



RÉPUBLIQUE
FRANÇAISE

*Liberté
Égalité
Fraternité*





MMXXIV

CYBER THREAT OVERVIEW

→ INTRODUCTION	4
I → OPPORTUNITIES FOR ATTACKERS	6
A → 2024 PARIS OLYMPIC AND PARALYMPIC GAMES	7
B → TECHNICAL WEAKNESSES	10
1/ A REMINDER OF 3 BEST PRACTICES FOR INFORMATION SYSTEM SECURITY	10
2/ HARDENING OF THE INFORMATION SYSTEM	10
C → EXPLOITED VULNERABILITIES	12
1/ SECURITY AND EDGE DEVICES: PRIME TARGET	12
2/ ACTORS RESPONSIBLE FOR THE EXPLOITATION OF VULNERABILITIES ON EDGE SECURITY DEVICES	16
3/ REGULATORY CHANGES AND COORDINATION IN THE HANDLING OF PRODUCT VULNERABILITIES	16
II → MEANS EMPLOYED BY ATTACKERS	18
A → TARGETING OF THE SUPPLY CHAIN	19
B → THE EVOLUTION OF ATTACK TOOLS AND INFRASTRUCTURE	22
1/ ANONYMISATION NETWORKS AND INFRASTRUCTURE	22
2/ ATTACKS WITH CAPABILITY OBJECTIVES	22
3/ THE USE OF COMMON RESOURCES OR CAPABILITIES BY STATE ACTORS AND CYBERCRIMINAL ACTORS	24
C → MERCENARIES AND SERVICE PROVIDERS	25
1/ FROM PROFITABLE BUSINESS TO ECOSYSTEM IN SERVICE OF A STATE	25
2/ THE TARGETING OF MOBILE DEVICES	25
3/ A CONSTANTLY-EVOLVING MARKET FACED WITH TECHNICAL LIMITATIONS AND MEDIA EXPOSURE	26
III → ATTACK OBJECTIVES	30
A → PROFIT-DRIVEN ATTACKS	31
1/ A PERPETUALLY HIGH LEVEL OF CYBERCRIMINAL ACTIVITY	31
2/ THE DISORGANISATION OF THE CYBERCRIMINAL ECOSYSTEM	31
3/ THE THEFT AND LEAK OF FRENCH ENTITIES' DATA	34
B → DESTABILISATION	37
1/ THE SABOTAGE OF SMALL INDUSTRIAL FACILITIES	37
2/ THE HEIGHTENED INTENSITY OF DDOS ATTACKS	38
3/ SABOTAGE AND PREPOSITIONING BY ADVANCED ACTORS	39
C → ESPIONAGE	40
1/ TARGETING LINKED TO STRATEGIC STATE INTERESTS	40
2/ THE TARGETING OF THE TELECOMMUNICATIONS SECTOR	42
→ BIBLIOGRAPHY	44

INTRODUCTION

→ The French Cybersecurity Agency (ANSSI) is the national authority in matters of cybersecurity.

ANSSI's *Cyber Threat Overview* is published annually, covering the period from January 1st to December 31st of the previous year. In this document, the Agency addresses prevalent cybersecurity threats and the pivotal incidents which occurred over the observed period.

Intended for the institutional sphere and for the Agency's beneficiaries, this *Threat Overview* is also more broadly aimed at the French cybersecurity community and at ANSSI's international partners.

Written from ANSSI's point of view, the items detailed herein do not constitute an exhaustive overview of the cybersecurity events which took place in France in 2024. This Threat Overview aims not only to raise awareness, but also to demonstrate the importance of implementing security measures.

In line with the previous years, ANSSI estimates that attackers associated with the cybercriminal ecosystem and reputedly linked to China and Russia are three of the main threats facing both critical information systems (ISs) and the national ecosystem as a whole.

This past year was marked by the hosting of the Paris Olympic and Paralympic Games which, by virtue of the event's media exposure and attack surface, presented golden opportunities for attackers. In this context, ANSSI has observed attacks aimed at extortion and strategic espionage, as well as a majority of attacks conducted by hacktivist groups for destabilisation purposes. None of these attacks have had a notable impact on the smooth running of the Games.

The year was also marked by the number and the impact of vulnerabilities affecting information systems' security edge devices: over half of ANSSI's

cyberdefense operations – which make up the highest level of the Agency's engagement in incident response – were brought about by the exploitation of vulnerabilities on such devices.

With regards to the means employed by attackers, ANSSI has noted that attacks on the supply chain are continuously being used as stepping stones to reach targets of interest. This type of attack – which has grown increasingly prevalent since the late 2010s – demonstrates the importance of organisations controlling their ISs, as well as their interconnections and dependencies.

Simultaneously, attackers also persist with their use of anonymisation networks. These networks of interconnected compromised devices allow attackers to conceal their actions and thus complicate their attribution at every stage of the cyberattack. They form increasingly developed and complex infrastructures whose users are not always easily identifiable. Private companies grow ever more involved in offensive cyberwarfare, providing to a relatively large number of clients advanced capabilities which hitherto had been reserved to states with more advanced cyber means.

In 2024 ANSSI's teams have been frequently mobilised to handle ransomware attacks, whose numbers were comparable to those of the previous year. Attacks aimed at espionage have also been characterised by the sustained targeting of telecommunication devices and infrastructure.

In addition to attacks aimed at espionage and extortion – which remain the primary types of incidents processed by ANSSI – 2024 was also marked by a notable rise in attacks aimed at destabilisation, particularly conducted by hacktivist groups. ←

How to proceed in the event of a compromise?

In the event of a compromise or suspected compromise, the CERT-FR recommends that you consult the following page: <https://www.cert.ssi.gouv.fr/les-bons-reflexes-en-cas-dinvasion-sur-un-systeme-dinformation/>

Contact the CERT-FR:

- By phone:
 - from mainland France at 3218 (free service + call charges) or at 09 70 83 32 18
 - from certain overseas territories or abroad at +33 9 70 83 32 18

- By e-mail
 - at cert-fr@ssi.gouv.fr



OPPORTUNITIES FOR ATTACKERS

This past year, in addition to the usual weaknesses impacting the security of ISs and to the technical vulnerabilities closely monitored by a multiplicity of actors, the 2024 Paris Olympic and Paralympic Games also presented a major opportunity for politically-motivated actors.

For attackers – whether they be backed by states intending to spy or destabilise, or simply

seeking to capitalise on a highly mediatised context – large-scale events present new motivations and opportunities to act.

Though most of the attention was turned towards the Games in 2024, the year was also marked by multiple electoral processes – including the French legislative and European elections – during which no attack of significant scale was observed.

A

2024 PARIS OLYMPIC AND PARALYMPIC GAMES

→ By virtue of their global exposure and of the financial flows they generate, the Games present a golden opportunity for attackers driven by various motivations. Malicious actors may seek to make a profit through cybercriminal activities, to disrupt the smooth running of the event, or to undermine the host country's reputation on the international scene. In the run up to the Games, the Olympic Organising Committee indicated that it was expecting eight to ten times more cyberattacks than during the Tokyo Games, and estimated that the threat level would be multiplied by ten. Against this backdrop of tensions, ANSSI undertook significant preparatory work alongside all of the entities involved in the organisation of the Games [01].

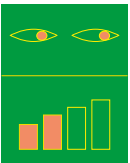
In its evaluation of the threat facing the 2024 Olympic and Paralympic Games [02], ANSSI had anticipated:



- A **high level of financially-motivated threat**: “common” scams, extortion attempts, data thefts, or opportunistic attacks taking advantage of a reliance on IT services;



- A **significant level of threat aimed at destabilisation**: attacks aimed at disrupting the organisation of the Games and the smooth running of the competitions – including cyber sabotage, distributed denial of service attacks (DDoS), website defacements, or disclosures of data;



- A **medium level of threat aimed at espionage**: attacks conducted by a potentially state-backed actor, against a foreign delegation or a subcontractor in possession of sensitive data, for example.

Though this was a period of high intensity, no cyberattacks disrupted the smooth running of the 2024 Olympic and Paralympic Games. Financially-motivated attacks and destabilisation or espionage attempts were, as expected, nevertheless observed.

• ANSSI has not noted any specific or mass targeting of the Games by cybercriminal actors. Given the sheer number of entities involved in the event, levels of cybercriminal activity have not been unusual. The ransomware attacks observed over the duration of the Games have had no impact on the hosting of the competitions.

Two major ransomware attacks were observed over this period:

→ In early August of 2024, the Grand Palais-Réunion des Musées Nationaux (RMN) network was compromised via the BrainCipher ransomware. A software used by several of the museums was rendered unavailable, but the compromise did not impact the hosting of competitions within the grounds of the Grand Palais – a separate entity from the Grand Palais RMN. The affected network had no interconnections with the information systems enabling the hosting of the competitions.

→ On the 11th of August, Paris-Saclay University notified ANSSI of its compromise by the WhiteRabbit ransomware. Hosted by the university, the French antidoping laboratory (LADF) was thereafter closely monitored by stakeholders. However, the compartmentalisation of ISs and the swift implementation of relief measures made it possible to preserve the integrity of the analyses and to ensure the continuity of the laboratory's activities during the Paralympic Games.

• ANSSI observed destabilisation operations throughout the entire duration of the Games. These actions were primarily undertaken by pro-Russian and pro-Palestinian hacktivists – some of which may have been state-sponsored – and often took the form of DDoS attacks or data exfiltration claims. Attackers capitalised on the specific context of the Games to

widen their actions' reach in an already dense geopolitical climate: war in Ukraine, war in the Middle East, the arrest of Pavel Durov – CEO and founder of the Telegram messaging app – by the French authorities. Some of the data leak claims involved entities involved in the organisation of the Games, though none of these incidents had a significant impact. On the 31st of July 2024, LulzSec Muslims claimed the exfiltration of data belonging to the French National Olympic and Sports Committee (CNOSF). According to the group, this attack was a response to the opening ceremony of the 2024 Olympic and Paralympic Games.

Abroad, the most notable destabilisation attempt was the exfiltration, in July of 2024, of data belonging to the Polish Anti-Doping Agency (POLADA) by the operators of the reputedly Russian UNC1151 intrusion set. On the 6th of August 2024, the data exfiltrated from POLADA's information systems was leaked by the pro-Russian hacktivist group Beregini, in collaboration with the Zarya hacktivist group. The purpose of this claim was to condemn anti-doping regulation as a means to coerce countries whose policies differed from those of the United States. The leaked data included personal and medical data belonging to athletes, failed anti-doping tests, information pertaining to the investigation of illegal chemical laboratories, and passwords. That same month, POLADA announced that disclosed information pertaining to Polish athletes' tests had been manipulated, seemingly to spread disinformation [03].

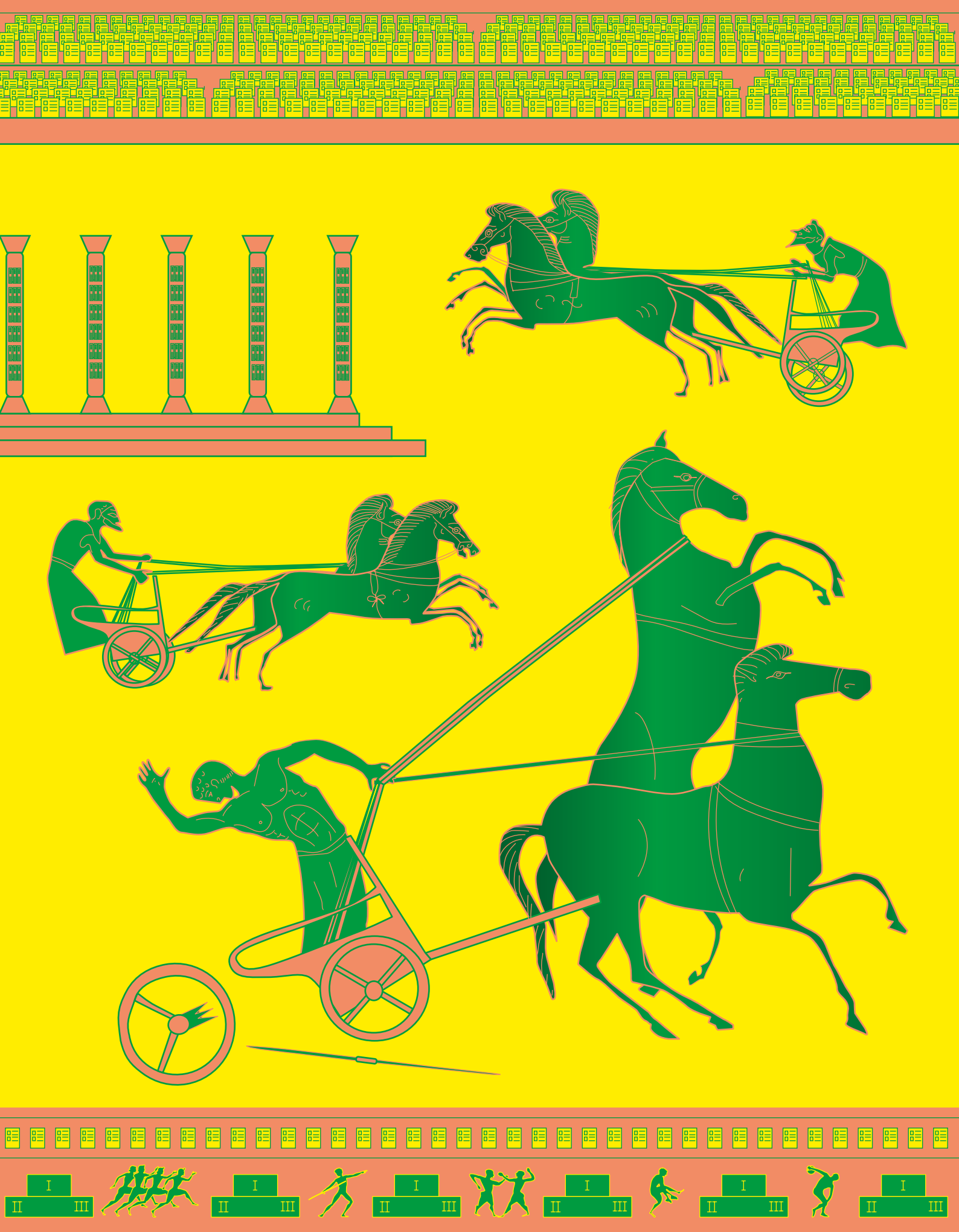
- Though ANSSI deemed possible the conduct of espionage operations against the 2024 Paris Olympic and Paralympic Games, these operations did not represent a significant threat to the smooth running of the competitions as they did not impair the availability or the integrity of the systems and of the data therein.

Attempted destabilisation operations in the context of the 2024 Paris Olympic and Paralympic Games

In late July of 2024, Viginum detected an influence and destabilisation operation conducted against the Games and against the Israeli delegation more specifically, carried out by reputedly Iranian hacktivists [04].

In this context, a notable compromise attempt aimed at destabilisation was recorded: on the 25th of July 2024, on the eve of the Olympic Games' opening ceremony, ANSSI was informed of the compromise of a company responsible for the management of advertising billboards. The Haywire Kitten intrusion set – operated, according to the FBI, by the Iranian company Emnnet Pasargad for the Islamic Revolutionary Guard Corps [05], – was observed in an unsuccessful attempt to hijack the billboards managed by the company to display photomontages condemning the participation of Israeli athletes in the Games. Once detected, the attack was swiftly thwarted by the collective efforts of the entities involved in the cybersecurity on the event [06]. ☞

ANSSI processed the compromise of a company involved in the hosting of the Game, targeted by an espionage operation likely conducted by a reputedly Chinese intrusion set. ANSSI's analyses brought to light malicious activities dating back to at least 2022, revealing that the attacker had begun pre-positioning efforts on the entity's IS very early on. This intrusion was detected prior to the start of the Games and therefore did not disrupt the smooth running of the competitions. ☜



B

TECHNICAL WEAKNESSES

→ If current large-scale events provide attackers with golden opportunities for action, the technical weaknesses revealed in information systems represent, for their part, a constant opportunity. As in previous years, ANSSI notes that attackers of varying proficiency levels are able to exploit vulnerabilities in information systems with subpar security levels. The hardening of ISs and the maintenance of their security conditions may reduce the attack surface and lower the risks of lateralisation, in accordance with the principle of defence in depth⁵.

1/ A REMINDER OF 3 BEST PRACTICES FOR INFORMATION SYSTEM SECURITY

ANSSI reiterates that the protection and maintenance of IS security can be achieved through the following best practices:

1. **Securing** the IS is the first line of defence. This step consists in preventing attacks by reducing the system's exposure and any opportunities for lateralisation – notably via the implementation of hardening measures – and aims to compel attackers to use techniques and tools likely to generate logged events;

2. **Supervision** allows for the detection of malicious activity through the analysis of system, application, or network logs, and makes it possible to lift alerts quickly as the attack progresses;

3. Incident **response** is the final step and includes crisis management, digital investigations, and remediation. In 2024, ANSSI published three guides on the strategic, organisational, and technical aspects of remediation [07].

The costs of securing the IS and implementing supervision are often much lower than those of remediation, and these measures greatly reduce the risks engendered by a security incident, its impact and severity.

2/ HARDENING OF THE INFORMATION SYSTEM

ANSSI notes that a significant number of its beneficiaries use incident detection software and services. However, such tools can only be used to their full potential if the IS has been secured and, more specifically, if defence-in-depth measures have been implemented. These measures can hamper the attacker's progress and facilitate their eviction before they are able to gain control of the IS. They also complexify lateralisation attempts and thus provide defenders with a greater window of opportunity for detection. Lastly, they significantly diminish the consequences of the compromise of the end-user workstation which, by nature, is one of the most exposed components of the IS.

According to this principle, the priority should therefore be to secure the IS's most critical asset: the authentication directory (or the tenant, wherever cloud services are used), most often an Active Directory⁶.

Though the hardening of the Active Directory is an essential step, it does not entirely prevent attacks. Incidents resulting in the deployment of ransomware were, for instance, observed in the following cases:

- The exploitation of the Zerologon vulnerability on Active Directory domain controllers whose version is not up to date, enabling the compromise of the entire IS [08];
- The lack of password management on the local administrator account of Windows servers and workstations, also enabling lateralisation. Certain solutions (such as Microsoft's LAPS service) can help to prevent this risk;
- The hijacking of legitimate but misconfigured or vulnerable asset management or business applications (backup tools, update deployment or remote handling tools, antivirus consoles or EDR, etc.), enabling the compromise of a significant portion of the IS.

5

These measures may include the hardening of configurations, the implementation of good administration practices, or the implementation of network segmentation.

6

Primary security backbone of Microsoft information systems, the Active Directory crucially enables the centralisation of accounts, resources, and permissions. Gaining high privileges on this directory allows the immediate and complete takeover of the resources administered.

The first example highlights the necessity of ensuring the security maintenance of the IS's most critical components. ANSSI notes that a substantial part of its beneficiaries operating ISs in Microsoft environment use obsolete or close to end-of-support servers and workstations:

- 82% of workstations belonging to organisations employing the Agency's ADS service use Windows 10 operating system, whose end of support is scheduled for the 14th of October 2025 (excepting the LTSC version and extended support). ANSSI recommends that a migration towards Windows 11 be initiated as early as possible.
- 36% of Windows servers belonging to organisations employing the ADS service are obsolete (Windows Server 2012R2 or lower). ANSSI recommends that operating systems be updated to their latest versions, in order to guarantee the longest period of support possible.

Amid existing defence-in-depth measures, internal network segmentation is an effective way of reducing the risks of lateralisation and of facilitating malicious activity detections. This segmentation may be implemented through the use of network mechanisms such as a private VLAN⁷ combined with filtering rules.

The securing of an IS also heavily relies on authentication processes. ANSSI observes that certain means of authentication – such, for instance, as the TOTP or the use of a third-party application – are now being circumvented by attackers equipped with new technologies and techniques (for example, see [09]). Stronger authentication processes involving the use of certificates or security keys should therefore be preferred.

Lastly, ANSSI also reiterates the importance of keeping backups – including offline backups. ←

Systemic bad practices in the configuration of Active Directories

The poor Active Directory configuration practices detailed below are common features to many of the ISs which have suffered cyberattacks and, more specifically, which have been encrypted by ransomware. Indeed, they are easily exploited by means of some widely available tools.

• Privileged accounts with the

ServicePrincipalName (SPN) attribute positioned:

The SPN attribute enables the association of Kerberos service names to Active Directory accounts. When an account has a Kerberos service name, any authenticated user may request a Kerberos ticket for this service and from there conduct a brute force attack in order to acquire the account's password (attack commonly known as "Kerberoasting". Given these risks, the SPN attribute should only be positioned on non-privileged service accounts.

• **High-privilege accounts whose passwords have not been changed for over 3 years:** High-privilege account passwords must be changed at least every 3 years, to ensure that they are only known by the current administrators. ANSSI frequently finds high-privilege account passwords which have not been changed in 15, 20, sometime 25 years, and whose complexity does not meet current criteria.

• **Enrolment permissions on certificate templates or certificate containers in AD-CS:** This type of vulnerability is linked to the poor configuration of the Microsoft AD-CS key management infrastructure, which makes it possible to generate security certificates. A valid certificate for Windows authentication can thus be generated for any of the directory's accounts, including high-privilege accounts.

• **Dangerous permissions:** The permissions of a non-privileged account – towards members of privileged groups, towards domain controllers, towards the root of "naming contexts", or towards the Group Policy Objects (GPO) applied to the members of privileged groups – may allow any attacker compromising the account to take control of one of the directory's critical components and, therefore, to compromise the entire IS.

All of these vulnerabilities are verified by the ADS service (<https://club.ssi.gouv.fr>) provided by ANSSI to its beneficiaries [10]. ↗

7

Private VLAN (or PVLAN) is a network segmentation technique which makes it possible to limit communications between devices connected to a common switch.

C EXPLOITED VULNERABILITIES

→ The exploitation of vulnerabilities – particularly those which impact equipment exposed on the Internet – is one of the main vectors of intrusion used by attackers. As such, 2024 was marked by mass campaigns of vulnerability exploitation, impacting systems' edge security devices.

The legal framework has also evolved with the promulgation of the French 2024-2030 military programming law which, amongst other things, requires that vendors report to ANSSI any significant vulnerabilities detected in their software.

1 SECURITY AND EDGE DEVICES: PRIME TARGETS

As with the previous year [01], in 2024 ANSSI has also observed the amplified exploitation of vulnerabilities affecting devices exposed on the Internet – including security devices implemented by countless entities as a means to secure remote access to the IS (e.g. firewalls or VPN gateways). Over the past year, ANSSI was notified of the compromise of thousands of edge devices across France and processed dozens of security incidents linked to the exploitation of software vulnerabilities on these devices, which represent prime targets for attackers.

ANSSI notes that a myriad of actors is conducting scans on networks, in search of potential vulnerabilities to exploit on edge devices exposed to the Internet. These scans are conducted regularly and extensively, and allow prospective attackers to systematically identify exposed devices which have not been updated and may therefore allow the opportunistic exploitation of vulnerabilities. In order to prevent such exploitation, the necessary patches should be applied as early as possible.

Given the increasingly rapid development of proofs-of-concept and of public exploit codes, vulnerabilities found in edge security devices are

indeed often exploited shortly after their publication⁸. However, ANSSI notes that these vulnerabilities are still being exploited by attackers even months after patches have been made available.

By way of example, in 2024 ANSSI processed the compromise and encryption by ransomware of a telecommunications entity. An edge device – a Palo Alto firewall vulnerable to CVE-2024-3400 (see the following focus) – was the target of multiple malicious login attempts over the course of a several months. Once the device had been successfully compromised, attackers used the access to lateralise themselves across the IS. This incident affected the victim's operations for several months and required significant reconstruction efforts. It should be noted that in this case, the vulnerability was exploited over two months after the publication of a patch by the vendor and of an alert by the CERT-FR.

ANSSI has also processed several cases of compromise resulting from the exploitation of 0-day vulnerabilities – such, for instance, as the CE-2024-47575 vulnerability affecting Fortinet FortiManager devices.

When an exploitation code is published before the security patch for the corresponding vulnerability has been applied to the IS, or in the case of a 0-day vulnerability, it is crucial to conduct investigations on the vulnerable equipment to ensure that the vulnerability has not been exploited. In 2024, for example, ANSSI conducted a campaign alerting its beneficiaries to a vulnerability affecting Fortinet FortiEMS products (CVE-2023-48788). The swift response of a beneficiary in possession of a vulnerable device made it possible to discover the compromise and to prevent the attacker's lateralisation. This type of scenario is frequent, and emphasises the importance of conducting investigations when a vulnerable device has been exposed to the Internet.

8

The detailed description of the exploitation of vulnerability CVE-2024-22024, affecting several Ivanti security products, was published just two days after the publication of the vendor's vulnerability notice.

This was also the case for the CVE-2024-24919 and CVE-2024-3400 vulnerabilities, which respectively impacted several CheckPoint and Palo Alto products and whose method of exploitation was published four days after the vendor's notice.



Incidents resulting from the exploitation of vulnerabilities on security and edge devices.

The most frequently exploited vulnerabilities in the compromise cases responded to by ANSSI are listed in the table below, in descending order. It is particularly notable that the nine most exploited vulnerabilities in 2024 have affected security edge devices. ANSSI published feedback on these campaigns – which primarily targeted firewall, VPN gateway, or filtering gateway solutions in June of 2024 [11], – containing prevention and hardening measures. This feedback illustrates why it is crucial for organisations to control their devices – whether they be deployed for their own use, for clients, or on their account by providers or subcontractors. The responsibility for supervision and for the maintenance in security conditions of the devices must be clearly established and known by all.

This trend may result from a number of these devices’ characteristics, which make them ideal targets for attackers:

- an attack surface broadened by the gradual accumulation of features, some of which rely on outdated software;
- the generally simple, reliable and repeatable exploitation of vulnerabilities;
- the possibility of the IS’s in-depth compromise, given its privilege and adherence to other software components (such as the Active Directory);
- a level of exposure which allows for the identification of potential vulnerabilities via scans.

This phenomenon is also exacerbated by the trust placed in these devices – which may lead users to ease up on the implementation of usual good practices – and by the too-frequent exposure of administration interfaces on the Internet. It must therefore be reiterated that these devices are not necessarily secure by default and that, given the opportunities they represent for attackers, particular attention should be paid to their administration and supervision. Furthermore, some security devices do not natively provide adequate response, supervision, and audit capabilities. ④

CYBER THREAT OVERVIEW 2024 ANSSI

CVE	SCORE CVSS3.x	ÉDITEUR	RISQUE	RÉFÉRENCE CERT-FR
CVE-2024-21887	9.1	IVANTI	Remote execution of arbitrary code, security policy and authentication bypass, access to restricted resources on different security and VPN gateways	CERTFR-2024-ALE-001 CERTFR-2024-AVI-0109 CERTFR-2024-AVI-0085
CVE-2023-46805	8.2			
CVE-2024-21893	8.2			
CVE-2024-3400	10.0	PALO ALTO NETWORKS	Remote execution of arbitrary code on different security devices	CERTFR-2024-ALE-006 CERTFR-2024-AVI-0307
CVE-2022-42475	9.8	FORTINET	Remote execution of arbitrary code on different SSL VPN gateways	CERTFR-2022-ALE-012 CERTFR-2022-AVI-1090
CVE-2024-8963	9.4	IVANTI	Remote execution of arbitrary code and security policy bypass on different security and VPN gateways	CERTFR-2024-ALE-013 CERTFR-2024-AVI-0796 CERTFR-2024-AVI-0917
CVE-2024-8190	7.2			
CVE-2024-47575	9.8	FORTINET	Remote execution of arbitrary code on different security devices	CERTFR-2024-ALE-014 CERTFR-2024-AVI-0917
CVE-2024-21762	9.8	FORTINET	Remote execution of arbitrary code on different security devices	CERTFR-2024-ALE-004 CERTFR-2024-AVI-0108
CVE-2021-44228	10.0	APACHE	Remote execution of arbitrary code	CERTFR-2021-ALE-022
CVE-2024-24919	8.6	CHECK POINT	Breach of data confidentiality	CERTFR-2024-ALE-008 CERTFR-2024-AVI-0449

Disclaimer:

this ranking only takes into account the events for which ANSSI or a digital investigation provider has confirmed (with a high degree of certainty) the exploitation of a vulnerability. Vulnerabilities belonging to the same chain of exploitation appear grouped.

2 ACTORS RESPONSIBLE FOR THE EXPLOITATION OF VULNERABILITIES ON EDGE SECURITY DEVICES

Vulnerabilities affecting edge security devices are exploited by a wide range of actors. State-backed actors with significant research or purchasing means at their disposal typically exploit these vulnerabilities in a targeted manner. These past few years, however, ANSSI has observed the proliferation of large-scale espionage operations hinging on the mass exploitation of vulnerabilities found in edge devices. Depending on the victim, exploitations are generally followed by selective post-exploitation phases. More advanced cybercriminal actors also have the means to purchase vulnerabilities and conduct exploitation campaigns for extortion purposes. Ultimately, once the exploit codes have been made public, the vulnerabilities can be broadly and opportunistically exploited by – primarily cybercriminal – actors.

Vulnerabilities may first be selectively exploited by a state-backed actor (as a 0-day vulnerability for example), then more massively by the same actor once the exploitation has been detected, and later by the entire ecosystem once the vulnerability and an exploit code have been made public.


3 REGULATORY CHANGES AND COORDINATION IN THE TREATMENT OF PRODUCT VULNERABILITIES

Several regulatory changes have been set in motion with the aim of improving vulnerability treatment and the security of products. In October of 2024, the European Union adopted the Cyber Resilience Act⁹ (CRA) with the aim of defining base cybersecurity requirements for all products with digital components, including software. These requirements include security by design obligations, the implementation by default of secure configurations, the automated management of updates, and the

Exploitation of vulnerabilities in Ivanti CSA devices

In 2024, ANSSI observed an attacker employing similar tactics, techniques and procedures (TTP) to UNC5174 to exploit vulnerabilities in Ivanti's Cloud Service Appliance (CSA) product. The repeated exploitation of the vulnerabilities CVE-2024-8963, CVE-2024-9380, and CVE-2024-8190 allowed the attacker to remotely execute arbitrary code on Ivanti CSA devices. The 0-day vulnerability CVE-2024-8190 was exploited several days prior to the publication of the Ivanti security advisory.

The investigations conducted by ANSSI on the ISs of multiple victims revealed the use – for the initial compromise – of a common intrusion set. Moderately sophisticated and discreet, this intrusion set is characterised by the use of intrusion tools largely available as open source and by the – already publicly reported – use of a rootkit¹⁰ code [12].

Post-exploitation activities do nevertheless differ from one incident to the next, which supports the hypothesis of an intrusion set being used as a means to secure initial access points, to then be sold off or entrusted to other operators. 

9

Regulation (EU) 2024/2847 of the European Parliament and Council, dated October 23 2024, on horizontal cybersecurity requirement for products with digital elements.

10

Malicious programs which make it possible to retain illegitimate high-privilege access on a system, and which can be used to conceal the presence of other malware on this same system.

obligation for all vendors distributing their products in the EU to report vulnerabilities to the relevant national CSIRTs [13].

France also implements a legal framework on the national level, allowing for the protection by ANSSI of the reporter of a vulnerability and enforcing obligations to report vulnerabilities to ANSSI for vendors distributing their products in France. These provisions share some grounds with the CRA, and will thus be reinforced by its entry into force in 2026.

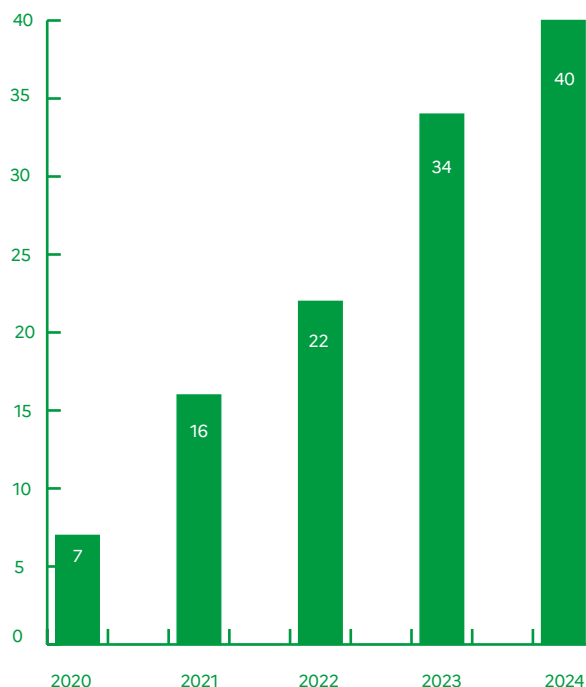
Operated by ANSSI, the CERT-FR is responsible for the coordinated treatment of vulnerabilities, together with the concerned stakeholders (reporter of the vulnerability, vendor of the vulnerable product), until they have been fully addressed. The CERT-FR is increasingly engaged in coordinated vulnerability treatment and has processed 40 coordination cases in 2024.

Vulnerabilities requiring coordination efforts may be discovered by ANSSI in the context of its activities, reported by its institutional partners, or directly notified to the CERT-FR.

Vulnerability reporters are protected by article L. 2321-4 of the Defence Code (DC) [14] when they are acting in good faith and reporting their discovery to ANSSI only. In 2024, the CERT-FR received a total of 236 vulnerability notifications. These notifications are anonymised by the CERT-FR and sent to either the owner of the affected service (in cases where the vulnerability is affecting services such, for instance, as a website) or to the vendor, when the vulnerability impacts a product. Whatever the case, the identity of the reporter and the circumstances of their discovery will be protected. For product vulnerabilities, the CERT-FR may offer its vulnerability coordination services.

In 2024, these legal provisions were reinforced with the introduction, in article L2321-4-1 CD [15]

Number of vulnerability coordination cases processed by the CERT-FR



of a new obligation which requires vendors supplying their products in France to notify ANSSI of any significant vulnerabilities and incidents affecting the security of their products¹¹. Should its obligations not be fulfilled by a vendor, ANSSI has several means of action at its disposal: issuing to the vendor an injunction to notify affected users before a set date after which the written injunction may be published if the vendor remained uncompliant, or directly notifying the vulnerability to affected users, or publishing the vulnerability. ←

11

To report a vulnerability or an incident:
ClubSSI – Faire une déclaration au CERT-FR
<https://club.ssi.gouv.fr/#/declarations>



II

MEANS EMPLOYED BY ATTACKERS

From malicious codes and anonymisation networks to the exploitation of vulnerabilities, attackers have various means and tools at their disposal which allow them to take advantage of these nume-

rous opportunities. The offensive arsenal of attackers may also be strengthened by the acquisition of tools designed and developed by private offensive cyberwarfare companies.


A TARGETING OF THE SUPPLY CHAIN

→ An information system's supply chain may take different forms (devices, software, service providers), and each of these forms may provide attackers with various opportunities. Attacks on the supply chain enable the indirect compromise of customer organisations using a common provider, software, or device. These attacks are diverse and stealthy; as such, they are particularly effective and may be the object of an investment which may result in significant benefits for attackers. ←

Software supply-chain attacks

This type of attack consists in maliciously modifying software with the intention of reaching all of its users. Several cases with significant repercussions have transpired over the past few years – such, for instance, as the compromise of MeDoc by the NoPetya attack in 2017, of Solardwind's Oriel software in 2020, and of the 3CX Desktop App in 2023, which occurred in the wake of the X_TRADER financial software's own compromise.

Most software supply-chain attacks are conducted via the compromise of a software vendor's IS. However, such an attack may also be carried out through the use of malicious code on an open-source project. The attack conducted in 2024 against the XZ Utils project, used in many Linux distributions, is a prominent example of this¹². The attack took place over the course of three years, allowing the perpetrator to acquire the position of co-maintainer of the project and, subsequently, to introduce malicious changes. This particular case highlights the complexity of securing the software supply chain.

In January of 2024, ANSSI was also notified of a data leak impacting the AnyDesk Software vendor, specialised in the development of remote desktop software solutions. Certificates, private keys, and the source codes of the vendor's applications may have been stolen, and two relay servers located in Europe were reportedly also impacted by the incident. Though there was no evidence to suggest that AnyDesk's softwares had been altered, this attack could have had significant repercussions given the type and wide distribution of the concerned software [16] 

12

The maliciously modified version of XZ Utils makes it possible to alter the behaviour of OpenSSH, and under certain conditions may offer the possibility of remotely executing code.

Supply-chain attacks via IT service providers

A supply-chain attack may also consist in compromising, this time via the service providers, the resources of a service provider who has access to the IS of the final target. In such cases, once the provider has been compromised, the attacker may use the privileges and resources of the provider on the final target's IS. The attacker will thus have taken advantage of the provider's lower security levels to reach its final target, discreetly and by means that are often difficult to detect.

In 2024, ANSSI responded to several compromises of important entities achieved by such means.

For example, a foreign IT subcontractor working alongside several major French companies was compromised in depth, allowing attackers to penetrate the companies' information systems. Through legitimate – and therefore difficult to detect – access, attackers were able to consult and exfiltrate data of interest.

That same year, ANSSI also responded to the attempted compromise, via the supply chain, of a leading French industrial. The attack came about following the initial compromise of business resources supplied by providers. Though no lateralisation was detected on the company's IS, ANSSI notes some recurrence in the methods used by attackers to reach strategic French entities. Indeed, in 2015 this same entity had suffered a similar incident after attackers had broken into the ISs of recently-acquired subsidiaries. These cases shed light on the active exploitation by some malicious actors of bonds of trust and potential network interconnections between final targets and their environment (providers, subsidiaries, etc.), as a means to reach their objectives.

Cybercriminal groups also take advantage of some service providers' lack of maturity in matters of cybersecurity. In 2024, several French entities were compromised through an IT provider and subsequently suffered data leaks [17]. Furthermore, in October of 2024, an affiliate the Qilin Ransomware as a Service (RaaS) compromised a managed service provider (MSP), leading to the encryption or exfiltration of data belonging to over thirty of the provider's clients. The attacker reportedly took advantage of the deployment of remote access solution by the provider to access and encrypt its clients' workstations. At least one of the clients suffered a case of lateralisation whereby the attacker was able to introduce malicious tools on its IS and exfiltrate sensitive data.

These cases (attempted compromises and incidents) are illustrative of a major trend observed by ANSSI: the growing experience and maturity of certain organisations encourage attackers to target digital service providers, to more discreetly reach their final target. 𐄂



B THE EVOLUTION OF ATTACK TOOLS AND INFRASTRUCTURE

1 ANONYMISATION NETWORKS AND INFRASTRUCTURE

The past few years have been marked by the development and use of anonymisation networks.

While they are primarily used by actors reputedly linked to China, state actors linked to Russia (including intrusion sets such as APT28 or Nobelium) have also been known to use networks of compromised devices for anonymisation purposes. These networks can be made up of compromised routers, of proxies, or of commercial VPN. Groups of attackers which are reputedly Russian remain actively involved in the targeting of e-mail accounts, and towards that end have developed new phishing techniques and attack infrastructure, with a reliance on brute force or password spraying. From the reconnaissance stage – which hinges on commercial VPNs or proxy services – to the use of free hosting services as a means of exposing phishing pages, the operators of such intrusion sets benefit from low-cost and ready-to-use managed infrastructure. These services offer great flexibility in the creation and administration of new resources, and are also used for legitimate purposes by individuals and companies. It can therefore be difficult to distinguish legitimate uses from illegitimate ones, which makes their detection and monitoring by security teams more complex. Cybercriminal groups also use such anonymisation infrastructure.

The extent of the use of anonymisation networks by attackers reputedly linked to China makes the study of these networks particularly necessary.

2 ATTACKS WITH CAPABILITY OBJECTIVES

In 2023 and 2024, attackers associated with strategic state interests achieved the compromise of companies from the digital and cybersecurity sector, specifically by means of the reputed Russian intrusion set Nobelium. The likely objective of these

initial attacks was to acquire access or information which might enable subsequent attacks – by, for instance, searching for vulnerabilities, reusing credentials, or even preparing an attack on the software supply chain. Nonetheless, it appears that in some cases operators also inquired into the state of knowledge pertaining to them.

Active since at least October of 2020 and reputedly linked to the Russian Foreign Intelligence Service (SVR) [21], the Nobelium intrusion set is connected to cyberattack campaigns conducted by means of spear phishing, with the intention of gathering strategic intelligence. The victims typically associated to these campaigns belong to governmental sectors, including the diplomatic ones, in France and Europe more broadly, in Africa, in North America, and in Asia. Between 2021 and 2023, this intrusion set was repeatedly used against French diplomatic entities.

According to the American company Microsoft (Microsoft, 2024), some of the attacks linked to Nobelium targeted entities of the digital sector from across the globe, including some from North American and Western Europe. In November of 2023, Microsoft reported a security incident during which Nobelium operators exfiltrated e-mails belonging to its legal and cybersecurity teams, as well as to members of its executive committee. As a cybersecurity vendor, Microsoft majorly contributes to the open-source knowledge on the Nobelium intrusion set and on the means of preventing attacks associated to it. According to Microsoft, during their attack on the company, Nobelium operators sought information on the intrusion set itself [22]. It may therefore be inferred that attackers intended to conduct a counter-espionage operation, likely in order to reinforce their operational security.

The use of anonymisation networks by attackers reputedly linked to China

Since 2022, the use of anonymisation networks by reputedly Chinese intrusion sets was observed by ANSSI during four cyber-defence operations.

Security vendors have also documented some of these networks, such, for instance, as ORBWEAVER, SPACEHOP [18] or KV Botnet [19].

The particularity of such anonymisation networks lays in the large number of devices involved, and in the industrialisation of their infection. Made up of several hundred – sometimes thousand – compromised or rented devices, these networks raise the cost of defence against cyberattacks through the evolution of attacking infrastructure and TTPs. The use of legitimate network devices in such infrastructure also complexifies detection and blocking, as it can be difficult to identify malicious traffic.

These anonymisation networks give rise to new paradigms in the field of threat management. They urge the re-evaluation of the idea that attackers control all attack infrastructure: indeed, in the case of reputed Chinese anonymisation networks, the infrastructure is generally administered by independent entities, providers, or administrators located in the People's Republic of China (PRC). They are not controlled by a single group of attackers, and seem to be shared between distinct groups. This re-evaluation must be apprehended in conjunction with the sharing of codes, infrastructure, and providers (institutionally, commercially, or informally) between different reputedly Chinese intrusion sets – which also significantly complexifies the imputation of a specific intrusion set.

Attack campaigns by intrusion set known as Volt Typhoon – used for prepositioning purposes in anticipation of forthcoming destabilisation efforts, and attributed to China by the Five Eyes¹³ – are also characterised by their discretion. Beyond the simple use of the KV Botnet anonymisation network, the application of particularly discreet TTPs – including the use of “Living off the Land” techniques¹⁴ – and the implementation of operational security precautions are all indicative of a continued effort for discretion. As an example, the operators of the intrusion set avoided using login details outside of what are considered to be “standard” working hours for their victims, to avoid generating security alerts [20]. ㊦

13

The term refers to the alliance between the intelligence services of the United States, Australia, New Zealand, the United Kingdom, and Canada.

14

In which an attacker makes use of the tools already present on the targeted information system. In such cases, detection and digital investigation can only revolve around the search of tools which are specific to the attacker.

In January of 2024, the American company Hewlett Packard Enterprise reported an attack allegedly linked to Nobelium on its cloud-based e-mail environment. Though the attackers' motivations remain unknown, they may have sought to obtain information pertaining to these products [23].

Lastly, according to a joint report published in December of 2023 by the Polish, British, and American authorities [24], Nobelium operators conducted a large-scale campaign of exploitation of the vulnerability CVE-2023-42793 affecting the host servers of the JetBrains software, developed by TeamCity. Given that this product is broadly used by software developers, this campaign could have enabled a subsequent software supply-chain attack.

3 THE USE OF COMMON RESOURCES OR CAPABILITIES BY STATE ACTORS AND CYBERCRIMINAL ACTORS

In 2024, ANSSI continued to observe an increasing porosity between the different profiles of attackers. The search for low-cost stealth and effectiveness encourages malicious actors to favour open-source commercial tools or "Living off the Land" techniques (LotL). For instance, reputedly Chinese intrusion sets notably use legitimate SOCKS5 proxy tools and the SoftEther VPN.

Malicious codes and services of cybercriminal origin are also being used by reputed state intrusion sets. The Remcos and DarkCrystal Remote Access Trojan (RAT) are or were deployed by both cybercriminal groups and actors reputedly linked to Russia [25] [26] [27]. Operators of the reputed Russian UNC5812 intrusion set also reportedly used the CraxsRAT Android malicious code of cybercriminal origin to target Ukrainian military entities, in the context of Russia's invasion of Ukraine [28].

Several state-backed actors also allegedly use ransomware, either to render sensitive data unavailable [29], or as a coverup to conceal more targeted espionage operations. Since 2021, the vendors SentinelOne and Recorded Future reportedly observed several campaigns of espionage conducted by the reputed Chinese ChamelGang group and involving the deployment of the CatB ransomware [30]. Twice in 2024, ANSSI observed the use of intrusion tools such as PlugX or Shadowpad – generally associated with reputedly Chinese intrusion sets – in attacks which resulted in the encryption of the victim's IS. Lastly, cybercriminal groups have grown increasingly professionalised; they are now able to employ sophisticated attack techniques and to exploit 0-day vulnerabilities [31] [29].

Some attackers may also target and subsequently compromise the offensive capabilities of other malicious actors, perhaps as a way to conceal their own activities. Operators of the Turla intrusion set, publicly attributed to the Russian FSB, thus exploited the tools and infrastructure of at least six different intrusion sets in their attacks [32].

This porosity in the activities of different malicious actors is further amplified by groups whose actions toe the line between different fields. This year, the group responsible for implementing the malicious code RomCom reportedly conducted several campaigns aimed at both strategic espionage and financial gain. These assumptions are based on the study of the group's victimology, which oscillates between the specific targeting of governmental and sensitive entities in Ukraine or other NATO countries, and the more opportunistic targeting of private entities from various sectors [33]. ←

C MERCENARIES AND SERVICE PROVIDERS

1 FROM PROFITABLE BUSINESS TO ECOSYSTEM IN SERVICE OF A STATE

While the offensive cyberwarfare sector continues to grow, ANSSI notes the simultaneous development of a private ecosystem within states such as China. As a result of the democratisation and increasing variety of the means of attack, new actors are also emerging.

The wide variety of means is evidenced by ADINT¹⁵, through which advertising market flaws are exploited. In order to recover the identifying features¹⁶ which define the relationship between supply and demand on the advertising market and which enable the association of a device to its user, ADINT companies either internalise the capabilities of advertisers or collaborate with them. In doing so, they are able to legally collect data on a large number of individuals, and to use said data during surveillance or espionage operations [34] [35] [36]. Given that these geo-surveillance tools do not involve the compromise of the targeted device, they are furthermore not considered to be dual-use goods¹⁷. As such, it is significantly easier to commercialise ADINT services than conventional spyware. In addition to its geographical surveillance purposes, recent publications have brought to light a new type of ADINT-based technology capable of compromising mobile devices and computers via the combined circulation of advertisements and exploitation of vulnerabilities. A targeted mobile phone could be compromised by simply displaying advertisements¹⁸ [37].

Today, the private ecosystem is diverse and brings together a wide variety of actors ranging from private companies and providers working for a given state, to mercenaries and hackers for hire. Though these activities were brought to the public's attention through spyware and attacks on mobile devices, they may cover a much wider variety of services – including the provision of services

(see focus page 28) and the supply of means of attack. The leak of data impacting the Chinese company I-SOON gives an idea of the type of organisation that such actors may have on hand (see focus page 27).

2 THE TARGETING OF MOBILE DEVICES

By virtue of their ubiquity and systematic use, mobile devices are particularly valuable when it comes to the acquisition of intelligence of cyber origin. The spyware supplied by offensive cyberwarfare companies represents a major threat to their users. Officially designed to counter organised crime and terrorism, these tools are used by certain states or intelligence services to keep political opponents, journalists, and NGOs under surveillance. The use of such software is however not limited to internal surveillance; some reported spyware cases have also involved political figures and governments. In late 2023, the mobile phones of two – French and Bulgarian – deputies of the European Parliament's Subcommittee on Security and Defence were compromised. This incident indicates that such tools are indeed being employed for the purpose of strategic espionage [44].

Trade in sophisticated surveillance tools primarily benefits states. On the one hand, these tools allow states which do not themselves possess such tools – or the technical capabilities necessary to develop them – to implement targeted surveillance measures. On the other hand, they allow states with more significant means to further complexify the imputation process by making it easier to conceal their attacks [45]. This anonymity is further reinforced by the sophistication of infection chains, the lapse of time between the compromise and the identification of the attack, and the lack of persistence on the targeted devices – all of which significantly hinder forensic analyses, as well as the detection of this type of tool and its uses.

¹⁵
A contraction of "advertising" and "intelligence" – may be defined as the specific or mass distribution of advertising content towards targets, for profiling or geolocation purposes.

¹⁶
Such as habits, interests, or equipment used.

¹⁷
Dual-use goods are sensitive goods often destined for civilian use, but which may also be employed for military purposes. As such, their exportation requires authorisation.

¹⁸
Products like Sherlock, Patternz, or Alladin, respectively developed by INSANET, ISA SECURITY, and INTELLEXA, possess such capabilities [84].

Consequently, particular attention must be paid to the notifications issued by vendors, whether they be produced by the phone manufacturer¹⁹ or by the vendor of an application (an e-mail application, for example).

Implementing a strict separation between professional and personal uses, or employing specific means for some of these uses, remains the best way to reduce one's exposure to these threats. Regularly rebooting devices may also limit the potential impact of a non-persistent compromise by forcing the attacker to re-infect them.

Lastly, the activation of the exploitation system's hardening mechanisms²⁰ should be prioritised, particularly for high-risk populations.

3 A CONSTANTLY-EVOLVING MARKET FACED WITH TECHNICAL LIMITATIONS AND MEDIA EXPOSURE

The targeting of mobile devices requires high levels of sophistication, marked by the use of stealthy infection techniques ("0-click" attack chains which do not require the target's input) and by the exploitation of 0-day vulnerabilities. These infection chains, however, are constrained by various factors: the development time of such vulnerabilities, their life span, and the counter-measures implemented by governments and manufacturers against this spyware. In February of 2024, the United Kingdom and France initiated the Pall Mall process – a discussion on the fight against proliferation and the irresponsible use of commercial cyber intrusion tools. This initiative brings together a coalition of states, companies, and representatives of civilian society. It has resulted in a multipartite declaration, and is working towards the elaboration of a code of good practices for the use of such tools [46]

Simultaneously, publications pertaining to these companies and their activities continue to be issued. Several security vendors and international organisations have developed capabilities enabling them to monitor the infrastructure of this spyware, which they expose publicly to diminish their capabilities. These reports compel offensive cyberwarfare companies to further develop their infrastructure, as Cytrox did following the publication by the vendor Sekoia of a document pertaining to the Predator spyware [47]. The Spanish company Variston reportedly suffered a significant loss of business and personnel following Google's exposition of the infection chain, which led to the deployment of its spyware [48] [49].

2024 was also marked by the growing number of legal proceedings initiated by spyware victims. The 2019 trial between NSO Group and Meta highlighted the desire of manufacturers to protect themselves from offensive cyberwarfare companies. Complaints have also been filed by civilians: the Catalan lawyer Andreu Van den Eynde Adroer, whose smartphone was infected by Pegasus in May of 2020, filed a complaint against NSO group and specifically targeted both its founders and its director [50].

The private cyberwarfare sector remains active nonetheless, and its companies are quick to adapt and reorganise themselves. They resort to using front companies or intermediaries which are not constrained by regulations on the employment of dual-use goods and are thus able to implant themselves in countries with more favourable legislation – such, for instance, as Indonesia and the United Arab Emirates [51]. ←

¹⁹
For example, Apple sends notifications out using the following address: threat-notifications@apple.com

²⁰
The Lockdown Mode of iOS environments servers is an example [82]

The disclosure of I-SOON's company data, a deep dive into the Chinese offensive ecosystem

On the 16th of February 2024, an unknown actor going by the username @iSOON on X (formerly Twitter) published data belonging to the Chinese company Sichuan I-SOON (or I-SOON) Information Technology Co., Ltd. on the project-hosting and software-development management platform GitHub. Though these documents appear to be authentic, at this stage it is impossible for ANSSI to confirm or deny their origin. According to open-source information, the company is a provider of the Ministry of Public Security (MPS), of the Chinese Ministry of State Security (MSS), and of the People's Liberation Army (PLA). On its website and on its registered patents, the company claims to provide surveillance software designed to collect sensitive information. It's CEO, Wu Haibo (also known as shutd0wn), belonged to the Honker Union hacktivist group, founded in 1999 as part of the first generation of Chinese "patriotic attackers".

I-SOON is fully integrated as an actor of the Chinese offensive cyberwarfare ecosystem. The documents and conversations disclosed revealed code, infrastructure, and contractual links between the company and several reputedly Chinese intrusion sets. The targeting intentions of these intrusion sets are in line with Chinese state interests, particularly with regards to espionage and the fight against the "Five Poisons"²¹. This data leak highlights the links forged by the provision of services with different governmental entities – whether they be the PLA, the MSS, or the MPS – and by the sharing of offensive tools between a multiplicity of actors, all apparent in the purchase contracts and service agreements leaked. This contractual arrangement further complexifies the attribution of attack campaigns to their instigators.

This divulgation also sheds light on the current degree of competition between Chinese offensive cyberwarfare companies, and on the difficulties they must face when attempting to stand out, on a national scale, amongst all major actors of the sector. According to excerpts of disclosed internal conversations, I-SOON must ally itself with larger companies in order to win public tenders. This results in more opportunistic and autonomous offensive activity, in line with Chinese state interests, with the aim of a posteriori selling these accesses and thus winning contracts. In this way, the disclosure of I-SOON's data reveals an approach that has thus far been poorly documented publicly: victims are no longer exclusively being targeted on the basis of a state contract, but rather in view of a future contract and remuneration by one or several potentially interested governmental actors. The items leaked as a result of I-SOON's extensive targeting of at least 45 countries – including France – may be interpreted through this new threat analysis framework. At present, the operations conducted by reputedly Chinese intrusion sets and observed by ANSSI remain consistent with this analysis. ANSSI expects this capacity for proliferation to grow alongside with the maturity of the Chinese cyber ecosystem – an ecosystem which tends to penetrate the public, private, and university spheres, in an effort to contribute to "national security" through both defensive and offensive cyberwarfare. ㊦

21

Taiwan independence activists, Uyghurs, Tibetans, Falun Gong, and supporters of democracy are the « Five Poisons » which the Chinese Communist Party (CCP) considers to be a threat to the stability of its regime.

The government classes them as priority targets and, as such, they recurrently appear in the victimology of reputed Chinese intrusion sets.

Bullet Proof Hosters

Previously mentioned in the *2021 Cyber Threat Overview*, Bullet Proof Hosters (BPH) play a central role in the cybercriminal ecosystem. Commonly located in countries beyond the bounds of mutual legal assistance agreements, these hosts base their economic model on the de facto immunity they grant their clients: inertia or inaction in the face of judiciary injunctions, accepting payments in cryptocurrency, little to no verification of clients' identities, no supervision of hosted activities, etc.

An analysis of the incidents reported to ANSSI in 2024 reveals that the infrastructure provided by such hosts is used by a wide variety of malicious actors. In addition to cybercriminals, reputedly state-backed hacktivists also employ BPHs. The pro-Russian hacktivist group NoName057 group is, for instance, known for using the infrastructure of Stark Industries [38] and Global Internet Solutions LLC (GIR) [39] hosts. Stark Industries has also appeared in incidents linked to the cybercriminal group FIN7 [40], and in attacks conducted by the reputed Iranian actor Haywire Kitten [41].

Several operators of reputed Chinese anonymisation networks are also known to base part of their anonymisation infrastructure on BPHs [18].

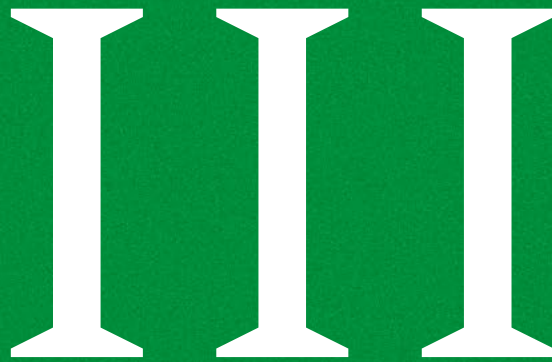
Similarly, the hosting provider GIR is used by the reputed Russian intrusion set Gamaredon [42], as well as by cybercriminals utilising the Emmenhtal loader [43].

Though BPHs regularly advertise their services on specialised forums, promoting the lack of monitoring of clients' activities, ANSSI has since observed several security incidents involving hosts which do not claim to be

BPHs. These hosts are documented in national registries and do not promote the malicious use of their infrastructure. However, a number of indications point to the existence of activities – such as the use of their services in security incidents, a lack of responsiveness when taking devices involved in security incidents offline, cryptocurrency payments, the absence of KYC policies²², and a relative opacity in the legal registration of associated companies – which are comparable to those practiced by BPHs. 𐄂

²²
"Know your customer" (KYC)





ATTACK OBJECTIVES

As with the previous years, attacks aimed at espionage and profit-making remain the most important in terms of involvement for ANSSI's teams. However, 2024 was also marked by an increase in the number of attacks aimed at destabilisation, often conducted by hacktivist groups. ANSSI notes that

ultramarine infrastructure is particularly exposed to such destabilisation or ransomware attacks, by virtue of the poor resilience of Internet access and public services, or because of greater response times for entities located on the mainland – whether they be ANSSI or specialised providers.

A PROFIT-DRIVEN ATTACKS

→ Attacks aimed at profit-making primarily rely on financial extortion, generally achieved through the theft or encryption of data. These two approaches may be combined in what are called “double extortion” attacks. This type of attack is often opportunistic and heavily mediated by attackers, as a means of amplifying the pressure exerted on victims.

1 A PERPETUALLY HIGH LEVEL OF CYBERCRIMINAL ACTIVITY

In 2024, the activity of ransomware groups – which makes up a large share of cybercriminal activity – has remained vigorous. Though profit-driven attacks are conducted by groups indistinctly targeting most sectors and geographical areas, cybercriminal actors tend to focus their efforts on developed countries in the hope of increasing the likelihood of getting a ransom.

In order to amplify the pressure exerted on victims, ransomware operators target the components of an IS which are likely to contain data – such, for instance, as cloud storage servers. Since 2023, ANSSI has also observed the continuous targeting of hypervisors (including VMware’s ESXi devices) which host a myriad of services and data. Groups such as Mallox, RansomHub or Qilin have developed new ransomware variants which specifically target these devices. The ability to encrypt several different types of devices is also used as a selling point by RaaS groups seeking to recruit new affiliates [53].

Whether they take the form of ransomware attacks or data exfiltration, attacks aimed at financial extortion can have significant repercussions on both the victim entity’s business continuity, and on its reputation. The financial losses engendered by these attacks may also be substantial and endanger victims in more precarious financial situations.

Previously mentioned in the feedback on the 2024 Paris Olympic and Paralympic Games, the ransomware attack on Paris-Saclay University had a significant operational impact, notably on the availability of several business applications during the student enrolment period and over the first few months of the academic year. These disruptions also affected the schools, associate-member universities, and research organisations whose infrastructure is shared with the university. Though remediation measures were progressively implemented, this incident emphasised the importance of business continuity plans (BCP) and disaster recovery plans (DRP) in the prioritisation of IS reconstruction efforts.

2 THE DISORGANISATION OF THE CYBERCRIMINAL ECOSYSTEM

The year 2024 was also marked by the disruption of the cybercriminal ecosystem, resulting from dismantlement operations and the successive breakaway of several major groups.

Mid-year, ANSSI observed the growing use of infostealers²³ in infection chains, leading up to the deployment of ransomware. Generally unsophisticated but widely used, these malicious programmes allow attackers to acquire credentials on the victim’s workstation. These credentials are subsequently sold on forums or through private Telegram channels, then reused by other attackers. Much like other actors of the cybercriminal ecosystem, some infostealer operators are focused on service offers and work with initial access brokers²⁴ or directly with ransomware affiliates.

23

An infostealer is a malicious code used to collect information on the victim’s workstation, including credentials stored in web browsers.

24

Cybercriminal actors specialised in obtaining and reselling non-authorised accesses to an information system.

The evolution of ransomware attacks monitored by ANSSI

In 2024, 144 cases of compromise by ransomware were reported to ANSSI. The number of attacks remains consistent with the previous year, and the associated threat maintains a strong presence in France.

Although the number of attacks remains generally comparable to that of the previous years, the ecosystem has reinforced itself in order to face this type of threat. This has allowed ANSSI to focus its efforts on attacks with a more significant impact, or which represent significant political risks.

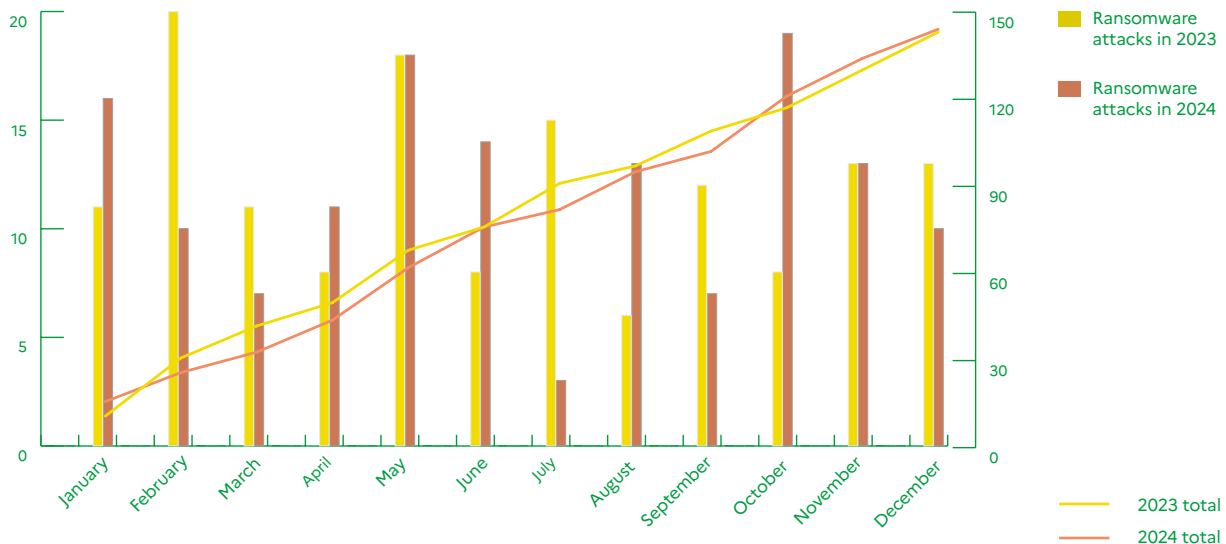
While SME/VSE/mid-caps are the most affected by cases of ransomware compromise, the proportion of local authorities (17%) and health facilities (4%) targeted by such attacks has declined. However, ANSSI notes an

increase in the number of ransomware attacks on higher-education establishments, which made up 12% of the victims of such attacks in 2024 – on par with strategic enterprises.

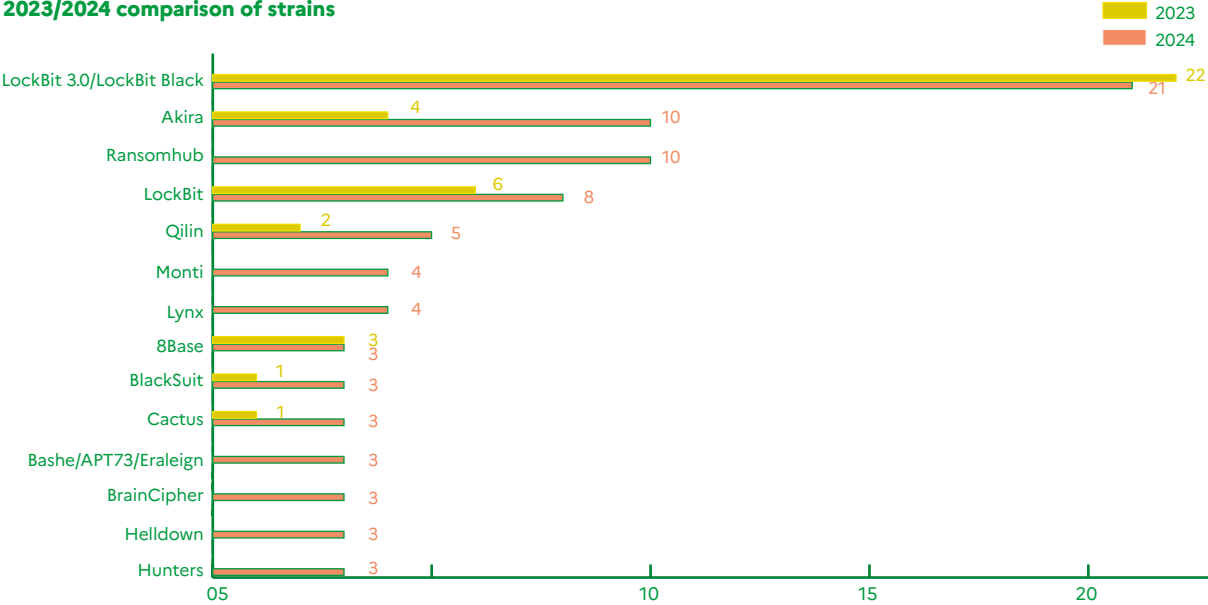
Over the studied period, ANSSI observed 39 different ransomware strains. The most represented strains were Lockbit 3.0 (15%), Ransomhub (7%), and Akira (7%). While Lockbit and Akira had already been responsible for the compromise of numerous French entities in 2023, the Ransomhub, Monti, and Lynx strains had not been observed by ANSSI prior to 2024. The Bashe ransomware strain, previously known as “Eraleign”, had also not been observed since 2021.

The types of strains most used by attackers have evolved over the years. Though Ryuk and Hive were the most used ransomware strains in 2021 and 2022 respectively, in 2023 they were replaced by Lockbit strains. ⚡

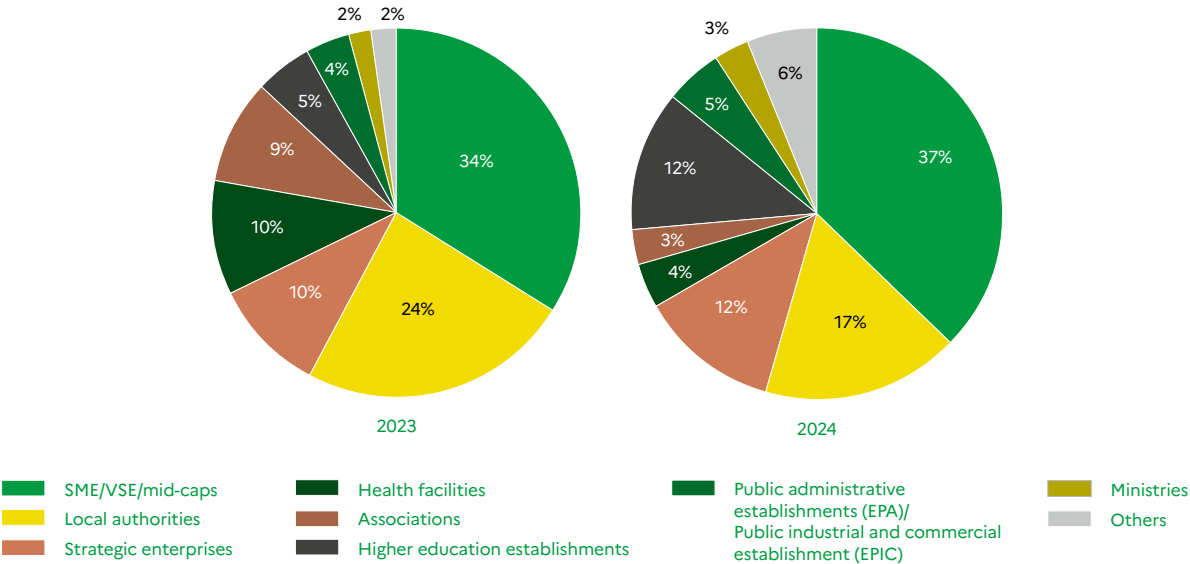
A yearly comparison of the number of ransomware attacks



2023/2024 comparison of strains



Breakdown of spyware victims



NOTE:
this breakdown only comprises the cases of compromise reported to ANSSI and may therefore vary according to the Agency's insight into these attacks.

In 2024, the cybercriminality section of the Paris Prosecutor's Office's national jurisdiction in the fight against organised crime (JUNALCO) observed a decrease in the number of attacks [52].

In February and March of 2024, the partial dismantlement of the LockBit group (see focus) and the BlackCat group's exit scam²⁵ contributed to the temporary disorganisation of the ransomware group ecosystem. With several hundred affiliates, these RaaS groups had been two of the most popular franchises in the ecosystem since 2022. Some of these affiliates turned to other franchises such as RansomHub and Hunters International, for whom ANSSI observed a significant increase in the number of attacks, with close to 200 claims each – several of which occurred in France [54] [55]. Other affiliates dissociated themselves from big RaaS groups by creating or joining smaller private groups. From the second half of 2024, ANSSI consequently observed a rise in the number of attacks by new, unsophisticated groups generally using modified versions of ransomware whose source codes have been publicly shared. Already identified in 2023, this trend was confirmed in 2024 by the multiple dismantlement operations which resulted in the breakaway of major cybercriminal groups and in the reorganisation of the ecosystem. The attacks conducted by these new actors have hitherto been fairly irregular – the activity of the Brain Cipher group, responsible for several attacks conducted in France between June and August of 2024, has for instance dropped drastically. The regular emergence of new ransomware strains based on previously-leaked source codes attests to the significant proliferation potential of these malicious cybercriminal programmes.

3 THE THEFT AND LEAK OF FRENCH ENTITIES' DATA

In 2024, several public and private French entities suffered the leak of their data on forums, Telegram channels, or websites dedicated to the disclosure of data [17].

Social sector entities are by nature required to handle personal data and, consequently, they

were the targets of several attacks at the beginning of the year. Amongst these cases, some of the most notable incidents affected the third-party payment providers Viamedis and Almerys, and also France Travail, and resulted in the exfiltration of large amounts of personal data belonging to French citizens [63]. These incidents have been indicative of a lack of protective measures, from the project design stage, in the means of accessing and processing data. In 2024, the CERT-FR published a feedback report on these incidents [64].

ANSSI notes that these data leaks – whether they be confirmed or not – are sometimes claimed and published several months after the incident and by multiple cybercriminal actors or hacktivists. ANSSI has also observed the excessive mediation, particularly during the 2024 Olympic and Paralympic Games, of false data theft claims by malicious actors. These claims generally contain old, previously-published data or very small amounts of information. In such cases, victim entities and security professionals must dedicate a significant amount of time to doubt removals. These claims may also impact the reputation of victims. In June and August of 2024, for example, over 15 reports were made to ANSSI concerning false publications made on several different Telegram channels posing as the LockBit ransomware group ←

²⁵

In an exit scam, an enterprise or cybercriminal group may stop providing its services and disappear with its clients or affiliates' funds.

Dismantlement operations

The international dismantlement operations conducted by law enforcement forces have targeted essential links in the cybercriminal ecosystem.

Several anti-cybercriminality operations have thus been conducted against forums dedicated to the reselling of data and accesses. In May of 2024, the German Dusseldorf police force seized the german-speaking cybercriminal forum CrimeMarket, which counted about 200,000 users [56]. As a response, cybercriminals have been reclaiming or creating new forums and capitalising on the reputation, user base, graphic identity, and content categories of previous forums. Such was the case with RaidForums, which was seized in 2022 then reclaimed and renamed BreachForums. The regular arrests of forum administrators such as those which occurred in March of 2023 [57] and May of 2024 have, to this day, only had a temporary impact on the existence of these communities.

Beyond cybercriminal platforms, several dismantlement operations have also been carried out in 2024 with the aim of destabilising groups of attackers and the cybercriminal ecosystem as a whole. In February of 2024, operation CRONOS – conducted by an international coalition of anti-cybercriminality agencies, including the French national Gendarmerie's *Unité Nationale Cyber* (UN Cyber) – resulted in the significant disruption of the LockBit RaaS group's activities [58]. In operation since 2019, this group has become the most active and attractive group in the ecosystem: in 2023, it was responsible for around 30% of all ransomware attacks [58] [59].

Between the 27th and the 29th of May 2024, a dismantlement operation targeting infrastructure linked to loaders²⁶ such as IcedID and Smokeloader was conducted in the

context of international judiciary cooperation between German, Dutch, Danish, French (coordinated by the judicial police's anti-cybercriminality office (OFAC)), British, and American authorities. Named ENDGAME, this operation was a follow-up to a previous dismantlement operation launched by the United States in August of 2023 against the Qakbot botnet. During this operation, ANSSI provided its support in the identification and notification of victims. The targeted malicious codes were primarily used as entry points on the victim's network, to later deploy – amongst other things – offensive generic tools such as Cobalt Strike and ransomware [60] [61]. ANSSI has not observed any significant resurgence of the loaders targeted by this dismantlement, with the exception of Bumblebee, whose activity remains very limited.

Though the effects of these operations are limited in terms of duration, they are nonetheless effective in disrupting the organisation of cybercriminal actors, who must reinvest time and money into the reconstruction of their infrastructure. Furthermore, the arrests of cybercriminals – such as those which occurred during operation CRONOS – may undermine the reputation of the concerned groups, which will subsequently need to rebuild their reputation and reclaim their status in the ecosystem [62]. ²⁶

26

A loader is a malicious code whose primary function is to place or execute another malicious code on the compromised device.



B DESTABILISATION

→ Destabilisation attempts targeting French entities were particularly numerous this year. Significantly influenced by current international events, these attacks are primarily conducted by hacktivist groups seeking attention. Large-scale political and sports events provide attackers with a significant platform, thus contributing to their destabilisation efforts.

Hacktivist groups traditionally favour DDoS attacks, website defacements, or data exfiltration claims. More recently, the attempted sabotage of small industrial facilities was observed. Though the consequences of such attacks are generally limited, they nevertheless signify the emergence of a logic of sabotage which calls for vigilance.

1 THE SABOTAGE OF SMALL INDUSTRIAL FACILITIES

In 2024, several hacktivist groups claimed to have taken over small industrial facilities primarily involved in the production of renewable energy. These attacks targeted facilities which belonged to either individuals or VSEs/SMEs, and whose management interfaces were exposed on the Internet with no authentication requirements or with default passwords.

These technically unsophisticated attacks are primarily used for mediatisation purposes. Indeed, ANSSI has observed a disparity between the attackers' claims and the consequences of their attacks: in the majority of cases, hacktivists overstate the impact of their efforts in an attempt to increase their visibility.

ANSSI reiterates that the measures implemented to secure industrial equipment and reduce their exposure to the Internet significantly minimise opportunities for attack. Manufacturers and distributors, in particular, must raise awareness amongst their clients on issues pertaining to security, and

The targeting of small industrial facilities

In 2024, ANSSI processed multiple reports pertaining to the targeting of entities belonging to the sectors of renewable energy production and water sanitation, by hacktivist groups boasting low levels of technical skill but the ability to effectively mediatise their activities. The operators of Cyber Army of Russia Reborn (CARR) and Lulzsec Muslims notably gained access to management interfaces exposed to the Internet. The most successful of these operations brought a windfarm to a complete standstill for a few hours, which resulted in a financial loss of a few thousand euros for the victim.

Over the course of 2024, pro-Russian hacktivist groups regularly claimed the compromise of devices linked to the water sector. Given its inherent criticality to both the population and the industry, attackers paid particular attention to the water sector. This interest was only heightened by the specific context of the Paris Olympic and Paralympic Games. CARR, for instance, claimed unsophisticated attacks against the industrial systems of micro-hydropower plants, which involved the remote control of a hydropower plant in Courlon-sur-Yonne but actually concerned the windmill of Courlandon [65]. The group later claimed the remote takeover of an Italian water treatment plant located in Dittaino (Sicily), and announced the targeting of Seine sewage treatments plants with the aim of disrupting the Olympic competitions set to take place in the river's waters. The support and the awareness-raising efforts of potentially targeted entities were successful in preventing attacks on the Seine during the Games. 🇫🇷

must communicate clear rules for the secure implementation of devices. Though they are generally industry professionals, installers are rarely informed of the importance of implementing cyber hygiene and security measures.

2 THE HEIGHTENED INTENSITY OF DDoS ATTACKS

DDoS attacks are the most common type of attack aimed at destabilisation. They are particularly popular amongst hackers, but are now also used by other actors of various backgrounds (cyber-criminal actors, but also state-backed groups).

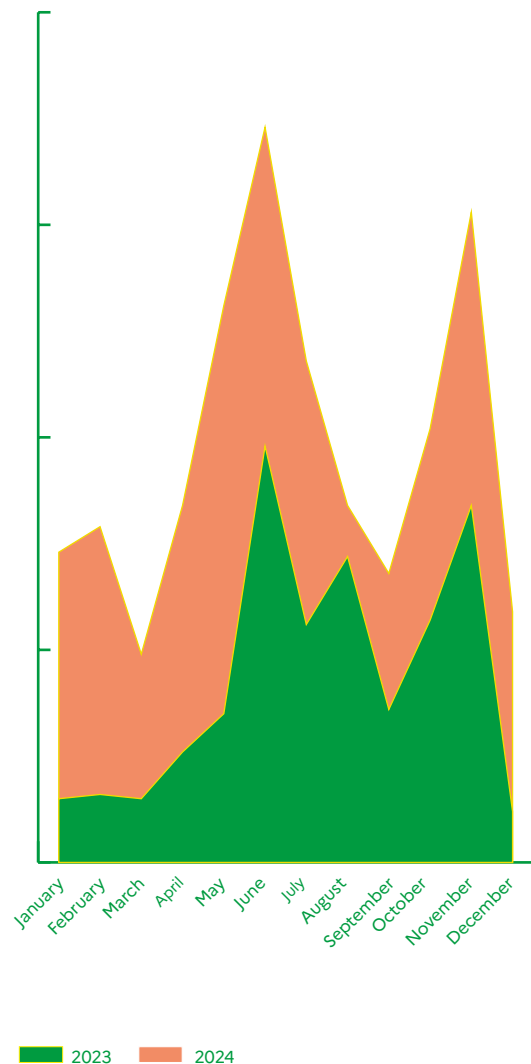
In 2024, public and private French entities were intensively targeted by DDoS attacks. The chart below illustrates this trend, indicating that the number of attacks of this type doubled between 2024 and 2023, and that they were particularly frequent during the Games.

In 2024, a couple of rare, widescale DDoS attacks against telecommunications infrastructure have had important repercussions on the availability of certain critical services.

Between the 10th and the 12th of March 2024, France's inter-ministerial network (RIE) was thus targeted over the course of several days, with significant reverberations on the activities of several ministries in spite of rapidly-implemented blocking measures. Following these attacks and in view of the upcoming Games, the RIE adopted additional security measures.

The telecommunications host and operator OVH was also targeted by an intense DDoS attack which was never claimed and whose goal could consequently not be determined [66]. These attacks are demonstrative of the capacity of DDoS attacks to periodically disturb essential infrastructure.

The number of DDoS attacks against French entities, as observed by ANSSI



Note:
a DDoS attack is considered to have had an impact when the availability of the targeted service has been affected.

In September of 2024, the U.S. Department of Justice announced the dismantlement of a global bot network (botnet) made up of thousands of connected devices, including cameras and storage devices. Dubbed “Raptor Train” by Lumen, this botnet was used by the reputedly state-sponsored intrusion set Flax Typhoon, itself potentially operated by the Chinese enterprise Integrity Technology Group. Raptor Train possessed numerous capabilities: exploitation of vulnerabilities, command and control, remote command execution, and DDoS attacks. Prior to its dismantlement, the network was reportedly used to target critical infrastructure across the world – including Taiwanese and American entities – for destabilisation purposes [67] [68]

3 SABOTAGE AND PREPOSITIONING²⁷ BY ADVANCED ACTORS

In 2024, ANSSI did not process any incidents which were the result of an advanced actor’s sabotage. This type of operation targeting critical ISs has more commonly been conducted in the context of geopolitical tensions, by state actors or by actors involved in conflicts, with the aim of destabilising and diminishing their opponent’s capabilities or of fulfilling military objectives.

Certain pro-Russian or pro-Ukrainian hackers have claimed attacks aimed at destruction. These attacks may also be linked to state operators using either authentic hacker channels or “sock-puppets” for influence and advertising purposes.

In January of 2024, the pro-Ukrainian hacker group BlackJack claimed the compromise of the Moscow-based telecom operator M9com via its Telegram channel. According to the group, this claim inscribed itself within a broader framework of retaliatory actions against the pro-Russian hacker group Solntsepëk²⁸. Pro-Ukrainian BlackJack activists changed the name of M9com’s

autonomous system to “SLAVAUKRAINI-AS”²⁹ and published allegedly exfiltrated data. The attack reportedly destroyed 20TB of data belonging to M9com and disrupted the provision of Internet access to Moscow citizens [69]. According to the specialised media The Record, the attack was conducted in cooperation with the Security Service of Ukraine (SBU) [70]. The SBU had already worked with pro-Ukrainian hacker groups in the past and were for example involved in the attack against the Russian Alpha Bank in October of 2023 [70].

The Ukrainian CERT (CERT-UA) [71] reported a campaign attributed to the Sandworm intrusion set which targeted, in March of 2024, about twenty companies from the energy, water, and heat supply sectors in ten different regions of Ukraine. Sandworm, also known as APT44 [72], is a reputedly Russian intrusion set which has been linked to espionage and sabotage operations conducted against multiple entities across the world – including Ukrainian entities, in the context of the war started by Russia. The objective of these attacks – all of which were successfully thwarted – was to compromise the proper functioning of the targeted entities’ industrial control systems. The CERT-UA was able to notify all of the concerned entities and assisted in countering the cyberattacks before the sabotage codes could be activated. It was estimated that this campaign aimed to amplify the effects of the bombardments on Ukrainian energy infrastructure in Spring of 2024. ←

²⁷

Prepositioning refers to the strategy used by cyber-attackers linked to states seeking to penetrate and remain on critical systems, potentially with the intention of engaging in acts of sabotage at a later date.

²⁸

The Solntsepëk group is presented as a sockpuppet for the operators of the Sandworm intrusion set, associated in open source with the Russian military intelligence service (GRU) [72].

²⁹

(“GLORY TO UKRAINE-AS”)

C ESPIONAGE

→ In 2024, as with the previous years, ANSSI's operational teams have been most involved in responding to attacks aimed at espionage. Given their longer duration and broader compromise perimeters, addressing such attacks requires significant means – particularly for digital investigations, for remediation, and for the characterisation of the threat.

Whether they be governmental bodies or a part of critical infrastructure, strategic entities are recurrent targets of strategic espionage operations by rival countries. Re-compromise and poly-compromise cases are still being observed, highlighting the perseverance of attackers and the means available to them in their efforts to achieve their goals.

1 TARGETING LINKED TO STRATEGIC STATE INTERESTS

In 2024, intrusion sets reputedly linked to Russian strategic interests were used for espionage purposes. These attack campaigns have been taking place since February of 2022, in the context of the war in Ukraine, and have primarily revolved around the search for information which may support Russian military or diplomatic efforts.

Over the course of the year, operators of the APT28 intrusion set associated in open source to the Russian military intelligence service (GRU) have conducted attacks on sectors of strategic interest for Russia – notably in Ukraine and within NATO countries. In 2024, the victimology associated with these attack campaigns has primarily included governmental, diplomatic, and research entities, as well as think tanks [73]. Some campaigns have been directed towards public French entities.

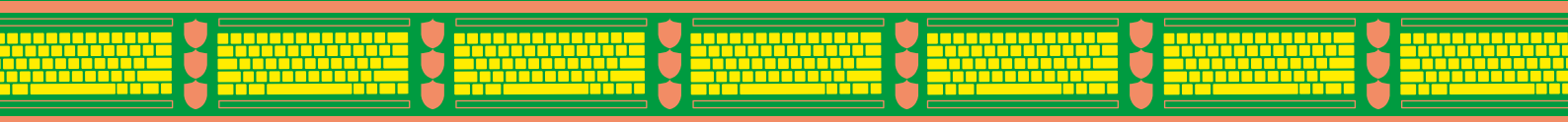
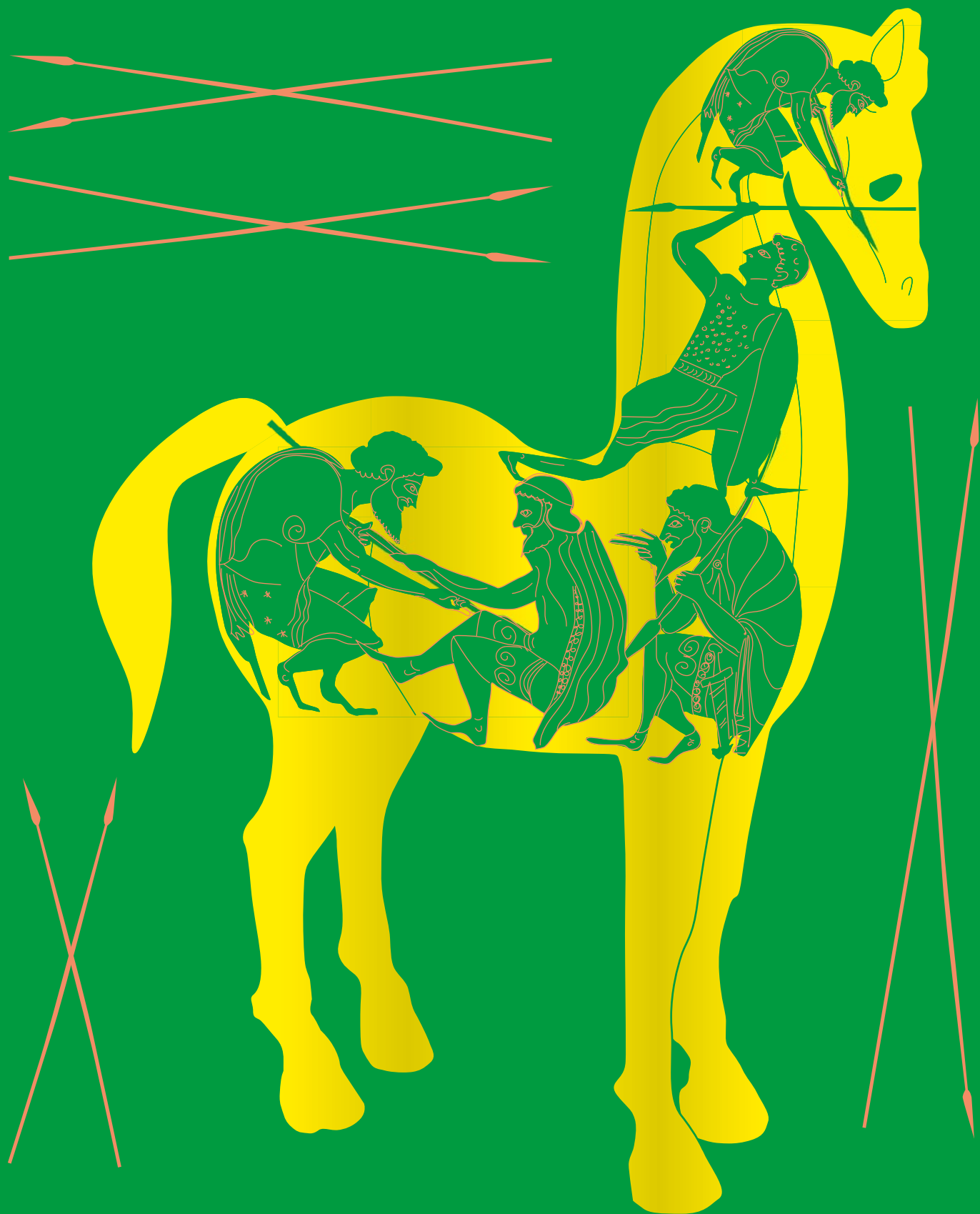
ANSSI notes that campaigns associated with the APT28 intrusion set are variably sophisticated and appear to mainly be used to gather immediate strategic intelligence. Some phishing campaigns may rely on compromised legitimate accounts, on

temporary e-mail address creation services, or on the usurpation of legitimate addresses. Operators also conduct brute-force attacks against webmails. APT28 operators have moreover exploited vulnerabilities, one of which was a 0-day vulnerability (CVE-2023-23397).

Other campaigns associated with intrusion sets reputedly linked to Russia were observed in 2024. The security vendor Google TAG [45] published information on the intrusion set Nobelium [21], which was reportedly used to carry out watering hole attack campaigns exploiting Mongolian governmental websites in 2023 and 2024. Attackers used similar vulnerability exploitation kits to those designed by the surveillance software companies NSO Group and Intellexa. These particular campaigns raised the question of how the operators of this intrusion set were able to access these tools. Indeed, tools developed in the offensive cyber-warfare ecosystem are rarely used outside of the seller-customer relationship, and Russia's offensive capabilities are known to traditionally be developed within its own national ecosystem. Detected by ANSSI long ago, the risk of proliferation engendered by the broad commercialisation of offensive tools is here further illustrated.

Activities associated with reputed Chinese intrusion sets have been particularly dense and well-documented during 2024. Vast sectors and geographical areas have been targeted by actors seeking to gather economic or strategic intelligence. For example, several countries attending the ASEAN-Australia Special Summit between the 4th and the 6th of March 2024 were targeted by at least two reputed Chinese intrusion sets – including the Mustang Panda intrusion set [74]. The transportation sector has also been impacted by such espionage operations.

In 2024, intrusion sets associated to China by different security vendors were used to target



the maritime transportation sector in Europe, as was suggested by the malicious implants found on on-board devices [75]. Asia remains the prime target of offensive operations linked to reputed Chinese intrusion sets, which have been known to conduct attacks against numerous governmental and private sectors. The RedJuliette intrusion set was thus used against multiple targets in Taiwan – including diplomatic representations [76].

One development observed in 2024 was the use, in Africa and in the Caribbean, of intrusion sets traditionally employed in campaigns conducted in Asia [77]. Several reputed Chinese intrusion sets have also intensely targeted the telecommunications sector – notably in France (see the next section).

Reputed Iranian offensive actors, meanwhile, have been associated with espionage operations against French universities, research organisations, and think tanks [73]. The reputed Iranian intrusion set APT42 was used in espionage and surveillance operations targeting individuals, and to a lesser extent organisations, perceived as threats to the stability of the Iranian regime³⁰. Its victimology includes researchers, journalists, dissidents, members of the Iranian diaspora, Western governmental representatives, think tanks, universities, and non-governmental organisations (NGOs). Since the end of 2023, however, the intrusion set's activities have involved a greater number of espionage operations conducted by its operators against entities such as NGOs, research centres, and universities. This activity was more recently observed by Microsoft against entities located in Belgium, France, Gaza, Israel, the United Kingdom, and the United States [78].

2 THE TARGETING OF THE TELECOMMUNICATIONS SECTOR

The targeting of telecommunications operators for espionage purposes is intense [1]. In France,

ANSSI has processed important cases in which the ISs of such operators were compromised, for espionage purposes, by intrusion sets in possession of advanced tools and techniques specifically developed to cater to this field.

In the United States, the intrusion set Salt Typhoon has been used against telecommunications infrastructure and reportedly targeted legal interception mechanisms (see focus page 43).

The telecommunications sector as a whole has been regularly and substantially targeted by attackers reputedly linked to China, particularly in Asia. Though the numerous cases of compromise reported by security vendors have involved the exfiltration of data, the nature of the leaks has not always been specified.

Over the past two years, ANSSI has processed several incidents affecting entities of the French telecommunications sector and aimed at espionage.

One of these incidents resulted in the compromise of a telecommunications operator's mobile core network. The intrusion set employed to achieve this compromise possessed a thorough understanding of the sector's specific communication protocols and concentrated its activities on unconventional devices or on devices which are rarely supervised by security solutions. These characteristics are indicative of the intrusion set's sophistication and significant adaptability. The investigations conducted by ANSSI reveal the alignment of the intrusion set with strategic state interests.

The Agency has also assisted an operator whose satellite communications infrastructure had been experiencing in-depth compromise for several years. During this attack, which was likely conducted for espionage purposes, attackers had the capacity to carry out acts of sabotage whose consequences might have proven critical given the

30

The American security vendor Mandiant (Mandiant, 2022) asserts with a high level of confidence that the operators of APT42 are working for the Islamic Revolutionary Guard Corps Intelligence Organisation (IRGC-IO).

Salt Typhoon

An attack campaign conducted by means of the Salt Typhoon intrusion set against major entities of the American telecommunications sector was reported in September of 2024. Indeed, several of such companies were compromised for espionage purposes. Following this campaign, over 150 victims were alerted by the FBI. Ongoing investigations suggest that the usurpation of a very high-privilege, insufficiently protected account allowed attackers to take control of 100 000 routers located all across the world. The operators of the intrusion set focused much of their attention on Washington D.C. and may have targeted legal interception systems with the aim of identifying the Chinese agents subjected to surveillance [79]. ↵

high availability requirements of satellite infrastructure. The information extracted from intercepted communications potentially allowed the attacker to conduct other attacks, or may have benefited other groups of attackers linked to the same strategic actor. According to ANSSI, it is very likely for this actor to keep targeting this type of infrastructure. As such, the Agency recommends that actors of the telecommunications sector pay closer attention to this threat.

Lastly, ANSSI has assisted a telecommunications operator in the eviction of a malicious actor which had been present on its IS since – at least – December of 2022. The level of privilege reached by the attacker – who was known to primarily target entities of this sector – granted them significant lateralisation, espionage, and sabotage capabilities on the victim's IS. The Agency's investigations confirmed that one of the objectives of the attack was to intercept the communications of specific targets.

The compromise of telecommunications operators may undermine the confidentiality of the data shared between clients. Though such activities have not been observed by ANSSI in practice, the accesses and privileges obtained by attackers during espionage operations can enable them to commit acts of sabotage. Traditionally used for emergency communication, satellite infrastructure is particularly vulnerable to this risk – as evidenced by the 2022 attack on the KA-SAT satellite communication network [80].

In the attacks observed by ANSSI, attackers have frequently used malicious codes developed for very specific technologies or devices. The limited reusability of such tools highlights the importance of the means deployed. What is more, in many of these cases the attack was detected several years after the initial compromise. ↵

BIBLIOGRAPHY

[01] CERT-FR.

Panorama de la cybermenace 2023.
23 février 2024.
<https://www.cert.ssi.gouv.fr/cti/CERTFR-2024-CTI-001/>

[02] GRANDS ÉVÈNEMENTS SPORTIFS EN FRANCE.

Évaluation de la menace 2024.
11 avril 2024.
<https://www.cert.ssi.gouv.fr/cti/CERTFR-2024-CTI-003/>

[03] THE NEW YORK TIMES.

Polish anti-doping agency targeted by cyber attack, 'fake' test results leaked.
14 août 2024.
<https://www.nytimes.com/athletic/5700428/2024/08/14/polish-anti-doping-cyber-attack/>

[04] SGDSN.

Synthèse de la menace informationnelle ayant visé les Jeux Olympiques et Paralympiques de Paris 2024.
13 septembre 2024.
<https://www.sgdsn.gouv.fr/publications/synthese-de-la-menace-informationnelle-ayant-vise-les-jeux-olympiques-et-paralympiques>

[05] FBI.

New Tradecraft of Iranian Cyber Group Aria.
30 octobre 2024.
<https://www.ic3.gov/CSA/2024/241030.pdf>

[06] IC3.

New Tradecraft of Iranian Cyber Group Aria Sepehr Ayandehsazan aka Emennet Pasargad.
30 octobre 2024.
<https://www.ic3.gov/CSA/2024/241030.pdf>

[07] CERT-FR.

L'ANSSI publie un corpus de guides dédiés à la remédiation d'incidents cyber.
16 janvier 2024.
<https://cyber.gouv.fr/actualites/lanssi-publie-un-corpus-de-guides-dedies-la-remediation-dincidents-cyber>

[08] CERT-FR.

Vulnérabilité dans Microsoft Netlogon.
11 mars 2021.
<https://www.cert.ssi.gouv.fr/alerte/CERTFR-2020-ALE-020/>

[09] SEKOIA.

Mamba 2FA: A new contender in the AiTM phishing ecosystem.
07 octobre 2024.
<https://blog.sekoia.io/mamba-2fa-a-new-contender-in-the-aitm-phishing-ecosystem/>

[10] CERT-FR.

Classe de vulnérabilités en environnement Active Directory.
15 octobre 2021.
<https://www.cert.ssi.gouv.fr/dur/CERTFR-2021-DUR-001/>

[11] CERT-FR.

Faillies sur les équipements de sécurité: retour d'expérience du CERT-FR.
12 juin 2024.
https://www.cert.ssi.gouv.fr/uploads/20240612_NP_ANSSI-SDO_Retex-Vuln_vf.pdf

[12] FORTINET.

Burning Zero Days: Suspected Nation-State Adversary Targets Ivanti CSA.
11 octobre 2024.
<https://www.fortinet.com/blog/threat-research/burning-zero-days-suspected-nation-state-adversary-targets-ivanti-csa>

[13] UNION EUROPÉENNE.

Règlement (UE) 2024/2847 du Parlement Européen et du Conseil concernant des exigences de cybersécurité horizontales pour les produits comportant des éléments numériques et modifiant les règlements (UE) n° 168/2013 et (UE) 2019/1020 et la directive (UE) 20.
20 novembre 2024.
<https://eur-lex.europa.eu/eli/reg/2024/2847/j?eliuri=eli%3Areg%3A2024%3A2847%3Aoj&locale=fr>

[14] CERT-FR.

Signalements du CERT-FR.
<https://www.cert.ssi.gouv.fr/signalements/>

[15] CERT-FR.

Signalement de vulnérabilité significative ou d'incident affectant significativement un logiciel (Art. L. 2321-4-1 du code de la Défense).
<https://www.cert.ssi.gouv.fr/signalement-vulnerabilite-incident-2321-4-1/>

[16] CERT-FR.

Incident affectant les solutions AnyDesk.
15 avril 2024.
<https://www.cert.ssi.gouv.fr/alerte/CERTFR-2024-ALE-003/>

[17] L'USINE DIGITALE.

Cybersécurité: Après Boulanger, Cultura révèle une fuite de données clients.
10 septembre 2024.
<https://www.usine-digitale.fr/article/cybersecurite-apres-boulanger-cultura-revele-une-fuite-de-donnees-clients.N2218245>

[18] MANDIANT.

IOC Extinction? China-Nexus Cyber Espionage Actors Use ORB Networks to Raise Cost on Defenders.
22 mai 2024.
<https://cloud.google.com/blog/topics/threat-intelligence/china-nexus-espionage-orb-networks/?hl=en>

[19] LUMEN.

KV-Botnet: Don't call it a Comeback.
07 février 2024.
<https://blog.lumen.com/kv-botnet-dont-call-it-a-comeback/>

[20] CISA.

MAR-10448362-1.v1 Volt Typhoon.
07 février 2024.
<https://www.cisa.gov/news-events/analysis-reports/ar24-038a>

[21] CERT-FR.

Malicious activities linked to the Nobelium intrusion set.
19 juin 2024.

<https://www.cert.ssi.gouv.fr/cti/CERTFR-2024-CTI-006/>

[22] MICROSOFT.

Microsoft Actions Following Attack by Nation State Actor Midnight Blizzard.
19 janvier 2024.

<https://msrc.microsoft.com/blog/2024/01/microsoft-actions-following-attack-by-nation-state-actor-midnight-blizzard/>

[23] SECURITIES AND EXCHANGE COMMISSION.

Hewlett Packard Enterprise company.
19 janvier 2024.

<https://www.sec.gov/Archives/edgar/data/1645590/000164559024000009/hpe-20240119.htm>

[24] CERT-PL.

Russian Foreign Intelligence Service (SVR) Cyber Actors Use JetBrains TeamCity CVE in Global Targeting.
13 décembre 2023.

<https://cert.pl/en/posts/2023/12/apt29-teamcity/>

[25] MORPHISEC.

Unveiling UAC-0184: The Steganography Saga of the IDAT Loader Delivering Remcos RAT to a Ukraine Entity in Finland.
26 février 2024.

<https://www.morphisec.com/blog/unveiling-uac-0184-the-remcos-rat-steganography-saga/>

[26] CERT-UA.

UAC-200: Cyberattaques ciblées utilisant DarkCrystal RAT et Signal comme véhicule de distribution de confiance (CERT-UA #9918) - UAC-0200: Цільові кібератаки з використанням DarkCrystal RAT та Signal як засобу довіреного розповсюдження (CERT-UA#9918).
<https://cert.gov.ua/article/6279561>

[27] ESENTIRE.

Blind Eagle's North American Journey.
20 février 2024.

<https://www.esentire.com/blog/blind-eagles-north-american-journey>

[28] GOOGLE THREAT INTELLIGENCE GROUP.

Hybrid Russian Espionage and Influence Campaign Aims to Compromise Ukrainian Military Recruits and Deliver Anti-Mobilization Narratives.
28 octobre 2024.

<https://cloud.google.com/blog/topics/threat-intelligence/russian-espionage-influence-ukrainian-military-recruits-anti-mobilization-narratives?hl=en>

[29] BSI.

The state of IT security in Germany in 2024.
18 novembre 2024.

https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2024.pdf?__blob=publicationFile&v=5

[30] SENTINELONE.

ChamelGang & Friends | Cyberespionage Groups Attacking Critical Infrastructure with Ransomware.
Juin 2024.

<https://www.sentinelone.com/blog/chamelgang-and-friends-cyberespionage-groups-attacking-critical-infrastructure-with-ransomware>

[31] GOOGLE TAG.

We're All in this Together | A Year in Review of Zero-Days Exploited In-the-Wild in 2023.
Mars 2024.

https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/Year_in_Review_of_ZeroDays.pdf

[32] MICROSOFT.

Frequent freeloader part I: Secret Blizzard compromising Storm-0156 infrastructure for espionage.
04 décembre 2024.

<https://www.microsoft.com/en-us/security/blog/2024/12/04/frequent-freeloader-part-i-secret-blizzard-compromising-storm-0156-infrastructure-for-espionage/>

[33] ESET.

RomCom exploits Firefox and Windows zero days In-The-Wild.
26 novembre 2024.

<https://www.welivesecurity.com/en/eset-research/romcom-exploits-firefox-and-windows-zero-days-in-the-wild/>

[34] FORBES.

Exclusive: Israeli Surveillance Companies Are Siphoning Masses Of Location Data From Smartphone Apps.
11 décembre 2020.

<https://www.forbes.com/sites/thomasbrewster/2020/12/11/exclusive-israeli-surveillance-companies-are-siphoning-masses-of-location-data-from-smartphone-apps/>

[35] WALL STREET JOURNAL.

How ads on your phone can aid government surveillance.
13 octobre 2023.

<https://www.wsj.com/tech/cybersecurity/how-ads-on-your-phone-can-aid-government-surveillance-943bde04>

[36] KTLA.

LAPD using Israeli spy company to gather personal data, report says.
28 novembre 2023.

<https://ktla.com/news/local-news/lapd-using-israeli-spy-company-to-gather-personal-data-report-says/>

[37] IRISH COUNCIL FOR CIVIL LIBERTIES.

Europe's hidden security crisis.
<https://www.iccl.ie/digital-data/europes-hidden-security-crisis/>

[38] KREBSONSECURITY.

Stark Industries Solutions: An Iron Hammer in the Cloud.
 23 mai 2024.
<https://krebsonsecurity.com/2024/05/stark-industries-solutions-an-iron-hammer-in-the-cloud/>

[39] SEKOIA.

NoName057(16)'s DDoSia project: 2024 updates and behavioural shifts.
 23 février 2024.
<https://blog.sekoia.io/Noname05716-Ddosia-project-2024-updates-and-behavioural-shifts/>

[40] TEAM-CYMRU.

FIN7: The Truth Doesn't Need to be so STARK.
 13 août 2024.
<https://www.team-cymru.com/post/fin7-the-truth-doesn-t-need-to-be-so-stark>

[41] CISA.

New Tradecraft of Iranian Cyber Group Aria.
 30 octobre 2024.
<https://www.ic3.gov/CSA/2024/241030.pdf>

[42] SECURITY INTELLIGENCE.

Hive0051 goes all in with a triple threat.
 09 avril 2024.
<https://securityintelligence.com/x-force/hive0051-all-in-triple-threat/>

[43] SEKOIA.

WebDAV-as-a-Service: Uncovering the infrastructure behind Emmenhtal loader distribution.
 19 septembre 2024.
<https://blog.sekoia.io/webdav-as-a-service-uncovering-the-infrastructure-behind-emmenhtal-loader-distribution/>

[44] LE MONDE.

Le logiciel espion Pegasus détecté dans le téléphone de Nathalie Loiseau et d'une autre eurodéputée.
 22 février 2024.
https://www.lemonde.fr/elections-europeennes/article/2024/02/22/le-logiciel-espion-pegasus-detecte-dans-le-telephone-de-nathalie-loiseau-et-d-une-autre-eurodeputee_6217981_1168667.html

[45] GOOGLE.

State-backed attackers and commercial surveillance vendors repeatedly use the same exploits.
 29 août 2024.
<https://blog.google/threat-analysis-group/state-backed-attackers-and-commercial-surveillance-vendors-repeatedly-use-the-same-exploits/>

[46] MINISTÈRE DE L'EUROPE ET DES AFFAIRES ÉTRANGÈRES.

Processus de Pall Mall: Lutter contre la prolifération et l'usage irresponsable des capacités d'intrusion cyber disponibles sur le marché (Lancaster House, Londres, 6 février 2024).
 06 février 2024.
<https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/securite-desarmement-et-non-proliferation/actualites-et-evenements-lies-a-la-securite-au-desarmement-et-a-la-non/2024/article/processus-de-pall-mall-lutter-contre-la-proliferation-et-l-usa>

[47] SEKOIA.

Active Lycantrox infrastructure illumination.
 02 octobre 2023.
<https://blog.sekoia.io/active-lycantrox-infrastructure-illumination/>

[48] GOOGLE.

Buying Spying: How the commercial surveillance industry works and what can be done about it.
 06 février 2024.
<https://blog.google/threat-analysis-group/commercial-surveillance-vendors-google-tag-report/>

[49] TECHCRUNCH.

Spyware startup Variston is losing staff — some say it's closing.
 15 février 2024.
<https://techcrunch.com/2024/02/15/variston-spyware-losing-staff-some-say-closing/>

[50] TECHCRUNCH.

Lawyer allegedly hacked with spyware names NSO founders in lawsuit.
 13 novembre 2024.
<https://techcrunch.com/2024/11/13/lawyer-allegedly-hacked-with-spyware-names-nso-founders-in-lawsuit/>

[51] AMNESTY INTERNATIONAL.

Indonesia: A web of surveillance: Unravelling a murky network of spyware exports to Indonesia.
 01 mai 2024.
<https://www.amnesty.org/en/documents/asa21/7974/2024/en/>

[52] ZDNET.

Rançongiciels: pourquoi la justice française a ouvert moins de nouvelles enquêtes l'an passé.
 06 janvier 2025.
<https://www.zdnet.fr/actualites/rancongiels-pourquoi-la-justice-francaise-a-ouvert-moins-de-nouvelles-enquetes-lan-passe-403845.htm>

[53] RECORDED FUTURE.

RansomHub Draws in Affiliates with Multi-OS Capability and High Commission Rates.
 20 juin 2024.
<https://www.recordedfuture.com/research/ransomhub-draws-in-affiliates-with-multi-os-capability-and-high-commission-rates>

[54] GROUP-IB.

RansomHub ransomware-as-a-service.
 28 août 2024.
<https://www.group-ib.com/blog/ransomhub-raas/>

[55] CISA.

#StopRansomware: RansomHub Ransomware.
 29 août 2024.
<https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-242a>

[56] BLEEPINGCOMPUTER.

Germany takes down cybercrime market with over 180,000 users.
01 mars 2024.

<https://www.bleepingcomputer.com/news/legal/germany-takes-down-cybercrime-market-with-over-180-000-users/>

[57] LE MONDE.

BreachForums: le fondateur du plus important site de vente de données personnelles volées condamné par la justice.
20 janvier 2024.

https://www.lemonde.fr/pixels/article/2024/01/20/breachforums-le-fondateur-du-plus-important-site-de-vente-de-donnees-personnelles-volees-condamne-par-la-justice_6211870_4408996.html

[58] EUROPOL.

Law enforcement disrupt world's biggest ransomware operation.
20 février 2024.

<https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation>

[59] TRENDMICRO.

Unveiling the Fallout: Operation Cronos' Impact on LockBit Following Landmark Disruption.
03 avril 2024.

https://www.trendmicro.com/en_us/research/24/d/operation-cronos-aftermath.html

[60] CERT-FR.

Opération ENDGAME.
30 mai 2024.

<https://www.cert.ssi.gouv.fr/cti/CERTFR-2024-CTI-004/>

[61] PARQUET DE PARIS.

Communiqué de presse.
2024.

https://www.linkedin.com/posts/parquet-de-paris_communique%C3%A9-de-presse-endgame-activity-7201856692140056576-v3jT

[62] EUROPOL.

LockBit power cut: four new arrests and financial sanctions against affiliates.
01 octobre 2024.

<https://www.europol.europa.eu/media-press/newsroom/news/lockbit-power-cut-four-new-arrests-and-financial-sanctions-against-affiliates>

[63] MINISTÈRE DE L'INTÉRIEUR.

Une lettre-plainte pour la violation des données personnelles via Viamedis et Almerys. Ministère de l'intérieur.
01 septembre 2025.

<https://www.masecurite.interieur.gouv.fr/fr/actualites/lettre-plainte-vol-donnees-personnelles-viamedis-almerys>

[64] CERT-FR.

Exfiltration de données du secteur social - retour d'expérience du CERT-FR.
24 septembre 2024.

<https://www.cert.ssi.gouv.fr/cti/CERTFR-2024-CTI-009/>

[65] LE MONDE.

Comment Sandworm, les hackers d'élite de l'armée russe, ont piraté un moulin français en pensant attaquer un barrage.
17 avril 2024.

https://www.lemonde.fr/pixels/article/2024/04/17/comment-sandworm-les-hackers-d-elite-de-l-armee-russe-ont-pirate-un-moulin-francais-en-pensant-attaquer-un-barrage_6228320_4408996.html

[66] OVH.

The Rise of Packet Rate Attacks: When Core Routers Turn Evil.
01 juillet 2024.

<https://blog.ovhcloud.com/the-rise-of-packet-rate-attacks-when-core-routers-turn-evil/>

[67] U.S JUSTICE.

Department of Court-Authorized Operation Disrupts Worldwide Botnet Used by People's Republic of China State-Sponsored Hackers.
18 septembre 2024.

<https://www.justice.gov/archives/opa/pr/court-authorized-operation-disrupts-worldwide-botnet-used-peoples-republic-china-state>

[68] LUMEN.

Derailing the Raptor Train.
18 septembre 2024.

<https://blog.lumen.com/derailing-the-raptor-train/>

[69] REUTERS.

Hackers hit Moscow internet provider in response to Kyivstar cyber attack.
01 septembre 2024.

<https://www.reuters.com/technology/cybersecurity/hackers-hit-moscow-internet-provider-response-kyivstar-cyber-attack-source-2024-01-09/>

[70] THE RECORD.

Pro-Ukraine hackers claim breach of Russian internet provider.
09 janvier 2024.

<https://therecord.media/ukraine-blackjack-hackers-sbu-claim-breach-russia-M9com>

[71] CERT-UA.

Le mode opératoire UAC-0133 (Sandworm) prévoit un cyber-sabotage sur près de 20 infrastructures critiques en Ukraine (Плани UAC-0133 (Sandworm) щодо кібердиверсії на майже 20 об'єктах критичної інфраструктури України).
19 avril 2024.

<https://cert.gov.ua/article/6278706>

[72] MANDIANT.

APT44: Unearthing Sandworm.
2024.

<https://services.google.com/fh/files/misc/apt44-unearthing-sandworm.pdf>

[73] CERT-FR.

Organismes de recherche et think tanks - État de la menace informatique.

02 septembre 2024.

<https://www.cert.ssi.gouv.fr/cti/CERTFR-2024-CTI-008/>

[74] UNIT 42.

ASEAN Entities in the Spotlight: Chinese APT Group Targeting.

26 mars 2024.

<https://unit42.paloaltonetworks.com/chinese-apt-target-asean-entities/>

[75] ESET.

Iran - Aligned Cyberattacks: Rise in Disruptive Operations.

2024.
<https://web-assets.esetstatic.com/wls/en/papers/threat-reports/eset-apt-activity-report-q4-2023-q1-2024.pdf>

[76] RECORDED FUTURES.

Chinese State-Sponsored RedJuliatt Intensifies Taiwanese Cyber Espionage via Network Perimeter Exploitation.

24 juin 2024.

<https://www.recordedfuture.com/research/redjuliatt-intensifies-taiwanese-cyber-espionage-via-network-perimeter>

[77] CHECKPOINT.

Chinese Espionage Campaign Expands to Target Africa and The Caribbean.

23 mai 2024.

<https://blog.checkpoint.com/research/chinese-espionage-campaign-expands-to-target-africa-and-the-caribbean/>

[78] MICROSOFT.

New TTPs observed in Mint Sandstorm campaign targeting high-profile individuals at universities and research orgs.

17 janvier 2024.

<https://www.microsoft.com/en-us/security/blog/2024/01/17/new-ttps-observed-in-mint-sandstorm-campaign-targeting-high-profile-individuals-at-universities-and-research-orgs/>

[79] WALL STREET JOURNAL.

How Chinese Hackers Graduated From Clumsy Corporate Thieves to Military Weapons.

04 janvier 2025.

<https://www.wsj.com/tech/cybersecurity/typhoon-china-hackers-military-weapons-97d4ef95?msockid=30240784eaf162d40dae1208eb9e631d>

[80] CERT-FR.

Panorama de la cybermenace 2022.

10 février 2023.

<https://www.cert.ssi.gouv.fr/cti/CERTFR-2023-CTI-001/>

[81] MANDIANT.

APT42: Crooked Charms, Cons and Compromises.

Septembre 2022.

<https://www.mandiant.com/sites/default/files/2022-09/apt42-report-mandiant.pdf>

[82] APPLE.

À propos du mode Isolement.

<https://support.apple.com/fr-fr/105120>

[83] GOOGLE.

Bringing Access Back — Initial Access Brokers Exploit F5 BIG-IP (CVE-2023-46747) and ScreenConnect.

21 mars 2024.

<https://cloud.google.com/blog/topics/threat-intelligence/initial-access-brokers-exploit-f5-screenconnect?hl=en>

[84] HAARETZ.

Israel Tried to Keep Sensitive Spy Tech Under Wraps. It Leaked Abroad.

11 avril 2024.

<https://www.haaretz.com/israel-news/security-aviation/2024-04-11/ty-article/.premium/israel-tried-to-keep-sensitive-spy-tech-under-wraps-it-leaked-abroad/0000018e-c948-d480-a99e-cf5f24900000>

CYBER THREAT OVERVIEW 2024

Published by
French Cybersecurity Agency (ANSSI)

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

REGISTRATION OF COPYRIGHT

February 2025
Published under open license/
Open Licence (Etalab — V2.0)

ISSN 2999-5612 (print)
ISSN 2801-4154 (online)

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

