker-ransomware-cheese

[12] UPDATED SHADOWPAD MALWARE LEADS TO RANSOMWARE DEPLOYMENT.
20 02 2025.
https://www.trendmicro.com/en_us/research/25/b/updated-shadowpad-malware-leads-to-ransomware-deployment.html

[13] SUPPLY CHAIN ATTACKS: MENACES SUR LES PRESTATAIRES DE SERVICE ET LES BUREAUX D'ÉTUDES.
07 10 2019.
https://www.cert.ssi.gouv.fr/cti/CERTFR-2019-CTI-004/

[14] CHINA-LINKED ESPIONAGE TOOLS USED IN RANSOMWARE ATTACKS.
13 02 2025.
https://www.security.com/threat-intelligence/chinese-espionage-ransomware

[15] RUSSIAN FSB CYBER ACTOR STAR BLIZZARD CONTINUES WORLDWIDE SPEARPHISHING CAMPAIGNS.
07 12 2023.
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-341a

[16] FRENCH NGO REPORTERS WITHOUT BORDERS TARGETED BY CALISTO IN RECENT CAMPAIGN.
03 12 2025.
https://blog.sekoia.io/ngo-reporters-without-borders-targeted-by-calisto-in-recent-campaign/

[17] RSF CIBLÉE PAR UNE CYBERATTAQUE ATTRIBUÉE À UN GROUPE RÉPUTÉ PROCHE DES SERVICES DE RENSEIGNEMENTS RUSSES.
08 12 2025.
https://rsf.org/fr/rsf-cibl%C3%A9e-par-une-cyberattaque-attribu%C3%A9e-%C3%A0-un-groupe-r%C3%A9put%C3%A9-proche-des-services-de-renseignements

[18] AIVD AND MIVD IDENTIFY NEW RUSSIAN CYBER THREAT ACTOR.
27 05 2025.
https://www.aivd.nl/documenten/publicaties/2025/05/27/aivd-en-mivd-onderkennen-nieuwe-russische-cyberactor

[19] APT31/WUHAN XIAORUIZHI SCIENCE &TECHNOLOGY COMPANY, LTD.
https://rewardsforjustice.net/fr/rewards/apt31-wuhan-xiaoruizhi-science-technology-company-ltd/

[20] STATEMENT BY THE GOVERNMENT OF THE CZECH REPUBLIC ON THE CYBER ATTACK FROM THE PEOPLE´S REPUBLIC OF CHINA.
08 05 2025.
https://mzv.gov.cz/jnp/en/issues_and_press/press_releases/statement_by_the_government_of_the_czech.html

[21] UAT-5918 TARGETS CRITICAL INFRASTRUCTURE ENTITIES IN TAIWAN.
20 03 2025.
https://blog.talosintelligence.com/uat-5918-targets-critical-infra-in-taiwan/

[22] SALT TYPHOON: DATA THEFT LIKELY SIGNALS EXPANDED TARGETING.
11 06 2025.
https://s3.documentcloud.org/documents/25998809/20250611-dhs-salt-typhoon.pdf

[23]WHEN NOKIA PULLED OUT OF RUSSIA, A VAST SURVEILLANCE SYSTEM REMAINED.
28 03 2022.
https://www.nytimes.com/2022/03/28/technology/nokia-russia-surveillance-system-sorm.html

[24] DECEPTION IN DEPTH: PRC-NEXUS ESPIONAGE CAMPAIGN HIJACKS WEB TRAFFIC TO TARGET DIPLOMATS.
25 08 2025.
https://cloud.google.com/blog/topics/threat-intelligence/prc-nexus-espionage-targets-diplomats?hl=en

[25] UNC6384 WEAPONIZES ZDI-CAN-25373 VULNERABILITY TO DEPLOY PLUGX AGAINST HUNGARIAN AND BELGIAN DIPLOMATIC ENTITIES.
30 10 2025.
https://arcticwolf.com/resources/blog/unc6384-weaponizes-zdi-can-25373-vulnerability-to-deploy-plugx/

[26] THE BADPILOT CAMPAIGN: SEASHELL BLIZZARD SUBGROUP CONDUCTS MULTIYEAR GLOBAL ACCESS OPERATION.
12 02 2025.
https://www.microsoft.com/en-us/security/blog/2025/02/12/the-badpilot-campaign-seashell-blizzard-subgroup-conducts-multiyear-global-access-operation/

[27] ENERGY SECTOR INCIDENT REPORT - 29 DECEMBER 2025.
29 12 2025.
https://cert.pl/en/posts/2026/01/incident-report-energy-sector-2025/

[28] DÉNI DE SERVICE RÉSEAU - QUALIFICATION.
28 07 2025.
https://www.cert.ssi.gouv.fr/fiche/CERTFR-2024-RFX-009/

[29] DÉNI DE SERVICE RÉSEAU - ENDIGUEMENT.
28 07 2025.
https://www.cert.ssi.gouv.fr/fiche/CERTFR-2024-RFX-010/

[30] RECOMMANDATIONS À DESTINATION DES ACTEURS DU SECTEUR DE L'ÉNERGIE ET DE L'EAU.
22 01 2026.
https://www.cert.ssi.gouv.fr/dur/CERTFR-2025-DUR-003/

[31] NORWAY'S SPY CHIEF BLAMES RUSSIAN HACKERS FOR DAM SABOTAGE IN APRIL.
13 08 2025.
https://www.reuters.com/technology/norway-spy-chief-blames-russian-hackers-dam-sabotage-april-2025-08-13/

[32] REMOTE MONITORING AND MANAGEMENT (RMM) TOOLING INCREASINGLY AN ATTACKER'S FIRST CHOICE.
07 03 2025.
https://www.proofpoint.com/us/blog/threat-insight/remote-monitoring-and-management-rmm-tooling-increasingly-attackers-first-choice

[33] UK ARRESTS FOUR IN 'SCATTERED SPIDER' RANSOM GROUP.
10 07 2025.
https://krebsonsecurity.com/2025/07/uk-charges-four-in-scattered-spider-ransom-group/

[34] APT28 LEVERAGES MULTIPLE PHISHING TECHNIQUES TO TARGET UKRAINIAN CIVIL SOCIETY.
17 05 2023.
https://blog.sekoia.io/apt28-leverages-multiple-phishing-techniques-to-target-ukrainian-civil-society/

[35] APT28 CAMPAIGN TARGETING POLISH GOVERNMENT INSTITUTIONS.
08 05 2024.
https://cert.pl/en/posts/2024/05/apt28-campaign/

[36] FIGHTING URSA LURING TARGETS WITH CAR FOR SALE.
02 08 2024.
https://unit42.paloaltonetworks.com/fighting-ursa-car-for-sale-phishing-lure/

[37] APT28 OPERATION PHANTOM NET VOXEL.
16 09 2025.
https://blog.sekoia.io/apt28-operation-phantom-net-voxel/

[38] APT28 ATTACKS UKRAINIAN GOVERNMENT AGENCIES VIA SIGNAL USING MALWARE.
01 07 2025.
https://csirt.csi.cip.gov.ua/en/posts/apt28-attacks-ukrainian-government-agencies-via-signal-using-malware

[39] APT MUDDYWATER DEPLOYS MULTI-STAGE PHISHING TO TARGET CFOS.
20 08 2025.
https://hunt.io/blog/apt-muddywater-deploys-multi-stage-phishing-to-target-cfos

[40] MAPPING THE INFRASTRUCTURE AND MALWARE ECOSYSTEM OF MUDDYWATER.
17 09 2025.
https://www.group-ib.com/blog/muddywater-infrastructure-malware/

[41] RECOMMANDATIONS DE SÉCURITÉ POUR UN SYSTÈME D'IA GÉNÉRATIVE.
29 04 2024.
https://messervices.cyber.gouv.fr/guides/recommandations-de-securite-pour-un-systeme-dia-generative

[42] SCATTERED SPIDER.
29 07 2025.
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a

[43] DEFENDING AGAINST SCATTERED SPIDER AND THE COM WITH CYBERCRIME INTELLIGENCE.
15 07 2024.
https://www.sans.org/blog/defending-against-scattered-spider-and-the-com-with-cybercrime-intelligence

[44] WHAT'S IN AN ASP? CREATIVE PHISHING ATTACK ON PROMINENT ACADEMICS AND CRITICS OF RUSSIA.
18 06 2025.
https://cloud.google.com/blog/topics/threat-intelligence/creative-phishing-academics-critics-of-russia?hl=en

[45] SAME SEA, NEW PHISH - RUSSIAN GOVERNMENT-LINKED SOCIAL ENGINEERING TARGETS APP-SPECIFIC PASSWORDS.
18 06 2025.
https://citizenlab.ca/research/russian-government-linked-social-engineering-targets-app-specific-passwords/

[46] STORM-2372 CONDUCTS DEVICE CODE PHISHING CAMPAIGN.
13 02 2025.
https://www.microsoft.com/en-us/security/blog/2025/02/13/storm-2372-conducts-device-code-phishing-campaign/

[47] MULTIPLE RUSSIAN THREAT ACTORS TARGETING MICROSOFT DEVICE CODE AUTHENTICATION.
13 02 2025.
https://www.volexity.com/blog/2025/02/13/multiple-russian-threat-actors-targeting-microsoft-device-code-authentication/

[48] FAKE CAPTCHA ATTACKS DEPLOY INFOSTEALERS AND RATS IN A MULTISTAGE PAYLOAD CHAIN.
19 05 2025.
https://www.trendmicro.com/fr_fr/research/25/e/unmasking-fake-captcha-cases.html

[49] ADWARE CAMPAIGN USES FAKE CAPTCHA TO DELIVER LUMMA AND AMADEY MALWARE.
10 09 2024.
https://www.broadcom.com/support/security-center/protection-bulletin/adware-campaign-uses-fake-captcha-to-deliver-lumma-and-amadey-malware

[50] Кібератака UAC-0001 (APT28): PowerShell-команда в буфері обміну як "точка входу" (CERT-UA#11689).
25 10 2024.
https://cert.gov.ua/article/6281123

[51] COLDRIVER UPDATES ARSENAL WITH BAITSWITCH AND SIMPLEFIX.
24 09 2025.
https://www.zscaler.com/blogs/security-research/coldriver-updates-arsenal-baitswitch-and-simplefix

[52] PHANTOMCAPTCHA | MULTI-STAGE WEBSOCKET RAT TARGETS UKRAINE IN SINGLE-DAY SPEARPHISHING OPERATION.
22 10 2025.
https://www.sentinelone.com/labs/phantomcaptcha-multi-stage-websocket-rat-targets-ukraine-in-single-day-spearphishing-operation/

[53] APT39: AN IRANIAN CYBER ESPIONAGE GROUP FOCUSED ON PERSONAL INFORMATION.
29 01 2019.
https://cloud.google.com/blog/topics/threat-intelligence/apt39-iranian-cyber-espionage-group-focused-on-personal-information?hl=en

[54] PHOSPHORUS AUTOMATES INITIAL ACCESS USING PROXYSHELL.
21 03 2022.
https://thedfirreport.com/2022/03/21/phosphorus-automates-initial-access-using-proxyshell/

[55] DALBIT (M00NLIGHT): CHINESE HACKER GROUP'S APT ATTACK CAMPAIGN.
13 02 2023.
https://asec.ahnlab.com/en/47455/

[56] ICEPEONY WITH THE '996' WORK CULTURE.
16 10 2024.
https://nao-sec.org/2024/10/IcePeony-with-the-996-work-culture.html

[57] APT41 HAS ARISEN FROM THE DUST.
18 07 2024.
https://cloud.google.com/blog/topics/threat-intelligence/apt41-arisen-from-dust?hl=en

[58] HOUKEN: SEEKING A PATH BY LIVING ON THE EDGE WITH ZERO DAYS.
01 07 2025.
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2025-CTI-009.pdf

[59] GAMAREDON X TURLA COLLAB.
19 09 2025.
https://www.welivesecurity.com/en/eset-research/gamaredon-x-turla-collab/

[60] FRAUDSTERS IMPERSONATE CLOP RANSOMWARE TO EXTORT BUSINESSES.
14 03 2025.
https://www.infosecurity-magazine.com/news/fraudsters-clop-ransomware-extort/

[61] SHINYHUNTERS BEHIND SALESFORCE DATA THEFT ATTACKS AT QANTAS, ALLIANZ LIFE, AND LVMH.
30 07 2025.
https://www.bleepingcomputer.com/news/security/shinyhunters-behind-salesforce-data-theft-attacks-at-qantas-allianz-life-and-lvmh/

[62] THE RANSOMWARE CYBER THREAT LANDSCAPE H1-23.
13 07 2023.
https://www.kovrr.com/reports/the-ransomware-threat-landscape-h123

[63] TRACKING ADVERSARIES: EVILCORP, THE RANSOMHUB AFFILIATE.
02 04 2025.
https://blog.bushidotoken.net/2025/04/tracking-adversaries-evilcorp-ransomhub.html

[64] RANSOMWARE ANNUAL REPORT 2024.
13 01 2025.
https://cyberint.com/blog/research/ransomware-annual-report-2024/

[65] RANSOMWARE DEBRIS: AN ANALYSIS OF THE RANSOMHUB OPERATION.
25 04 2025.
https://www.group-ib.com/blog/ransomware-debris/

[66] BLACK BASTA RANSOMWARE LEAK: KEY FINDINGS AND INSIGHTS.
25 04 2025.
https://www.first.org/blog/20250321-black-basta-ransomware-leak

[67] INSIDE THE LOCKBIT'S ADMIN PANEL LEAK: AFFILIATES, VICTIMS AND MILLIONS IN CRYPTO.
12 06 2025.
https://www.trellix.com/blogs/research/inside-the-lockbits-admin-panel-leak-affiliates-victims-and-millions-in-crypto/

[68] CYBER THREAT OVERVIEW 2024.
11 03 2025.
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2025-CTI-004.pdf

[69] STATE SECRETS FOR SALE: MORE LEAKS FROM THE CHINESE HACK-FOR-HIRE INDUSTRY.
01 07 2025.
https://spycloud.com/blog/state-secrets-for-sale-chinese-hacking/

[70] KNOWNSEC BREACH: WHAT WE KNOW SO FAR.
06 11 2025.
https://substack.com/home/post/p-178189244

[71] ILLUSTRATION DES PROBLÉMATIQUES LIÉES À L'INTÉGRATION DE LOGICIELS NON MAÎTRISÉS.
23 11 2022.
https://www.cert.ssi.gouv.fr/cti/CERTFR-2022-CTI-006/

[72] MANIPULATION D'ALGORITHMES ET INSTRUMENTATLISATION D'INFLUENCEURS - ENSEIGNEMENTS DE L'ÉLECTION PRÉSIDENTIELLE EN ROUMANIE ET RISQUES POUR LA FRANCE.
02 2025.
https://www.sgdsn.gouv.fr/files/files/Publications/20250204_NP_SGDSN_VIGINUM_Rapport_public_Elections_roumanie_risques_france_VFF.pdf

[73] COMUNICAT DE PRESĂ.
04 12 2024.
https://www.presidency.ro/ro/media/comunicate-de-presa/comunicat-de-presa1733327193

[74] PRO-RUSSIAN GROUP CLAIMS HITS ON DANISH PARTY WEBSITES AS VOTERS HEAD TO POLLS.
18 11 2025.
https://therecord.media/denmark-election-political-government-websites-ddos-incidents

[75] FLERE PARTIERS HJEMMESIDER RAMT AF DDOS-ANGREB.
17 11 2025.
https://samsik.dk/artikler/2025/11/flere-partiers-hjemmesider-ramt-af-ddos-angreb/.

[76] A VISUAL EXPLORATION OF EXPLOITATION IN THE WILD.
https://www.cyentia.com/wp-content/uploads/2024/07/EPSS-Exploration-Of-Exploits.pdf

[77] VULNCHECK STATE OF EXPLOITATION 2026.
21 01 2026.
https://www.vulncheck.com/blog/state-of-exploitation-2026

[78] SHADOWSERVER.
https://dashboard.shadowserver.org/statistics/combined/tree/?date_range=1&source=http_vulnerable&source=http_vulnerable6&tag=cve-2023-*&tag=cve-2024-*&geo=FR&data_set=count&scale=log

[79] SECURITY ADVISORY IVANTI CONNECT SECURE, POLICY SECURE & ZTA GATEWAYS (CVE-2025-0282, CVE-2025-0283).
08 01 2025.
https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283?language=en_US

[80] VULNÉRABILITÉ DANS LES PRODUITS IVANTI.
07 05 2025.
https://cert.ssi.gouv.fr/alerte/CERTFR-2025-ALE-001/

[81] SHAREPOINT UNDER SIEGE: TOOLSHELL EXPLOIT.
18 07 2025.
https://research.eye.security/sharepoint-under-siege/

[82] UNC1151 EXPLOITING ROUNDCUBE TO STEAL USER CREDENTIALS IN A SPEAR PHISHING CAMPAIGN.
05 06 2025.
https://cert.pl/en/posts/2025/06/unc1151-campaign-roundcube/

[83] ESET IDENTIFIE UNE CAMPAGNE D'ESPIONNAGE DU GROUPE SEDNIT (APT28) EXPLOITANT DES FAILLES XSS DANS DES MESSAGERIES EN LIGNE.
15 05 2025.
https://www.eset.com/fr/about/newsroom/press-releases/recherche/espionnage-campagne-sednit-xss/

[84] 0DAY .ICS ATTACK IN THE WILD.
09 30 2025.
https://strikeready.com/blog/0day-ics-attack-in-the-wild/

[85] ZIMBRA VULNERABILITY TO TARGET WEBMAIL PORTALS OF NATO-ALIGNED GOVERNMENTS IN EUROPE.
03 30 2023.
https://www.proofpoint.com/us/blog/threat-insight/exploitation-dish-best-served-cold-winter-vivern-uses-known-zimbra-vulnerability

[86] VMSA-2025-0004: VMWARE ESXI, WORKSTATION, AND FUSION UPDATES ADDRESS MULTIPLE VULNERABILITIES (CVE-2025-22224, CVE-2025-22225, CVE-2025-22226).
04 03 2025.
https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390

[87] YOU NAME IT, VMWARE ELEVATES IT (CVE-2025-41244).
29 09 2025.
https://blog.nviso.eu/2025/09/29/you-name-it-vmware-elevates-it-cve-2025-41244/

[88] ANOTHER BRICKSTORM: STEALTHY BACKDOOR ENABLING ESPIONAGE INTO TECH AND LEGAL SECTORS.
24 09 2025.
https://cloud.google.com/blog/topics/threat-intelligence/brickstorm-espionage-campaign?hl=en

[89] ÉTAT DE LA MENACE INFORMATIQUE SUR LES ÉQUIPEMENTS MOBILES.
26 11 2025.
https://cyber.gouv.fr/actualites/etat-de-la-menace-informatique-sur-les-equipements-mobiles/

[90] CYBERDICO.
https://cyber.gouv.fr/cyberdico/#S

[91] APT TODDYCAT.
21 06 2022.
Unveiling an unknown APT actor attacking high-profile entities in Europe and Asia.
https://securelist.com/toddycat/106799/

[92] SHARPPANDA: CHINESE APT GROUP TARGETS SOUTHEAST ASIAN GOVERNMENT WITH PREVIOUSLY UNKNOWN BACKDOOR.
03 06 2021.
https://research.checkpoint.com/2021/chinese-apt-group-targets-southeast-asian-government-with-previously-unknown-backdoor/

[93] SECTEUR DU CLOUD - ÉTAT DE LA MENACE INFORMATIQUE.
20 02 2025.
https://www.cert.ssi.gouv.fr/cti/CERTFR-2025-CTI-001/

CYBER THREAT OVERVIEW 2025

Published by
French Cybersecurity Agency (ANSSI)

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

REGISTRATION OF COPYRIGHT

May 2026
Published under open license/
Open Licence (Etalab — V2.0)

ISSN : 2801-4154

FRENCH CYBERSECURITY AGENCY

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