RÉPUBLIQUE
FRANÇAISE

Liberté
Égalité
Fraternité

CYBER THREAT OVERVIEW 2022

CYBER THREAT OVERVIEW 2022

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Despite a year marked by the Russia-Ukraine conflict and its repercussions in cyberspace, the cyber threat has not evolved significantly as the trends observed in 2021 bore out in 2022. The overall threat level sustained in 2022 with a total of 831 confirmed incidents compared to 1,082 in 2021.[1] However, a lower figure does not equate to a decreased threat level. Indeed, ANSSI observed a drop in ransomware attacks targeting public and private regulated operators, except hospitals, but it does not illustrate the overall evolution of this cyber threat which remained at a high level while carrying over to more vulnerable entities.

Malicious actors continue to steadily improve their capabilities for financial gain, espionage and destabilisation motives. This improvement particularly shows in how attackers have progressed in selecting the targets' networks they seek to gain discret and long-term access to. Such targeting is also exemplified by the type of targeted entities and confirms the attackers' interest in contractors, suppliers, subcontractors, regulatory bodies and the wider ecosystem of their ultimate targets.

The convergence of tools and techniques used by different attacker profiles also continued in 2022 and still complicates threat assessment. As already identified in 2021, the use of ransomware by state-sponsored attackers highlights the porosity between different attacker profiles. Their use for destabilisation purposes in the context of sabotage operations actually materialised in 2022 and further disrupts the grasp of malicious activities. The emergence of alternatives to generic codes used by several attacker profiles, such as Cobalt Strike, leads to detection challenges and also muddles the uncovering of associated activities.

Financially motivated attacks remain the most prevalent in 2022. While they declined in the first half of 2022, ransomware attacks surged from Summer onwards – particularly against local authorities and healthcare institutions, with significant consequences. Other cybercriminal activities such as scams, sale of access-as-a-service (AaaS) or malware-as-a-service (MaaS) and cryptomining continued.

Cyber espionage also lingered on in 2022 both in France and around the world, and remained. ANSSI teams primarily handled this category of threat during the past year. As in 2021, most of espionage incidents involved once

again intrusion sets publicly associated with China. These repeated intrusions attest to an ongoing effort to breach the networks of strategic French companies.

The Russian invasion of Ukraine was also a key driver of strategic espionage campaigns throughout 2022 and laid the groundwork for destabilisation efforts in Europe. While sabotage operations have so far been relatively confined to the battleground, other modes of action such as distributed-denial-of-service (DDoS) attacks, website defacement and information operations combined with data exfiltration, have affected numerous victims in Europe and North America.

Uncontrolled digital uses and poor data security continue to provide far too many opportunities to conduct malicious activities. Cloud computing and the outsourcing of services to managed service providers, without adequate cyber security clauses, still represent a valued vector of indirect attacks. Despite a decreasing number of supply chain attacks in 2022, this trend remains extant and underlines a systemic risk. Finally, the exploitation of patchable vulnerabilities is still too often encountered, notably amongst incidents handled by or reported to ANSSI, despite the publication of advisories and alerts on the CERT-FR website or reporting campaigns. ANSSI urges priority be given to applying patches to systems exposed on the Internet or, failing that, implementing workaround measures.

The geopolitical context and the major events of the 2023 Rugby World Cup and the 2024 Olympic and Paralympic Games will provide attackers with numerous opportunities to cause disruption. The rigorous implementation of an update policy, regular user awareness training and the development of incident detection and response capabilities can help ward against the most common threats.

1. 1,082 confirmed intrusions were reported to ANSSI in 2021.

1 → ATTACKERS WITH CONSTANTLY EVOLVING CAPABILITIES

A → INCREASED CONVERGENCE OF ATTACKERS' TOOLS

State-sponsored attackers continue to use codes and methods historically employed by the cybercriminal community. This is particularly true of ransomware, which in 2022 was again used for destabilisation purposes by state-sponsored attackers. In July 2022, Albania was the target of several cyber attacks, including ransomware and wipers[2] as part of a destabilisation operation (1). These attacks led to the temporary unavailability of several of the Albanian government's digital services and websites on 15 July 2022 (2).

Other malware has been associated with both cybercriminal and espionage activities. This is notably the case of the DarkCrystal RAT modular backdoor, which was first sold in 2018 on Russian-speaking forums and includes a stealer,[3] a command and control interface, and an administration tool (3). Its modular structure means it can be tailored for the attacker's objectives by adding modules for keystroke logging, web browser logging and screen capture.

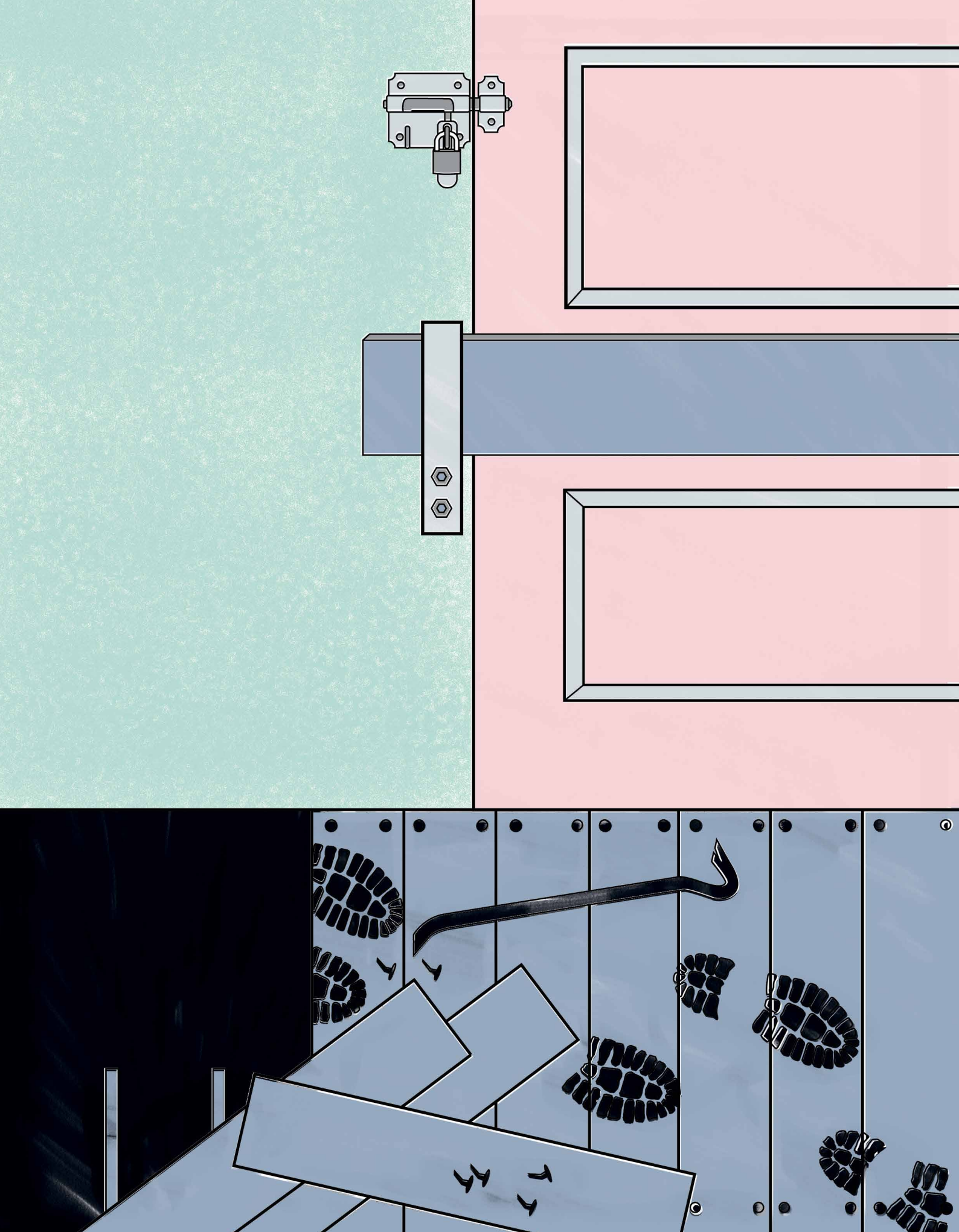
2. Malware aimed at destroying data on an IT system.
3. A malicious program that collects various data (logins and passwords, authentication tokens) before transmitting them to its operator.

The relatively cheap price of this tool[4] and its public availability quickly made it popular amongst several cyber criminals. DarkCrystal RAT was also reportedly used by the Sandworm intrusion set in June 2022 to compromise Ukrainian media and telecommunications organisations, according to CERT-UA (4) (5).

This phenomenon is compounded by the suspected proximity of some cybercriminal groups to governments. In the early months of the Russia-Ukraine conflict, Russian-speaking cybercriminal groups, such as Conti, shifted their focus to align with Russian interests in Ukraine and displayed support for the Russian government (6). Conversely, some groups wanted to target Russia. Other groups have chosen to remain neutral and focus on purely lucrative attacks. These patriotic stances, whether spontaneous or orchestrated, again make it difficult to assess and attribute malicious activities.

The increased reuse of open source and commercial tools such as Cobalt Strike[5] by both state-sponsored and cybercriminal attackers also contribute to the difficulty in identifying the threat. The emergence of alternatives to these generic tools further complicates the detection of malicious activities. Whether they are commercial, like Brute Ratel, or publicly available, such as Mythic or Sliver, these tools are increasingly used by different attacker profiles for espionage and other cybercriminal activities (7) (8). Their use reflects attackers' desire for discretion.

4. 500 rubbles for a two-month subscription.
5. Commercial penetration testing tool.



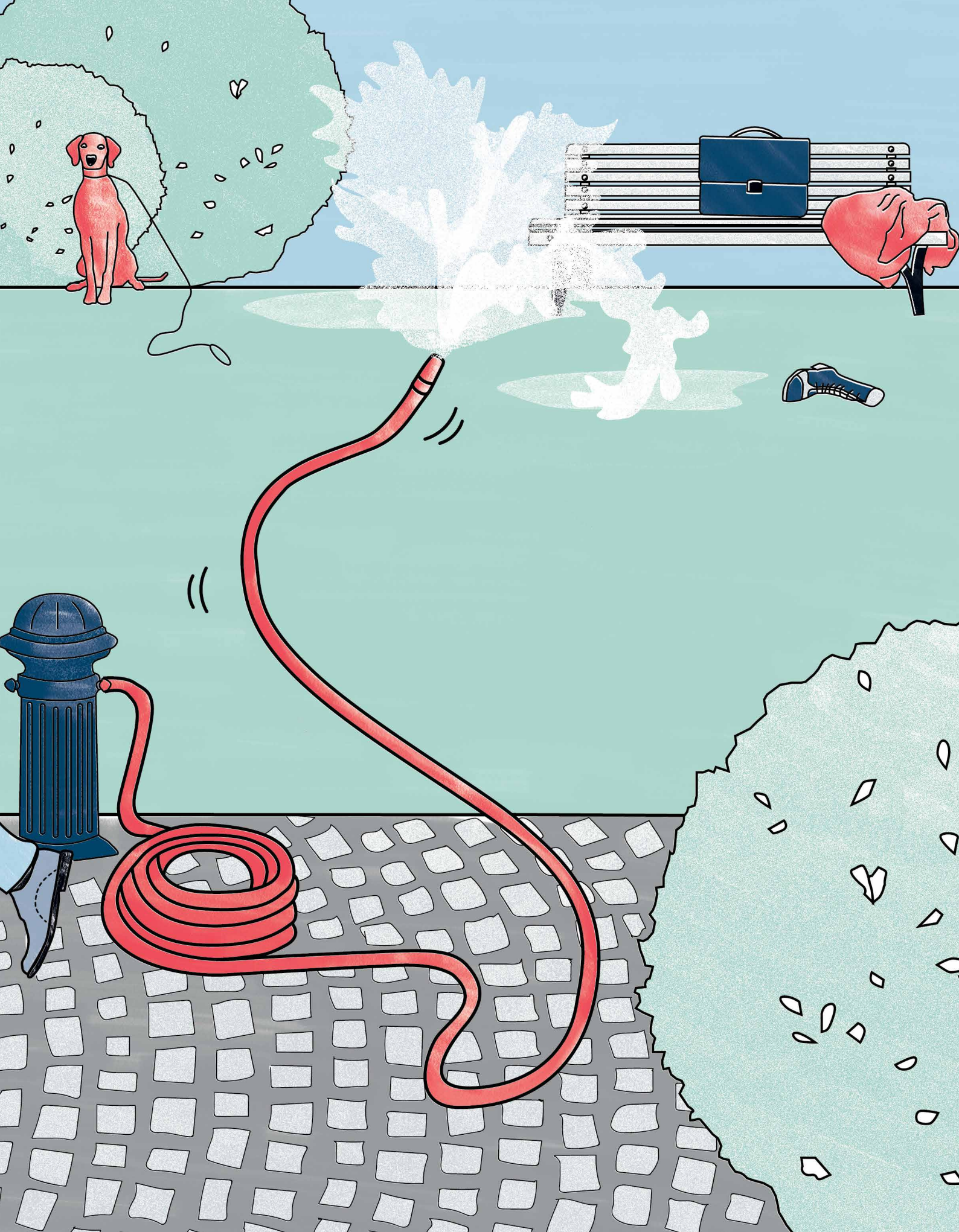
B → TARGETING OF PERIPHERAL DEVICES

Attackers' concern for stealth can also be noticed when looking at the type of device targeted. Compromising peripheral devices, such as firewalls or routers, offers multiple benefits. These devices, which are permanently connected and generally not monitored neither by consumer nor professional tools, provide attackers with stealthy and sustained access to their victims' networks. The nature of these devices means that tools and methods related to collection and analysis have to be adapted as part of remediation operations.

These devices can also be incorporated to the malicious actors' infrastructure in order to anonymise their communications or a reconnaissance activity. This technique was employed by attackers using the APT31 intrusion set to build a Command and Control (C2) and reconnaissance infrastructure by compromising Pakedge, Cyberoam and Cisco routers (9).

This type of targeting has been observed and analysed recently by ANSSI. The agency was informed of malicious activities carried out between April and December 2021 on the network equipment of a French entity with an international presence. ANSSI's analysis showed that an attacker had compromised this equipment and installed Remote Administration Tools (RATs). Having gained undetected access on these peripheral devices, the attacker was able to connect to machines on the victim's internal network, despite having been booted out of it a year earlier after remediation of a previous compromise. Then, they exfiltrated technical information and business data. Having taken control of various firewalls, the attacker was also able to intercept a certain type of traffic between a few offices of the entity that were targeted specifically.

Cybercriminal actors have also resorted to these procedures. The operators of the Trickbot Trojan used this method to compromise MikroTik routers which were then added to their C2 (10).



C → THE PERSISTENT ISSUE OF PRIVATE SURVEILLANCE COMPANIES

Despite the revelations about NSO Group's Pegasus program in 2021, the private cyber-arms industry remains very active, as evidenced by the recent acquisition of Italian company RCS Lab by its competitor Cy4Gate (11). RCS Lab's products, and in particular its Hermit spyware, have been the subject of publications by cybersecurity vendor Lookout (12) and Google's Threat Analysis Group (13). Hermit was reportedly used in Kazakhstan to target Android devices following protests in early 2022. While no targeting of France or French figures using this spyware has been reported, the potential misuse of this type of tool warrants the monitoring of these companies and their capabilities.

The spyware issue is being addressed at the European level by the European Parliament's PEGA Committee of Inquiry,[6] which released its preliminary report on 8 November 2022 (14).

In addition to these actors selling spyware solutions, companies like BellTrox InfoTech Services (15) provide less sophisticated but persistent services such as human expertise: 'hackers for hire'. They carry out intense economic and political espionage activities on behalf of various clients that may lead to an infringement of business confidentiality or national security.

Recent revelations by *The Sunday Times* newspaper and the non-governmental organisation *The Bureau of Investigative Journalism* (16) about campaigns to spy on public figures who criticised the selection of Qatar to host the 2022 football World Cup further illustrate this. Four French public figures are among the presumed targets (17). Regular publications on offensive cyber capacities in the private sphere highlight the need to strengthen detection and investigation capabilities.

6. Committee created on 10 March 2022 to investigate the use of Pegasus and equivalent spyware surveillance software. It has been mandated to gather information on the use by Member States and other countries of surveillance software that allegedly violates the rights and freedoms enshrined in the Charter of Fundamental Rights of the European Union.

2 →

FINANCIAL GAIN, ESPIONAGE AND DESTABILISATION REMAIN THE MAIN OBJECTIVES OF ATTACKERS

A → ATTACKS FOR PROFIT STILL COMMON

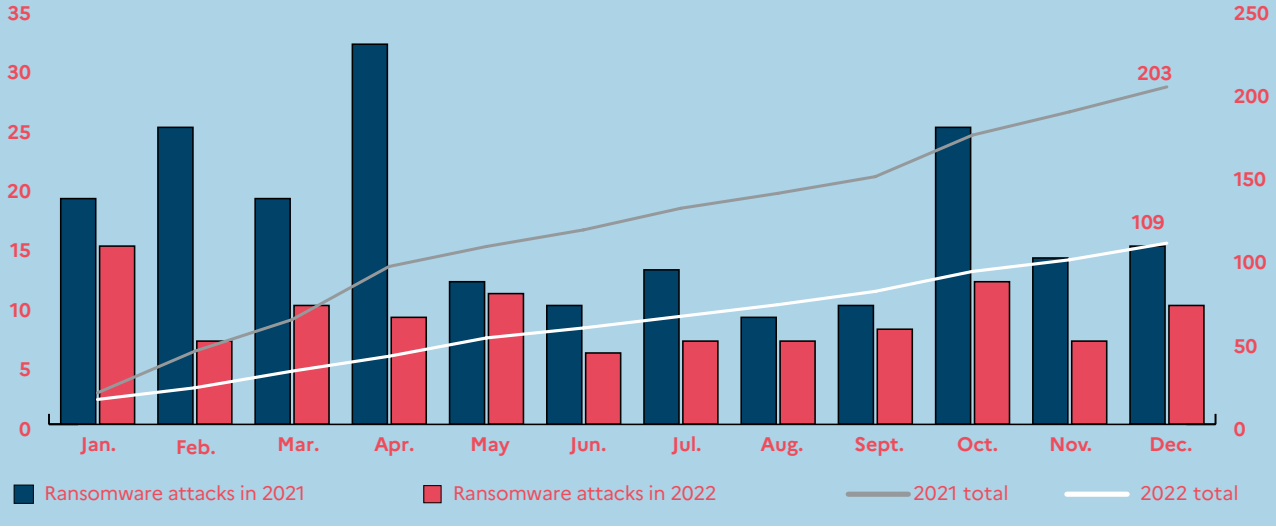
→ While financially-motivated attacks remain commonplace, a decline in ransomware activity in France and Europe has been observed since the beginning of 2022, both by ANSSI and certain foreign partners and cyber security vendors (18). The total number of compromises brought to the attention of ANSSI is thus 46% lower compared to the same period in 2021. This decline was first observed in late 2021. It is nonetheless limited to incidents reported to the agency and does not necessarily reflect the full picture. However, ANSSI has noted an increase in ransomware attacks since September, which could herald a forthcoming intensification of these malicious activities. Several local authorities have fallen victim to ransomware since the summer of 2022 (19) (20) (21) (22) (23) (24).

↓

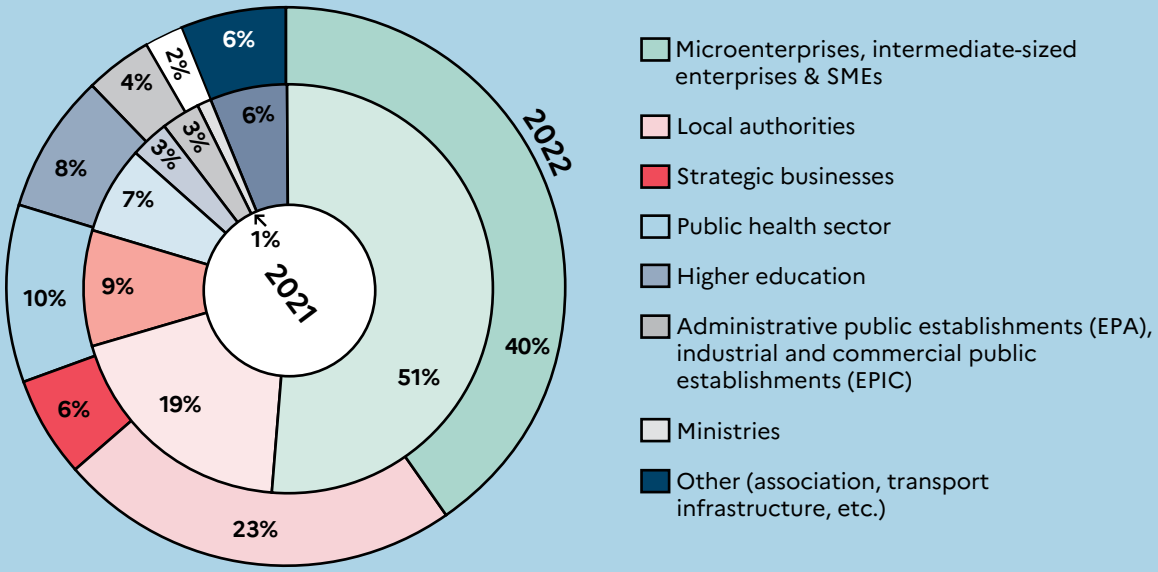
LOCAL AUTHORITIES HAVE BEEN PARTICULARLY AFFECTED BY RANSOMWARE ATTACKS,

representing the second most affected category of victims after micro-businesses & SMEs. They account for 23% of the ransomware incidents reported to or handled by ANSSI in 2022. These destructive attacks have significant consequences for the communities impacted, sometimes disrupting payroll services, social benefit payments and the management of civil registers. Once the attack is uncovered, the day-to-day operations of these entities continues to deteriorate during the rebuild period, with a lasting effect on services for the public.

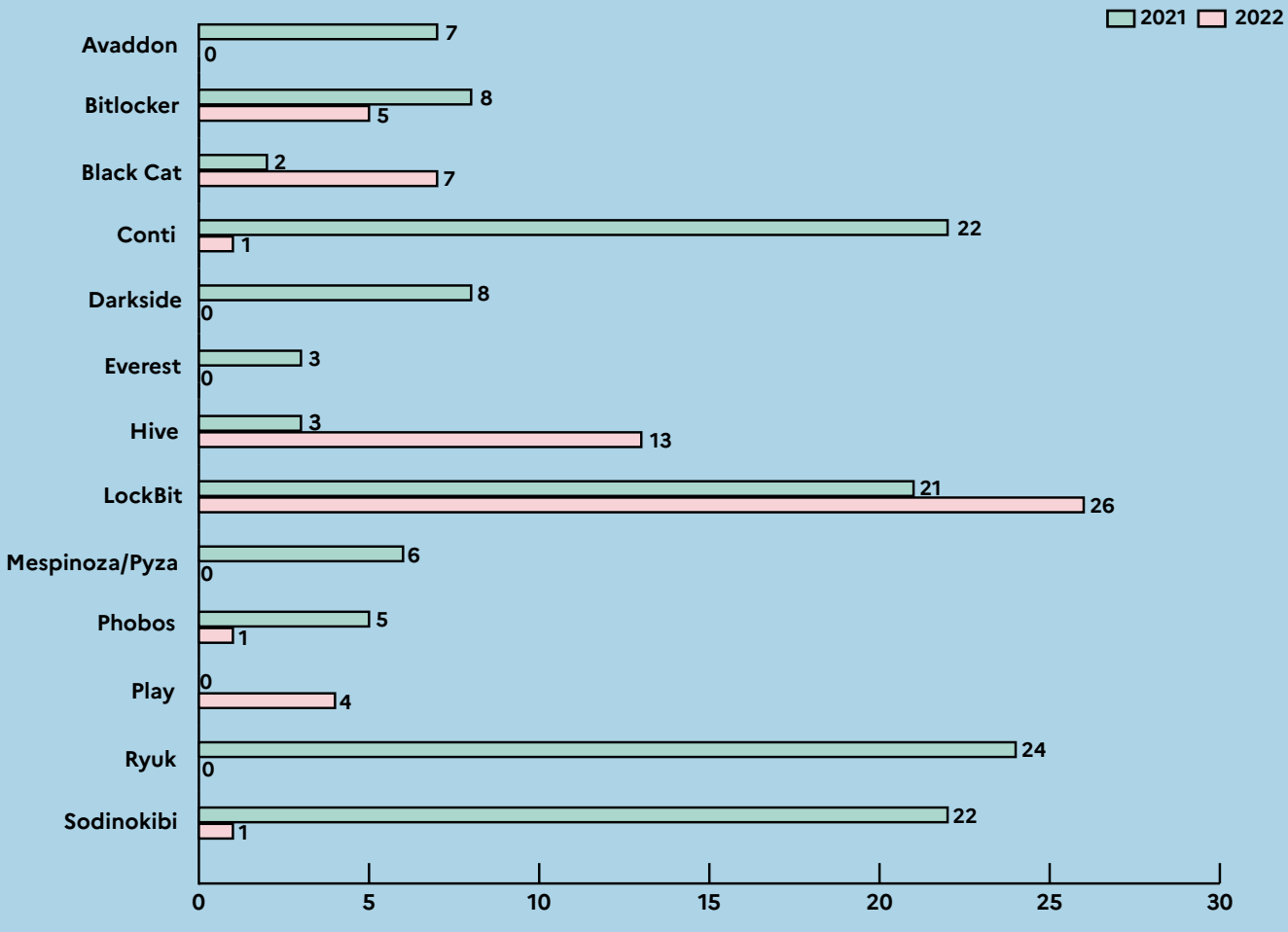
→ COMPARISON OF RANSOMWARE ATTACKS REPORTED IN 2021 AND 2022.



→ BREAKDOWN OF TYPES OF RANSOMWARE VICTIMS IN 2021 AND 2022



→ COMPARISON OF THE MAIN STRAINS USED IN INCIDENTS REPORTED TO ANSSI IN 2021 AND 2022.



Several factors may explain this perceptible decline. After the Russian invasion of Ukraine, a shift in targeting by cybercriminal groups was noticed. Some groups have chosen to align themselves with the interests of the warring parties. Other groups have substantially changed their geographical focus, targeting Latin America in particular (25). The deterrent commitment of some countries, such as the United States (26), to the fight against cybercrime may have influenced the targeting of cybercriminal actors. The Russia-Ukraine conflict has also led to the reorganisation of some Russian-speaking cybercriminal groups, such as Conti, which suffered data leaks presumably orchestrated by a Ukrainian member of the group (27). This restructuring may have had an impact on the operational tempo of these groups.

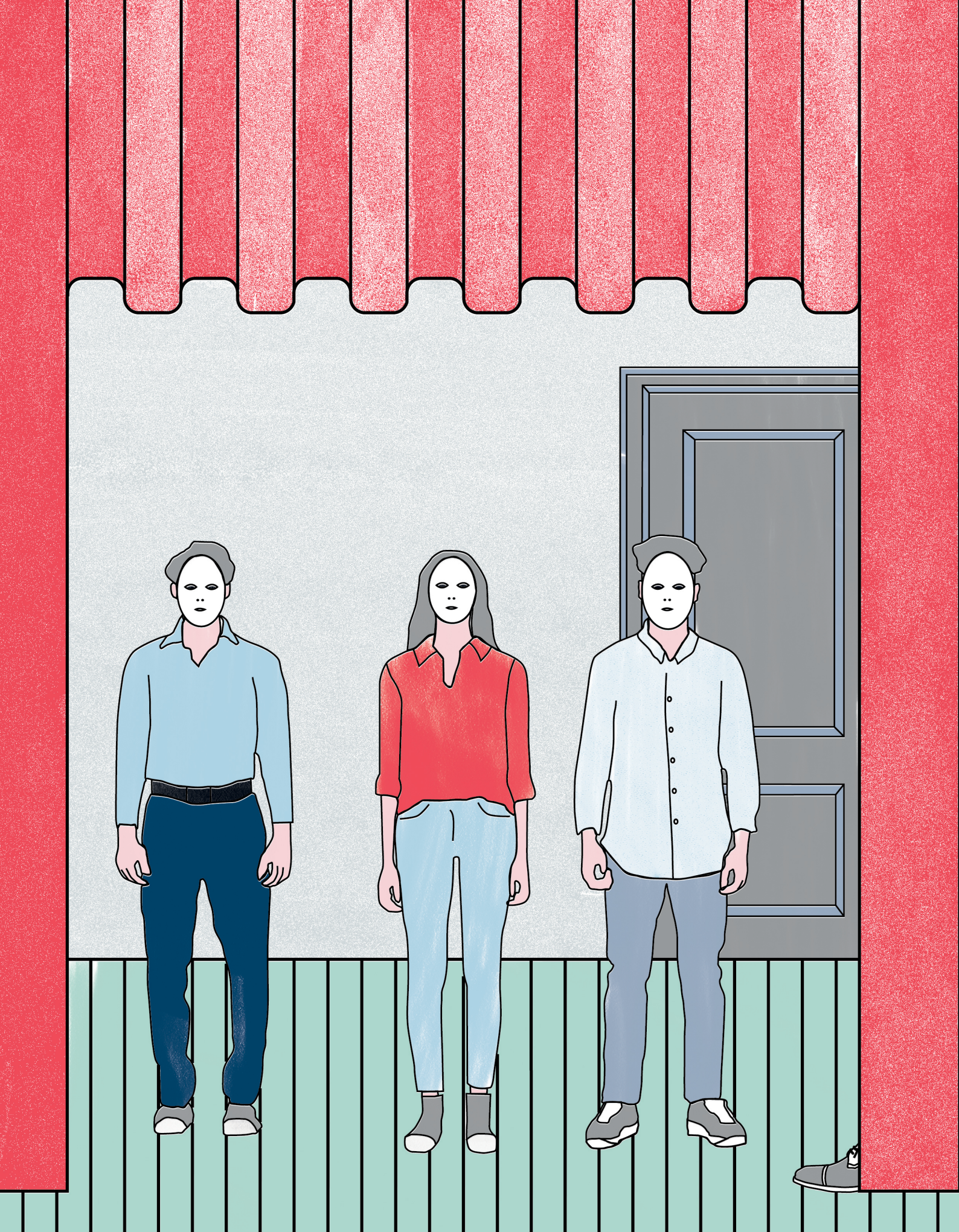
However, as in 2021, the main French victims of ransomware attacks observed by the agency in 2022 remain micro-businesses, SMEs and intermediate-sized enterprises (ETI), followed by local authorities and public health institutions.

In 2022, the main ransomware strains used in incidents reported to ANSSI were LockBit, Hive and BlackCat. While the number of ransomware attacks declined over 2022, their consequences remain highly significant, especially in critical sectors such as healthcare. In addition to the financial repercussions, this type of event can also impact patient treatment (28) and the confidentiality of their health data. During the night of 20-21 August 2022, the Centre Hospitalier Sud Francilien was the victim of a ransomware attack carried out by the Lockbit group. The unavailability of certain data and applications in the information system forced hospital services to function in a degraded mode. Furthermore, on 23 September 2022, 11 gigabytes of data exfiltrated during the attack were published on the cybercriminal group's website. The data leaked included medical and personal data relating to patients and hospital staff. A similar situation occurred a few months later at the Centre Hospitalier de Versailles (29).

Action taken by the hospital's technical teams, assisted by ANSSI and several service providers, enabled critical services to be restarted. The secure reconstruction of the IT system and a return to nominal operation will require long-term work.

Some governments have also fallen victim to ransomware attacks, including Peru and Costa Rica in April 2022. In May 2022, the Costa Rican government declared a state of emergency after a Conti ransomware attack (30). This was also the case for the government of Montenegro, which suffered a Cuba ransomware attack in August 2022 (31). The impact on the administration's operations and certain digital public services impelled the government, which feared a spread to certain critical infrastructures, to seek the help of the international community. To assist them in their investigations and the remediation of their key services, a team from ANSSI was deployed on-site in September.

Cybercriminal activity is not restricted to ransomware. Other types of activities, such as the resale of personal or banking information and more traditional scams, continued throughout the year. A change to phishing campaigns themes was also observed. Reports made to ANSSI show that the theme of taxes is gradually being superseded by that of healthcare, in particular by usurping the identity of Assurance Maladie.



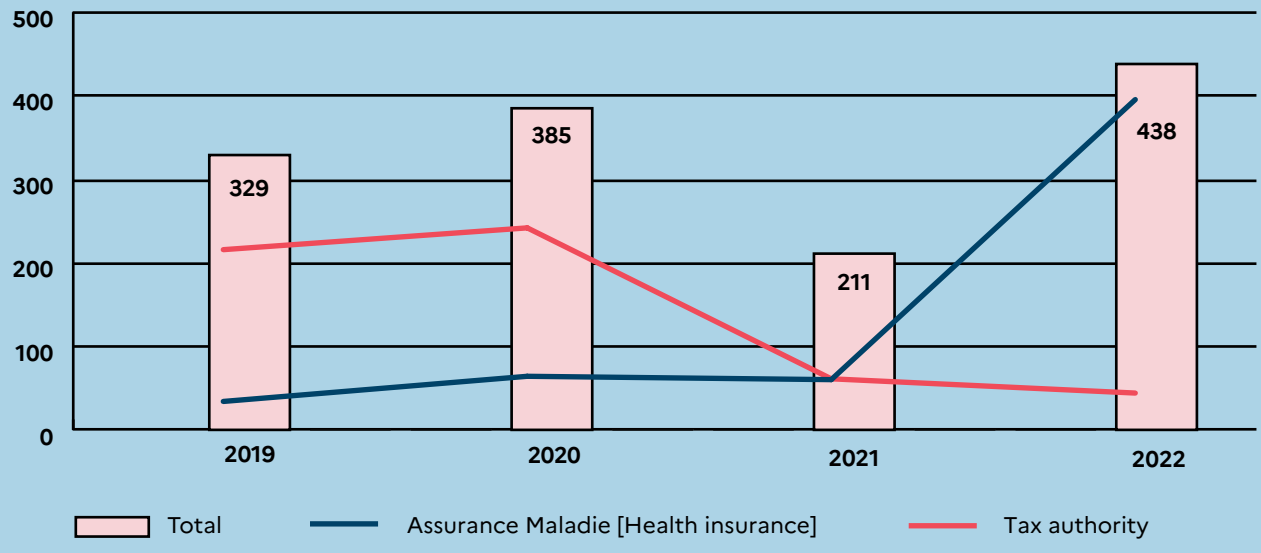
Attackers are thus seeking to exploit the health context and news related to the creation of "mon espace santé".[7]

Actors providing infrastructure services for hosting or distributing malicious services also continued their activities. These essential links in the cybercrime ecosystem have resisted law enforcement takedowns (32). While some services like Dridex and TrickBot seem to have disappeared (33), others such as QakBot or Emotet have resurfaced (34).

Particular scrutiny should be exercised on cryptomining activities. Cybercriminals have tailored their tactics, techniques and procedures (TTPs) to be less detectable, for example by consuming less computing power (CPU) on the compromised machines or by concealing traces of their activities. This is particularly relevant for the TeamTNT group, which announced the end of their operations in November 2021 (35). However, this modus operandi may inspire other groups. Although these activities are sometimes inconspicuous to the victims, they generate considerable revenue that could be reinvested by attackers to acquire new capabilities. One example is the particular care that members of the Kinsing group have taken to conceal their activities through various obfuscation techniques. This group is also known for automating the exploitation of vulnerabilities, such as Log4J[8] which was exploited two days after its disclosure (36).

7. Digital space proposed by Assurance Maladie and the Ministry of Health which is intended to become the interactive digital health record for all insured individuals.
8. Vulnerability discovered in the Apache Log4j logging library.

→ EVOLUTION OF THE THEME EXPLOITED IN PHISHING EMAILS SINCE 2019



B → CONTINUED ESPIONAGE ACTIVITIES IN FRANCE AND AROUND THE WORLD

As in 2021, ANSSI teams primarily dealt with the computer espionage threat in 2022. Thus, in 2022, 9 out of 19 cyber defence operations and major incidents handled by the agency involved intrusion sets openly associated with China. These repeated intrusions attest to an ongoing effort to breach the networks of strategic French entities.

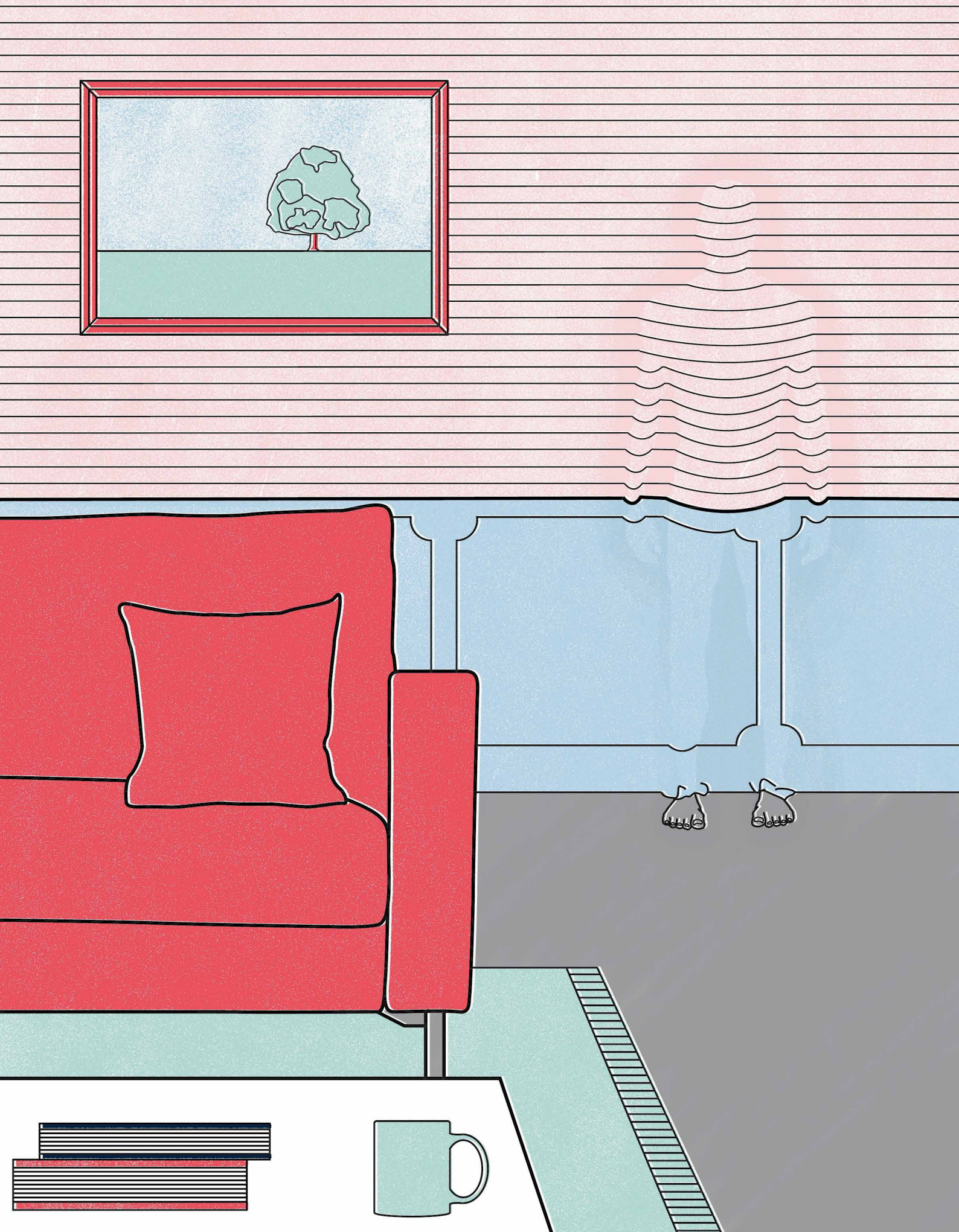
> Warning: the evolution of the number of major incidents and cyber defence operations does not illustrate the overall evolution of the threat level. These numbers are the result of the different levels of support provided by the ANSSI teams, which also rely on qualified security incident response service providers for the handling of incidents falling within their scope.

During the first half of 2022, ANSSI dealt with an in-depth compromise of the information system of a specialised supplier in the defence sector, whose know-how may elicit the interest of a foreign government. ANSSI's investigations confirmed and traced back the presence of a malicious actor in the information system to at least March 2021. Multiple instances of data exfiltration were detected over the same period. Remediation efforts were undertaken by the victim, in coordination with ANSSI, to ensure the removal of the attacker and enable the rebuilding of a secure infrastructure.

These various compromises also reflect a more sustainable evolution of the attackers' targeting scope, which is not restricted to a given organisation. Following the trend of supply chain attacks, malicious actors are more commonly targeting the companies, partners, subcontractors, service providers and umbrella organisations of their ultimate targets as part of long-term global espionage campaigns.

This observation is not limited to France. Various security vendors exposed several espionage campaigns targeting, for example, the Defence Industrial and Technological Base (DITB) in Russia (37) (38) (39).

The context of the Russian invasion of Ukraine has also been a key driver of strategic espionage campaigns against European countries and NATO members. Several intrusion sets were operated in such campaigns in 2022, such as Gamaredon (40), APT28 (41) and Turla (42). This targeting is likely to continue under the cloak of a particularly tense geopolitical context.



C → A THREAT OF DESTABILISATION TO MONITOR IN A SENSITIVE GEOPOLITICAL BACKDROP

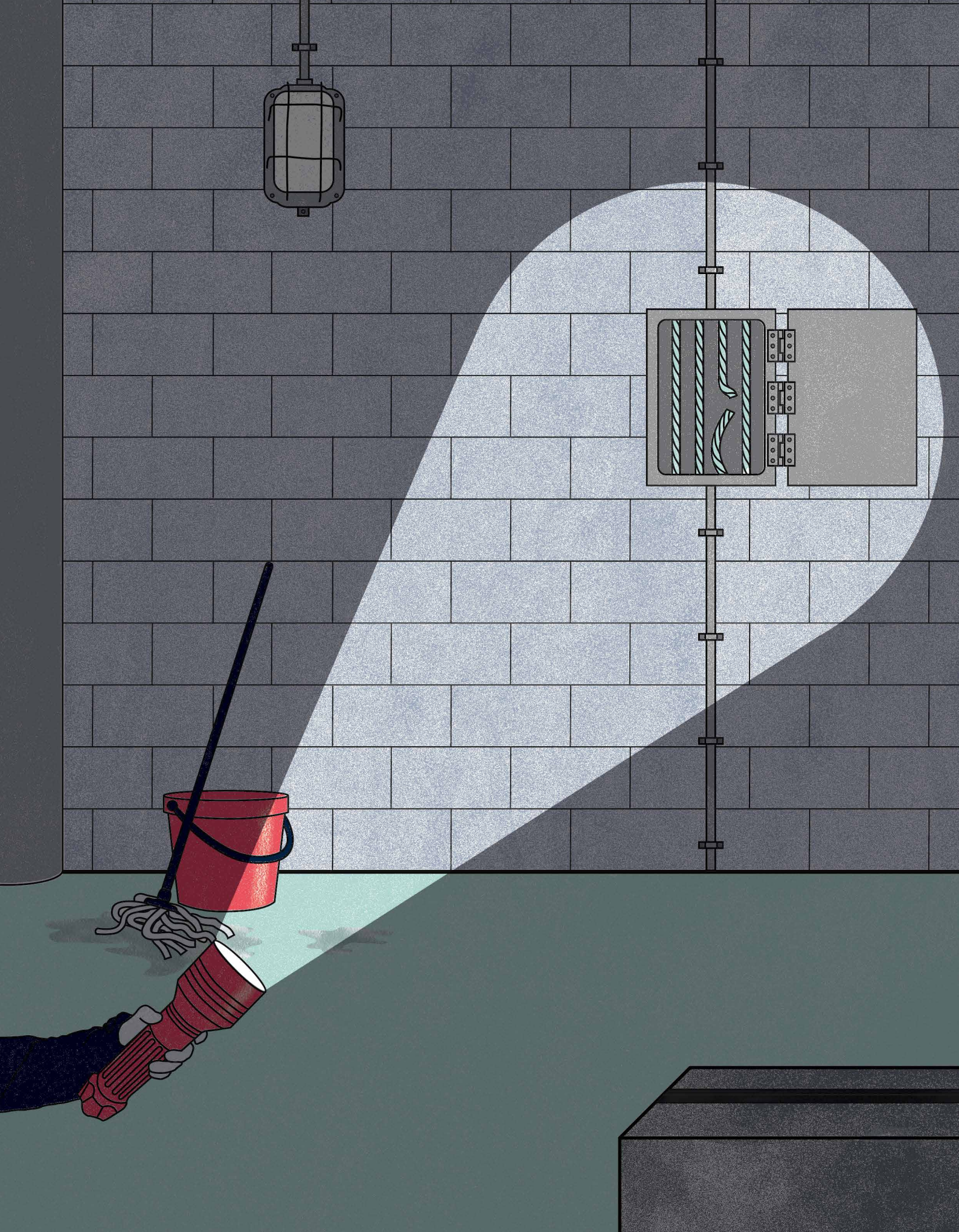
The Russian invasion of Ukraine has provided a propitious context for increasing the threat level of destabilisation in Europe. This increase has materialised in different forms. Distributed-denial-of-service attacks, computer sabotage and information operations relying on compromised information systems have been observed. While there have been numerous attempts at computer sabotage against critical infrastructure in this context, they have been relatively confined, geographically, to the Ukrainian battleground. There was little collateral damage, with the exception of the attack on the KA-SAT satellite communication network,[9] which had knock-on effects outside the Ukrainian borders.

This attack, carried out on the night of 23-24 February 2022 and attributed to Russia by the European Union and its Member States on 10 May 2022 (43), did not target the actual satellite itself – which remained fully functional – but the ground segment. Several tens of thousands of modems were cut off in Europe, many of them in France. Because of this satellite communication outage, several thousand French citizens living in dead zones were deprived of means of communication with emergency and rescue services. Public structures, as well as many companies that used this service, were also affected. It took up to several months to regain normal service for some French customers.

However, the economic fallout of the conflict, more specifically in the energy sector, call for particular vigilance on the part of all organisations in the sector – from vital operators to subcontractors, service providers and suppliers. According to cyber security vendor Dragos, intrusion sets Kamacite and Xenotime carried out reconnaissance activities against a liquefied natural gas terminal in the Netherlands (44). In view of past attacks using such intrusion sets, the threat of destabilisation through computer sabotage seems credible in this context.

The Russia-Ukraine conflict has also impelled an upsurge in hacktivism, particularly in Eastern Europe in support of both Russia and Ukraine. These hacktivist groups, such as KillNet (45), Squad303 (46) and the IT Army of Ukraine (6) carry out DDoS attacks, data exfiltration or website defacement, and sometimes leak data as part of information operations. Their targets are diverse but are mainly concentrated in Europe and North America. The media impact of their operations is often disproportionate to the skill level involved and the real impact on their targets' functioning. However, the consequences of this type of attack, which render certain resources unavailable or damage the reputation of institutions, should not be overlooked.

9. Operated by the American company Viasat.



3 → THE SAME WEAKNESSES ARE STILL BEING EXPLOITED

A → EXPLOITATION OF VULNERABILITIES

Many of the incidents observed and reported to ANSSI in 2022 were prompted by the exploitation of vulnerabilities with available patches by vendors and were the subject of advisories or alerts mentioned on the CERT-FR website. For the most critical ones, these publications were accompanied by reporting campaigns.

These vulnerabilities particularly affect common software used by numerous public and private organisations. Some of the most exploited vulnerabilities could have been patched since 2021.

Warning: This ranking only takes into account events for which ANSSI or an investigation provider was able to confirm, with a high degree of certainty, the exploitation of a vulnerability in 2022. The actual number of events where exploitation of one of these vulnerabilities is suspected (strongly assumed even) is considerably higher. The ranking below is indicative, given that the confirmed occurrences of the exploitation of vulnerabilities constitute a proportionally representative sample of the whole.

→ LIST OF THE MOST EXPLOITED VULNERABILITIES IN THE INCIDENTS HANDLED BY OR REPORTED TO ANSSI IN 2022.

ANSSI		
CVE	**PUBLISHER**	**CERT-FR REFERENCE**
CVE-2021-34473	MICROSOFT EXCHANGE	CERTFR-2021-ALE-017
CVE-2021-44228	APACHE	CERTFR-2021-ALE-022
CVE-2022-26134	CONFLUENCE	CERTFR-2022-ALE-006
CVE-2022-35914	GLPI	CERTFR-2022-ALE-010
CVE-2022-27925	ZIMBRA	CERTFR-2022-AVI-736
CVE-2022-41040 CVE-2022-41082	MICROSOFT EXCHANGE	CERTFR-2022-ALE-008
CVE-2021-26855	MICROSOFT EXCHANGE	CERTFR-2021-ALE-004
CVE-2021-31207 CVE-2021-34523	MICROSOFT EXCHANGE	CERTFR-2021-ALE-017
CVE-2022-22954	VMWARE WORKSPACEONE	CERTFR-2022-AVI-318
CVE-2021-34527	MICROSOFT WINDOWS	CERTFR-2021-ALE-014

ID	CVE-2021-34473	PUBLICATION DATE	14/07/2021
PUBLISHER	MICROSOFT	CVSS SCORE[10]	10.0

Multiple vulnerabilities were discovered in MICROSOFT EXCHANGE. They allow an attacker to **remotely run arbitrary code** and take control of the MICROSOFT EXCHANGE email server. The technique, dubbed *PROXYSHELL*, relies on the existence of several vulnerabilities which could have been patched since April and May 2021 (47).

10. The COMMON VULNERABILITY SCORING SYSTEM (CVSS) is a standardised system for assessing the criticality of vulnerabilities according to objective and measurable criteria. This assessment is comprised of three metric groups: Base, Temporal, and Environmental. The final score ranges from 0 to 10, with 10 being the most critical vulnerability. More information available at www.first.org/cvss.

ID	CVE-2021-44228	PUBLICATION DATE	10/12/2021
PUBLISHER	APACHE	CVSS SCORE	9.3

A vulnerability was discovered in the APACHE LOG4J logging library. This library is very often used in JAVA/J2EE application development projects. This vulnerability enables an attacker to **remotely run arbitrary code** on a system that uses the LOG4J library to log events (48).

ID	CVE-2022-26134	PUBLICATION DATE	03/06/2022
PUBLISHER	ATLASSIAN	CVSS SCORE	7.5

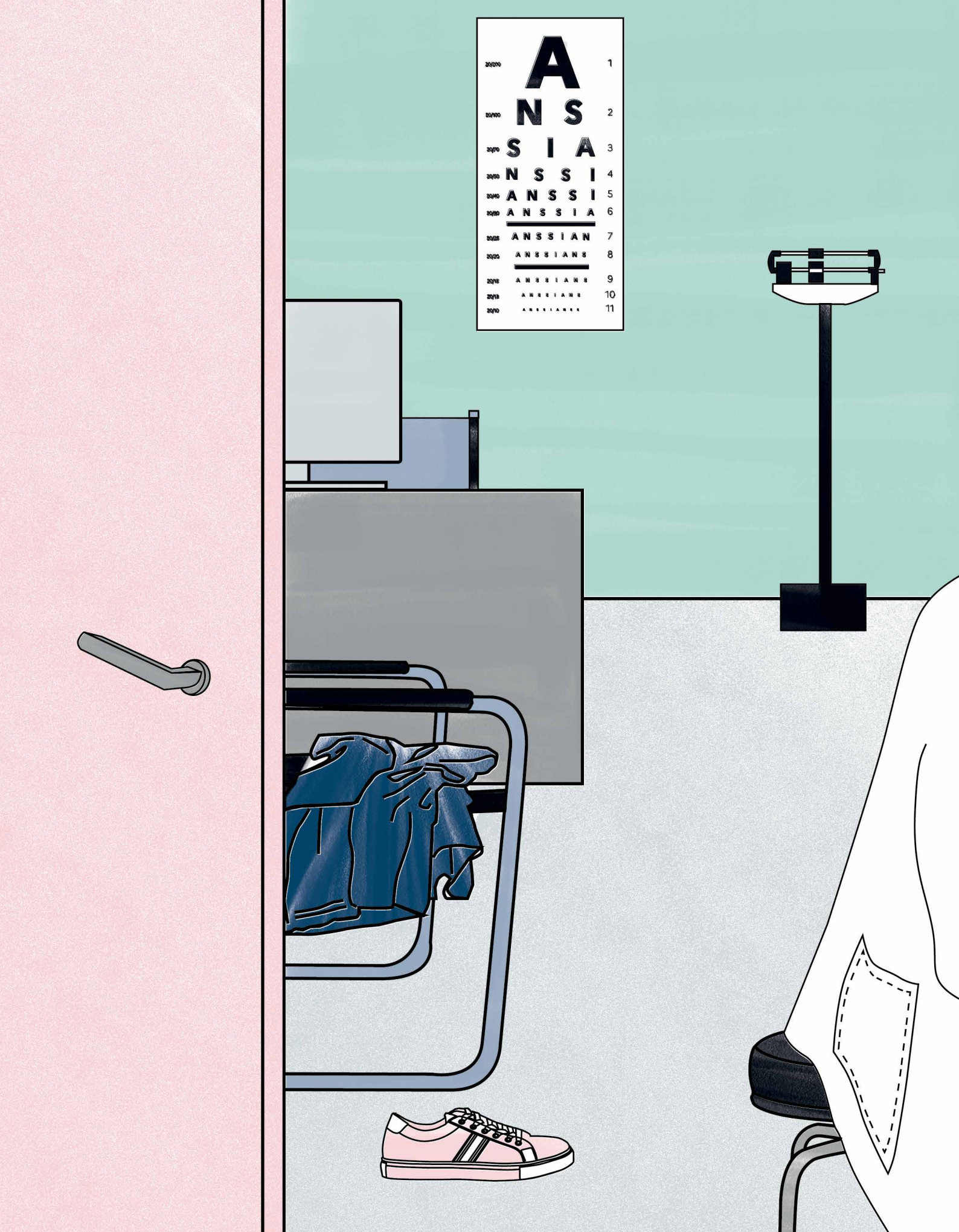
A vulnerability was discovered in ATLASSIAN CONFLUENCE. It allows an unauthenticated attacker to **remotely run arbitrary code**. This vulnerability is **exploited by attackers** to deploy various backdoors (web shells) to maintain their presence on compromised servers (49).

ID	CVE-2022-35914	PUBLICATION DATE	19/09/2022
PUBLISHER	GLPI	CVSS SCORE	9.8

Multiple vulnerabilities were discovered in the GLPI (GESTIONNAIRE LIBRE DE PARC INFORMATIQUE - open source service management software) solution. In particular, this vulnerability enables an attacker to **remotely run arbitrary code** and **bypass security measures**. The identified vulnerability affects a third-party library - *HTMLAWED* - embedded in GLPI (50).

ID	CVE-2022-27925	PUBLICATION DATE	21/04/2022
PUBLISHER	ZIMBRA	CVSS SCORE	7.2

Multiple vulnerabilities were discovered in ZIMBRA. The vulnerability referenced as CVE-2022-27925 allows an attacker to upload arbitrary files to the system and thus **breach the confidentiality and integrity of data** (51).


A
N S
S I A
N S S I
A N S S I
A N S S I A
A N S S I A N
A N S S I A N S
A N S S I A N S
A N S S I A N S
A N S S I A N S

B → THE EXPLOITATION OF NEW DIGITAL USES FOR MALICIOUS ENDS

New technologies and the new uses they entail alter, and tend to expand, the users' attack surface. ANSSI has thus observed that virtualisation solutions are increasingly being targeted. These solutions are particularly popular because of the versatility and flexibility they provide to the management of information systems. However, in addition to the detection challenges associated with these environments, once compromised, attackers can maintain persistent access to all virtual machines managed by the hypervisor.[11] In September 2022, vendors Mandiant and VMware (52) reported that attackers were specifically targeting the vSphere virtualisation solution for espionage purposes, to deploy two backdoors named "VirtualPita" and "VirtualPie". Targeting hypervisors is also particularly interesting for cybercriminals operating ransomware, such as the Conti group (53).

This assessment is shared by the agency, which dealt with several incidents involving the compromise of VMWare hypervisors in 2022. On multiple separate occasions, state-sponsored attackers compromised a vSphere environment by exploiting a vulnerability. This access, achieved either through a vCenter console, or by directly targeting an ESXi hypervisor, allowed them to take control of all the virtual machines hosted in the environment. Cybercriminal actors have also displayed an interest for these solutions without exploiting the same vulnerabilities. As virtualisation solutions are frequently included in the Active Directory, ransomware operators target them during encryption to quickly render a large number of machines unusable. To support victims, ANSSI has made a tool called DFIR4vSphere available on the agency's GitHub, allowing them to collect logs and artefacts on a vSphere (54) environment to conduct forensic analysis.

In addition, cloud computing and more generally the outsourcing of IT services to managed service providers (MSP) also contribute to the expansion of the organisations' potential attack surface.

Cloud infrastructures can be exploited for financial gain, such as cryptocurrency mining, or integrated into the attackers' infrastructure. They can also be an effective attack vector.

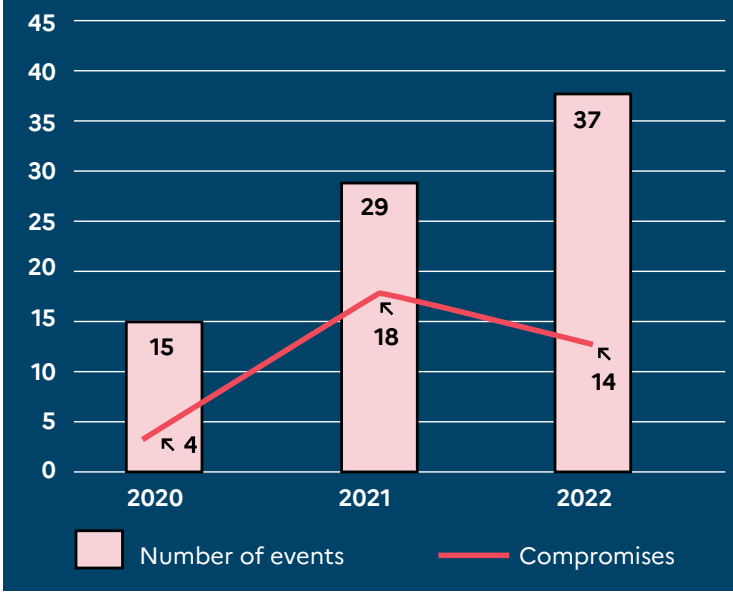
The deployment of Single Sign-On (SSO) solutions and the widespread use of the cloud are posing an increasing threat to session cookies. These cookies, used for authentication, are a prime target for several attacker profiles. They constitute an effective attack vector or lever for lateralisation by allowing attackers to bypass authentication, including multi-factor authentication. They are regularly collected by cybercriminals using stealers placed in their victims' systems or during phishing operations. These cookies, associated with logins, provide access

to online systems and applications such as identity management platforms. Okta, one such platform, fell victim to the LAPSUS$ group in March 2022 (55). The attack originated from the compromised account of a Sitel engineer, Okta's service provider. According to the latest information, the attackers gained access to Sitel's network through its subsidiary Sykes (56). This attack illustrates the domino effect that attacks stemming from a service provider or subsidiary can have.

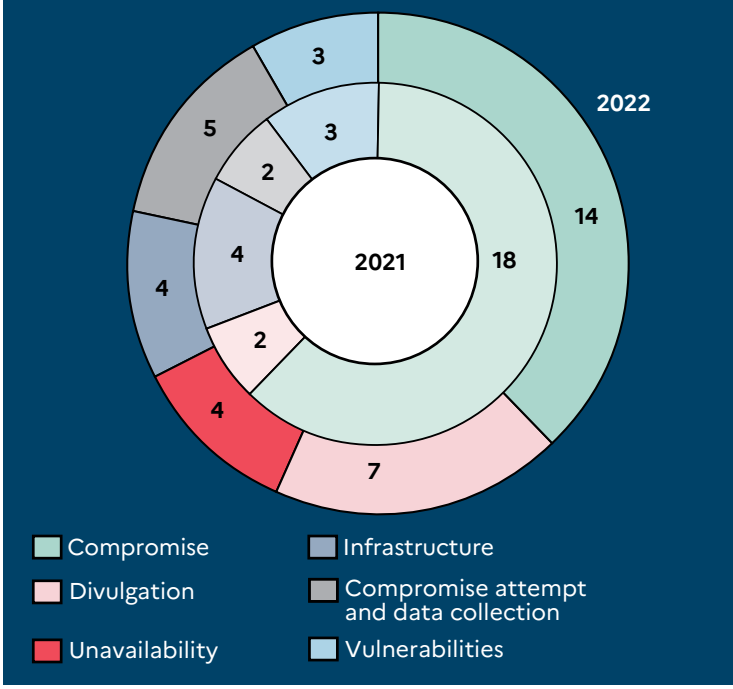
Recommendations on the security policy related to authenticated sessions and information systems hardening are available on the CERT-FR website (57) and in the guides published by ANSSI.

Digital supply chain attacks decreased in 2022. The agency also observed this decline. The incidents handled by or reported to ANSSI show that the number of cases of MSP compromise dropped slightly between 2021 and 2022. However, attacks targeting the supply chain – whether they involve a service provider such as a MSP or a software distribution chain – continue to pose a systemic risk, as illustrated by the abovementioned case of Okta or that of the Rust development community (7) disclosed in May 2022.

→ EVOLUTION OF EVENTS AFFECTING MSPS SINCE 2020.



→ COMPARISON OF THE TYPES OF INCIDENTS AFFECTING MSPS IN 2021 AND 2022.



11. A software component that acts as an interface between virtual machines (VMs) and the host server. The hypervisor controls access to host machine resources and is responsible for partitioning VMs. Exploiting hypervisor vulnerabilities can allow an attacker to compromise the entire host and the VMs it hosts.

C → THE OPPORTUNITIES PROVIDED BY DATA LEAKS

Whether they are the result of ransomware attacks (58) or negligence (59), sold by cybercriminals (60) or exposed as part of ideologically or politically motivated information operations (61), data leaks constitute an opportunity for attackers.

Such data can be reused to carry out credible phishing campaigns. When data consists of logins and passwords, it can be reused directly by attackers. Enabling multi-factor authentication goes a long way towards preventing this. As with reputation monitoring, it is advised to watch out for data leaks concerning one's organisation or partners, and that recommendations relating to multi-factor authentication and passwords (available on the ANSSI website) be applied.

4 → CONCLUSION

→ Despite the Russia-Ukraine conflict, the cyber threat has not significantly changed between 2021 and 2022. It remains at a high level with regard to espionage in the public and private sphere.

The evolution of the conflict and the ensuing economic tensions, particularly in the energy sector, call for vigilance by all organisations. Given the nature of past cyber attacks in the context of this conflict and the involvement of European countries, the threat of destabilisation and pre-positioning activities is deemed credible. Attackers may claim responsibility for these destabilising efforts that can take the form of DDoS attacks or orchestrated data leaks, or even computer sabotage attacks.

Cybercrime, and more specifically ransomware attacks, remained a sustainable threat with a noticeable increase in activity at the end of 2022. Moreover, other types of cybercriminal activity – such as cryptomining – should not be overlooked. Stealthier than ever before, it generates significant funds that can be reinvested by malicious actors to acquire new capabilities.

While the French presidential and legislative elections of 2022 were not subjected to major computer attacks, other upcoming events – such as the Rugby World Cup in 2023 and the Paris Olympic and Paralympic Games in 2024 – will provide various profiles of attackers with opportunities, whether their motives are financial gain, espionage or destabilisation.

The rigorous application of an update policy and ANSSI's Guideline for a Healthy Information System, along with regular user awareness training and the development of incident detection and handling capabilities, help to protect against the most common threats.

Recent legislative developments, such as the new Network and Information System Security Directive (NIS2) adopted by the European Parliament on 10 November 2022, which will be transposed into French law by September 2024, will strengthen the agency's supervisory powers by extending its scope to a larger number of economic sectors and public and private players. This directive, which covers the digitalisation of supply chains, should also enable to set tighter security requirements for companies, increase the maturity level of organisations and thus help reduce the risks of indirect attacks.

ANNEX →
BIBLIOGRAPHY

[1]
MINISTÈRE DES AFFAIRES ÉTRANGÈRES ET EUROPÉENNES.
8 September 2022.
URL: https://www.diplomatie.gouv.fr/fr/dossiers-pays/albanie/evenements/article/albanie-q-r-extrait-du-point-de-presse-08-09-22

[2]
ASSOCIATED PRESS.
Albania Cuts Diplomatic Ties with Iran over July Cyberattack. 7 September 2022.
URL: https://apnews.com/article/nato-technology-iran-middle-east-6be153b291f42bd549d5ecce5941c32a

[3]
BLACKBERRY.
Dirty Deeds Done Dirt Cheap: Russian RAT Offers Backdoor Bargains.
5 September 2022.
URL: https://blogs.blackberry.com/en/2022/05/dirty-deeds-done-dirt-cheap-russian-rat-offers-backdoor-bargains

[4]
CERT-UA.
Масована кібератака на медійні організації України з використанням шкідливої програми CrescentImp (CERT-UA#4797). 6 June 2022.
URL: https://cert.gov.ua/article/160530

[5]
FORTINET.
Ukraine Targeted by Dark Crystal RAT (DCRat). 27 June 2022.
URL: https://www.fortinet.com/blog/threat-research/ukraine-targeted-by-dark-crystal-rat

[6]
THE RECORD.
Russia or Ukraine: Hacking Groups Take Sides. 25 February 2022.
URL: https://therecord.media/russia-or-ukraine-hacking-groups-take-sides/

[7]
SENTINEL ONE.
CrateDepression Rust Supply-chain Attack Infects Cloud CI Pipelines with Go Malware. 19 May 2022.
URL: https://www.sentinelone.com/labs/cratedepression-rust-supply-chain-attack-infects-cloud-ci-pipelines-with-go-malware/

[8]
MICROSOFT SECURITY BLOG.
Looking for the 'Sliver' lining: Hunting for merging command-and-control frameworks. 24 August 2022.
URL: https://www.microsoft.com/en-us/security/blog/2022/08/24/looking-for-the-sliver-lining-hunting-for-emerging-command-and-control-frameworks/

[9]
CERT-FR.
APT31: Pakdoor, Synthèse technique.
15 December 2021.
URL: https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-012b.pdf

[10]
MICROSFOT SECURITY BLOG.
Uncovering Trickbot's use of IoT devices in command-and-control infrastructure.
16 March 2022.
URL: https://www.microsoft.com/en-us/security/blog/2022/03/16/uncovering-trickbots-use-of-iot-devices-in-command-and-control-infrastructure/

[11]
INTELLIGENCE ONLINE.
RCS Lab Leads new owner Cy4gate's Europen growth goals. 15 April 2022.
URL: https://www.intelligenceonline.com/surveillance--interception/2022/04/15/rcs-lab-leads-new-owner-cy4gate-s-european-growth-goals,109768275-art

[12]
LOOKOUT.
Lookout Découverte du logiciel espion Hermit déployé au Kazakhstan.
16 June 2022.
URL: https://fr.lookout.com/blog/hermit-spyware-discovery

[13]
GOOGLE THREAT ANALYSIS GROUP.
Spyware vendor targets users in Italy and Kazakhstan. 23 June 2022.
URL: https://blog.google/threat-analysis-group/italian-spyware-vendor-targets-users-in-italy-and-kazakhstan/

[14]
PEGA.
PEGA: Findings. *Parlement européen*.
14 November 2022.
URL: https://www.europarl.europa.eu/committees/en/pega-findings/product-details/20221114CAN67684

[15]
CITIZEN LAB.
Dark Basin Uncovering a Massive Hack-For-Hire Operation. 9 June 2020.
URL: https://citizenlab.ca/2020/06/dark-basin-uncovering-a-massive-hack-for-hire-operation/

[16]
THE BUREAU OF INVESTIGATIVE JOURNALISM.
How Qatar hacked the World Cup.
URL: https://www.thebureauinvestigates.com/stories/2022-11-05/how-qatar-hacked-the-world-cup

[17]
MEDIAPART.
Le Qatar soupçonné d'avoir ciblé Mediapart dans une opération mondiale de hacking. 6 November 2022.
URL: https://www.mediapart.fr/journal/international/061122/le-qatar-soupconne-d-avoir-cible-mediapart-dans-une-operation-mondiale-de-hacking

[18]
ZDNET.
Ransomware has gone down because sanctions against Russia are making life harder for attackers. 10 May 2022.
URL: https://www.zdnet.com/article/ransomware-has-gone-down-because-sanctions-against-russia-are-making-life-harder-for-attackers/

[19]
MARIANNE.
Face à l'explosion des cyberattaques, la solution contestée du gouvernement.
27 September 2022.
URL: https://www.marianne.net/societe/big-brother/face-a-lexplosion-des-cyberattaques-la-solution-contestee-du-gouvernement

[20]
PARIS NORMANDIE.
Le Département de Seine-Maritime touché par une cyberattaque : les services publics « dégradés ».
10 October 2022.
URL: https://www.paris-normandie.fr/id349866/article/2022-10-10/le-departement-de-seine-maritime-touche-par-une-cyberattaque-les-services

[21]
VILLE DE CHAVILLE.
La Ville de Chaville victime d'une cyberattaque. 17 October 2022
URL: https://www.ville-chaville.fr/actualites-evenements/toute-l-actualite-77/la-ville-de-chaville-victime-dune-cyberattaque-5426.html?cHash=d24693b307b60aabf87ac7b4a08e4e4d

[22]
MIDI LIBRE.
Cyberattaque à Frontignan : les services de la mairie piratés, les hackeurs demandent une rançon. 31 October 2022.
URL: https://www.midilibre.fr/2022/10/31/la-mairie-de-frontignan-victime-dune-cyberattaque-et-dune-demande-de-rancon-10774268.php

[23]
20 MINUTES.
Essonne : La mairie de Brunoy visée par une attaque au rançongiciel.
2 November 2022.
URL: https://www.20minutes.fr/faits_divers/4008154-20221102-essonne-mairie-brunoy-visee-attaque-rancongiciel

[24]
LE MONDE.
Cyberattaque : une rançon de 10 millions de dollars réclamée au département de Seine-et-Marne. 17 November 2022.
URL: https://www.lemonde.fr/societe/article/2022/11/17/cyberattaque-une-rancon-de-10-millions-de-dollars-reclamee-au-departement-de-seine-et-marne_6150336_3224.html

[25]
CYBERSCOOP.
Latin America governments are prime targets for ransomware due to lack of resources, analysis argues. 16 June 2022.
URL: https://www.cyberscoop.com/latin-america-ransomware-recorded-future/

[26]
CNN.
Cyber Command head says US has carried out a 'surge' to address ransomware attacks. 3 November 2021.
URL: https://edition.cnn.com/2021/11/03/politics/nakasone-ransomware-surge/index.html

[27]
BREACHQUEST.
The Conti Leaks | Insight into a Ransomware Unicorn. 9 March 2022.
URL: https://www.breachquest.com/blog/conti-leaks-insight-into-a-ransomware-unicorn/

[28]
TIC SANTÉ.
Le coût total de la cyberattaque du CH de Dax s'est élevé à 2,3 millions d'euros (RSSI). 8 April 2022.
URL: https://www.ticsante.com/story?ID=6141

[29]
FRANCEINFO.
L'hôpital André-Mignot du centre hospitalier de Versailles victime d'une cyberattaque. 4 December 2022.
URL: https://www.francetvinfo.fr/internet/securite-sur-internet/cyberattaques/info-franceinfo-l-hopital-andre-mignot-du-centre-hospitalier-de-versailles-victime-d-une-cyberattaque_5522235.html

[30]
BLEEPING COMPUTER.
Costa Rica declares national emergency after Conti ransomware attacks.
8 May 2022.
URL: https://www.bleepingcomputer.com/news/security/costa-rica-declares-national-emergency-after-conti-ransomware-attacks/

[31]
LE MONDE.
Le Monténégro, visé par une cyberattaque, appelle à l'aide internationale et accuse la Russie. 27 August 2022.
URL: https://www.lemonde.fr/international/article/2022/08/27/le-montenegro-vise-par-une-cyberattaque-appelle-a-l-aide-internationale-et-accuse-la-russie_6139205_3210.html

[32]
EUROPOL.
Internet Organised Crime Threat Assessment (IOCTA) 2021. Publications Office of the European Union, Luxembourg, 2021.
URL: https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf

[33]
MALWAREBYTES LABS.
TrickBot takes down server infrastructure after months of inactivity.
28 February 2022.
URL: https://www.malwarebytes.com/blog/news/2022/02/trickbot-takes-down-server-infrastructure-after-months-of-inactivity

[34]
BLEEPING COMPUTER.
Emotet botnet starts blasting malware again after 4 month break.
2 November 2022.
URL: https://www.bleepingcomputer.com/news/security/emotet-botnet-starts-blasting-malware-again-after-4-month-break/

[35]
TREND MICRO.
Probing the Activities of Cloud-Based Cryptocurrency-Mining Groups.
29 March 2022.
URL: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/probing-the-activities-of-cloud-based-cryptocurrency-mining-groups

[36]
JUNIPER NETWORKS.
Log4j Attack Payloads In The Wild.
17 December 2021.
URL: https://blogs.juniper.net/en-us/security/in-the-wild-log4j-attack-payloads

[37]
THE NEW YORK TIMES.
Chinese Hackers Tried to Steal Russian Defense Data, Report Says.
19 May 2022.
URL: https://www.nytimes.com/2022/05/19/world/asia/china-hackers-russia.html

[38]
SECURITY PARROT.
Chinese hackers attack defense companies and government agencies in Russia and Eastern Europe. 8 August 2022.
URL: https://securityparrot.com/news/chinese-hackers-attack-defense-companies-and-government-agencies-in-russia-and-eastern-europe/

[39]
POSITIVE TECHNOLOGIES.
APT31 new dropper. Target destinations: Mongolia, Russia, the U.S., and elsewhere.
3 August 2022.
URL: https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/apt31-new-attacks/

[40]
CERT-UA.
Кібератака групи UAC-0010 (Armageddon) на державні інституції країн Європейського Союзу (CERT-UA#4334).
CERT-UA. 4 April 2022.
URL: https://cert.gov.ua/article/39086

[41]
CLUSTER25 THREAT INTEL TEAM.
In the footsteps of the Fancy Bear: PowerPoint mouse-over event abused to deliver Graphite implants. *DuskRise*.
23 September 2022.
URL: https://blog.cluster25.duskrise.com/2022/09/23/in-the-footsteps-of-the-fancy-bear-powerpoint-graphite/

[42]
GOOGLE THREAT ANALYSIS GROUP.
Update on cyber activity in Eastern Europe. 3 May 2022.
URL: https://blog.google/threat-analysis-group/update-on-cyber-activity-in-eastern-europe/

[43]
COUNCIL OF THE EUROPEAN UNION.
Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union. 10 May 2022.
URL: https://www.consilium.europa.eu/en/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union/

[44]
NL TIMES.
Russian hackers targeting Dutch gas terminal: report. 25 November 2022.
URL: https://nltimes.nl/2022/11/25/russian-hackers-targeting-dutch-gas-terminal-report

[45]
CBS NEWS.
U.S. airport websites knocked offline in apparent pro-Russia hacking attack. 10 October 2022.
URL: https://www.cbsnews.com/news/airport-websites-hacked-pro-russia-ddos-attack/

[46]
THE RECORD.
'We are unstoppable': How a team of Polish programmers built a digital tool to evade Russian censorship. 17 March 2022.
URL: https://therecord.media/we-are-unstoppable-how-a-team-of-polish-programmers-built-a-digital-tool-to-evade-russian-censorship/

[47]
CERT-FR.
Multiples vulnérabilités dans Microsoft Exchange. 27 August 2021.
URL: https://www.cert.ssi.gouv.fr/alerte/CERTFR-2021-ALE-017/

[48]
CERT-FR.
Vulnérabilité dans Apache Log4j. 10 December 2021.
URL: https://www.cert.ssi.gouv.fr/alerte/CERTFR-2021-ALE-022/

[49]
CERT-FR.
Vulnérabilité dans Atlassian Confluence. 6 June 2022.
URL: https://www.cert.ssi.gouv.fr/alerte/CERTFR-2022-ALE-006/

[50]
CERT-FR.
Multiples vulnérabilités dans GLPI. 7 October 2022.
URL: https://www.cert.ssi.gouv.fr/alerte/CERTFR-2022-ALE-010/

[51]
CERT-FR.
Multiples vulnérabilités dans Zimbra. 31 March 2022.
URL: https://www.cert.ssi.gouv.fr/avis/CERTFR-2022-AVI-291/

[52]
MANDIANT.
Bad VIB(E)s Part One: Investigating Novel Malware Persistence Within ESXi Hypervisors. 29 September 2022.
URL: https://www.mandiant.com/resources/blog/esxi-hypervisors-malware-persistence

[53]
TRELLIX.
Conti Group Targets ESXi Hypervisors With its Linux Variant. 20 April 2022.
URL: https://www.trellix.com/en-us/about/newsroom/stories/research/conti-group-targets-esxi-hypervisors-with-its-linux-variant.html

[54]
CERT-FR.
DFIR4vSphere: Investigation numérique sur la solution de virtualisation VMWare vSphere. 22 June 2022.
https://www.cert.ssi.gouv.fr/actualite/CERTFR-2022-ACT-027/

[55]
OKTA.
Frequently Asked Questions Regarding the January 2022 Compromise. 26 April 2022.
URL: https://support.okta.com/help/s/article/Frequently-Asked-Questions-Regarding-January-2022-Compromise?language=en_US

[56]
WIRED.
Leaked Details of the Lapsus$ Hack Make Okta's Slow Response Look More Bizarre. 29 March 2022.
URL: https://www.wired.com/story/lapsus-okta-hack-sitel-leak/

[57]
CERT-FR.
Menaces liées aux vols de cookies et contre-mesures. 25 May 2022.
URL: https://www.cert.ssi.gouv.fr/cti/CERTFR-2022-CTI-005

[58]
RAPID7.
New Report Shows What Data Is Most at Risk to (and Prized by) Ransomware Attackers. 6 June 2022.
URL: https://www.rapid7.com/blog/post/2022/06/16/new-report-shows-what-data-is-most-at-risk-to-and-prized-by-ransomware-attackers/

[59]
GROUP-IB.
Thousands of IDs exposed in yet another data breach in Brazil. 16 June 2022.
URL: https://blog.group-ib.com/brazil-exposed-db

[60]
BLEEPING COMPUTER.
14 November 2022.
URL: https://www.bleepingcomputer.com/news/security/whoosh-confirms-data-breach-after-hackers-sell-72m-user-records/

[61]
SOCRADAR.
Hacktivist Group Black Reward Leaked Iran's Nuclear Program Secrets. 4 November 2022.
URL: https://socradar.io/hacktivist-group-black-reward-leaked-iran-nuclear-program-secrets/

[62]
TREND MICRO.
Credential Stealer Targets US, Canadian Bank Customers. 17 December 2020.
URL: https://www.trendmicro.com/en_us/research/20/l/stealth-credential-stealer-targets-us-canadian-bank-customers.html

[63]
PROOFPOINT.
Asylum Ambuscade: State Actor Uses Compromised PRivate Ukrainian Military Emails to Target European Governments and Refugee Movement. 1 March 2022.
URL: https://www.proofpoint.com/us/blog/threat-insight/asylum-ambuscade-state-actor-uses-compromised-private-ukrainian-military-emails

[64]
STATE SERVICE OF SPECIAL COMMUNICATIONS AND INFORMATION PROTECTION OF UKRAINE.
Who is behind the Cyberattacks on Ukraine's Critical Information Infrastructure: Statistics for March 15-22. 25 March 2022.
URL: https://cip.gov.ua/en/news/khto-stoyit-za-kiberatakami-na-ukrayinsku-kritichnu-informaciinu-infrastrukturu-statistika-15-22-bereznya

CYBER THREAT OVERVIEW 2022 CREDITS

CYBER
THREAT
OVERVIEW
2022

Published by the French National
Cyber Security Agency (ANSSI)

Artistic direction, layout and
illustrations by Cercle Studio
(www.cerclestudio.com)

LEGAL DEPOSIT
January 2023

Paperback ISBN: 978-2-11-167130-0
Digital ISBN: 978-2-11-167131-7

FRENCH NATIONAL
CYBER SECURITY
AGENCY

ANSSI – 51 boulevard
de la Tour-Maubourg
75700 PARIS 07 SP

www.ssi.gouv.fr
www.cert.ssi.gouv.fr
cert-fr@ssi.gouv.fr