TLP:WHITE

CYBER THREAT OVERVIEW 2021

1.9.1

March 9, 2022

TLP:WHITE

Table of contents

EXECUTIVE SUMMARY

In this Cyber threat overview, the ANSSI looks back at **the major trends** that have marked the cyber landscape in **2020-2021** and proposes **short-term prospects for change**. These trends are part of a continuing increase in the threat level. This is backed up by the fact that the ANSSI was made aware of 1082 proven intrusions into information systems in 2021, compared with 786 in 2020. This represents a 37 % increase in proven intrusions during the year. This increase can be explained by the developing and **constantly improving the capacities of malicious actors** whose main objectives remain **financial gain, espionage and destabilisation**. These actors have been able to seize upon **multiple opportunities offered by the widespread use of digital technologies, often without the necessary levels of control**. Particular vigilance is therefore required in the context of major events in France such as the French presidency of the European Union, the presidential and legislative elections in 2022 and the Paris 2024 Olympic Games, which all represent contextual opportunities for attackers to exploit.

The evolution of the cyber crime ecosystem is marked by constantly increasing levels of professionalism and specialisation, both a cause and a consequence of the maturity and financial gains acquired by its actors. Ransomware-as-a-Service (*RaaS*) and unscrupulous companies offering hosting capacity to malicious actors (*Bullet Proof Hosters*) are a perfect example of this. Cyber criminals are also adopting similar intrusion sets to government-backed actors, carefully planning their operations, remaining on their victims' networks for long periods of time in search of resources of interest and sometimes exploiting unknown *0-day* vulnerabilities. Furthermore, the availability of such ready-made malicious tools and services could benefit other types of attackers, especially those ideologically motivated, such as hacktivists.

State-sponsored attackers also draw on cyber crime methods by appropriating codes and tools traditionally used by cyber crime attackers such as ransomware or phishing techniques. To hide themselves, they exploit legitimate tools on the victims' networks, thus avoiding detection (using the *living off the land - LotL* technique). This **porosity between different attacker profiles** makes it difficult to characterise malicious activities.

The building of offensive capacities by private companies such as the NSO Group makes sometimes cutting-edge capacities available to actors who cannot afford to build them or who wish to maintain plausible deniability. This provision of advanced and sometimes highly sophisticated capacities contributes to the general increase in the threat level by multiplying its sources and encouraging the uninhibited use of cyber attacks.

While attacks for profit have occupied the media scene, they should not overshadow espionage campaigns, which are inherently less visible, and those carried out for the purpose of computer sabotage.

Computer espionage remains **the main objective pursued** by state attackers and constitutes the main activity dealt with in the context of cyber defence operations conducted by the ANSSI. In some cases, computer espionage can be **facilitated by the implementation or misuse of legal mechanisms**.

The targeting of critical infrastructure also remains a **major concern**. Several cyber criminals have targeted hospitals in France using ransomware that paralyses the activity of vital structures. The increase in dismantling operations, the arrests of cyber crime networks through international cooperation and the stance taken by several states, particularly the United States, seem to have had an effect on the targeting of critical infrastructure. Cyber criminals could thus avoid deliberately compromising this type of structure in the near future. However, their targeting by actors reputed to be state-owned is likely to continue in part in the event of strong geopolitical tensions, such as between Israel and Iran, where various critical infrastructure has been the subject of computer attacks (water and energy supplies). French entities located abroad could thus be collateral victims of this type of operation.

Finally, **computer attacks used to influence and destabilise** are to be anticipated, particularly in the run-up to major events in France. An increasing number of information operations in fact rely on IT systems being compromised to exfiltrate documents and gain initial access, such as with the "Ghostwriter" campaign. This campaign has been attributed to Russia by many ANSSI partners and has affected Poland and Germany, among others, in 2021.

Whether in the context of extortion, espionage, influence or destabilisation operations, attackers take full advantage of the fragility of digital infrastructures.

2020-2021 has therefore seen an **explosion in the number of *0-day*** vulnerabilities exploited, mainly by state actors, but also by a few cyber criminal groups, notably during the 2 July 2021 attack against the remote administration solution provider Kaseya. This last example also reminds us that special attention should be paid to **attacks targeting the supply chain**, a method particularly popular with attackers. This trend presents risks of spreading rapidly from a targeted software editor or digital services company, with the risk of a cascade effect in terms of compromises. Attackers have also been able to take advantage of new **digital uses, often without the necessary levels of control, such as the cloud** for profit and espionage purposes.

The increase in computer attacks has led to an explosion in data leaks, particularly personal data. Whether from disclosures by ransomware operators, destabilisation operations or the resale of information by cyber criminals, this data feeds a vicious circle. Indeed, it facilitates many computer attacks by providing entry points for attackers.

Rapid spreading to an entire information system can be hindered by two main defensive measures:

- system administrator protection, especially for Active Directory domains. Their administration accounts should ideally never be used for web browsing, email or office purposes;
- strict network segmentation, limiting the possibilities of flows between zones dedicated to different uses (for example, according to business lines, geographical areas or type of machines).

The use of password managers, the widespread activation of multi-factor authentication, and raising awareness among users of strong passwords could significantly reduce attackers' possibilities. A review of update policies within organisations and the partitioning of networks would also help to slow down or even prevent many computer attacks.

The ANSSI invites you to consult the guides "Recommendations for multi-factor authentication and passwords" (https://www.ssi.gouv.fr/administration/guide/recommandations-relatives-a-lauthentification-multifacteur-et-aux-mots-de-passe/) and "Ransomware attacks, all concerned - How to prevent them and respond to an incident" (https://www.ssi.gouv.fr/en/guide/ransomware-attacks-all-concerned/).

1. Offensive actors with constantly developing capacities

1.1. Cyber crime: specialisation and professionalisation of actors

Like traditional organised crime, cyber crime is an economic network of specialised service providers whose members work together more or less closely depending on the opportunities and objectives at the time. This organisation is both the cause and the consequence of the maturity of the cyber criminal ecosystem, which is directly fuelled by its financial gains, estimated at more than one billion euros per year.

This ecosystem has specialised around a galaxy of professions and roles that often correspond to the different stages of a computer attack. Cyber criminals specialise in providing services such as malware, anonymisation infrastructure, access to compromised networks (*Access Broker*), *botnets*, spamming services and money laundering. Very few cyber criminal groups have all these skills in-house. However, these groups are likely to provide several types of services, like Evil Corp, which has been both operating ransomware since 2017 and distributing the Dridex backdoor [1] [2].

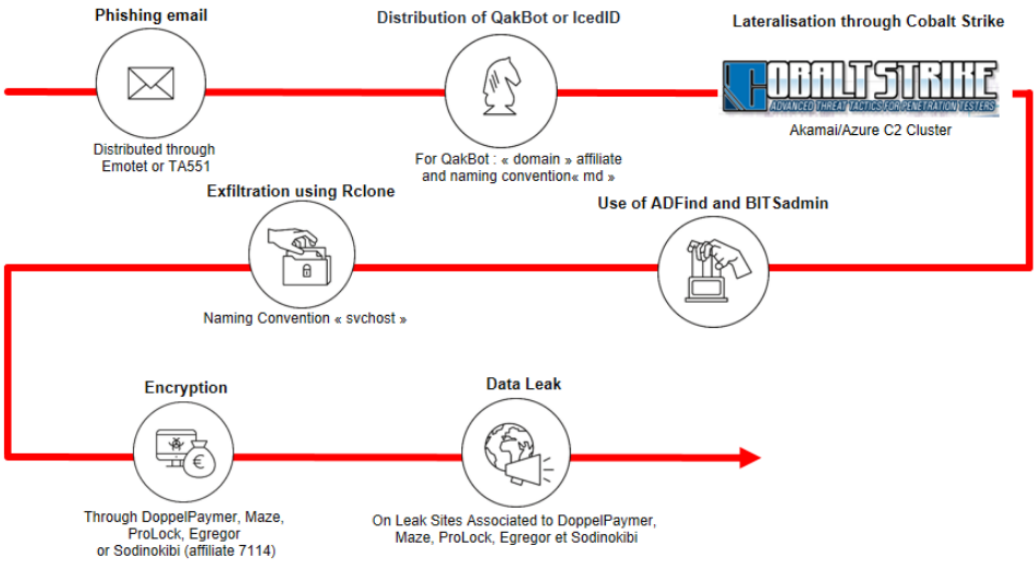

Fig. 1.1. – Summary of the infection chain associated with the Lockean cyber criminal group.

This specialisation and service offer leads to an increase in the potential infection chains, and makes them more complicated to detect and monitor. However, some malicious services such as Emotet [3] or Cobalt Strike are becoming widespread code or infrastructure nodes whose monitoring and blocking can stop an attack in the early stages of the infection chain.

Bullet Proof Hosters are also a perfect example of this specialisation phenomenon. These hosts are therefore particularly accommodating to their customers, providing services that are widely used by malicious actors. These hosts are characterised by:

- a non-existent *Know Your Client* (KYC) policy;
- payment in cryptocurrencies;
- the frequent offer of a very fast DNS change service or *Fast Flux* DNS;
- a failure to control or even explicit promotion of malicious activities;
- hosting the infrastructure in jurisdictions beyond the reach of judicial cooperation treaties.

These ”bulletproof” hosts are used by many cyber criminal groups to rent technical resources. Several of them have been the subject of open source investigations such as Yalishanda [4], Dr. Samuil [5], CCWeb or BraZZZerS [6].

Comment: Preventive blocking of their sub-networks or even the corresponding (Autonomous Systems - AS) can greatly improve the security of an organisation. However, side effects are possible.

Ransomware, and in particular Ransomware-as-a-Service (RaaS), also illustrates these phenomena of specialisation and professionalisation of the cyber crime ecosystem. They involve a range of groups and individuals, sometimes specifically recruited for their skills, as in the case of FIN7 [7]. An *access broker* can thus conduct vulnerability scans to identify potential targets, on average within 48 hours of the disclosure of a vulnerability and an exploitation method. The broker may also operate a targeted or non-targeted phishing service, which remains the most common vector of primary infection. The access obtained in this way is shared with other attackers, who may for example have expertise in lateral movement within networks managed by the *Active Directory*, critical components of information systems. Once the resources of interest have been identified and exfiltrated, the encryption of the computer equipment can be initiated using the ransomware made available by the ransomware operators.

In 2021, the ANSSI monitored on average around 40 different ransomware programs.

Targeting all sectors of activity, this threat remains mostly opportunistic and seeks out targets with little security, significant financial resources and that cannot allow disruption of activity. However, there are subtleties in targeting. While some groups seek to maximise their profit by targeting as many victims as possible, others target only large and particularly profitable companies in so-called *Big Game Hunting* operations. These variations are also reflected in the speed of the infection chain, the deployment and encryption phase. However, some cyber criminal attacker groups may remain in their victims' networks for days or weeks to identify key resources, study their contents before exfiltration and threatening to publish them to exert further pressure in the extortion and ransom negotiation phase.

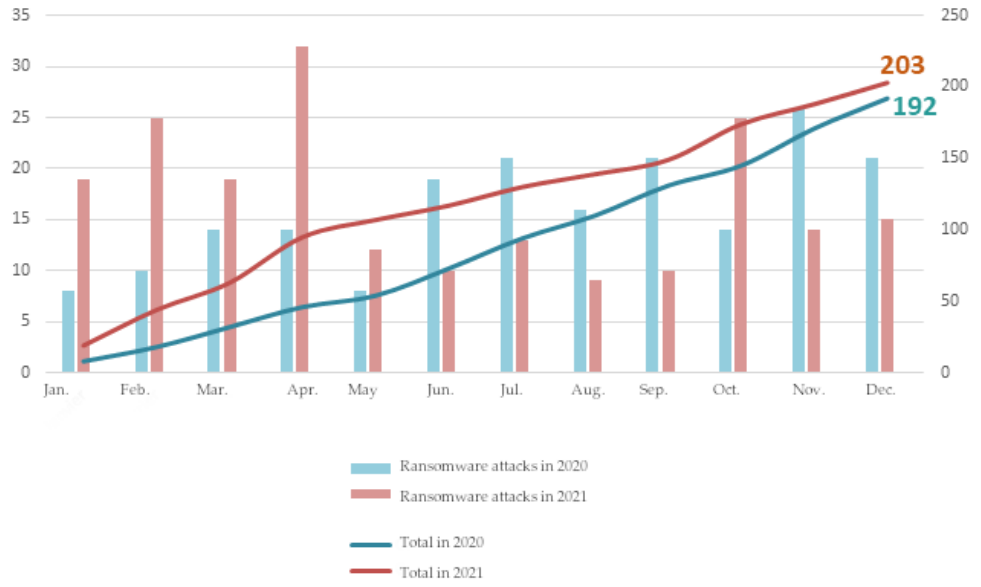

Fig. 1.2. – Statistics on ransomware attacks handled by the ANSSI in 2020 and 2021.

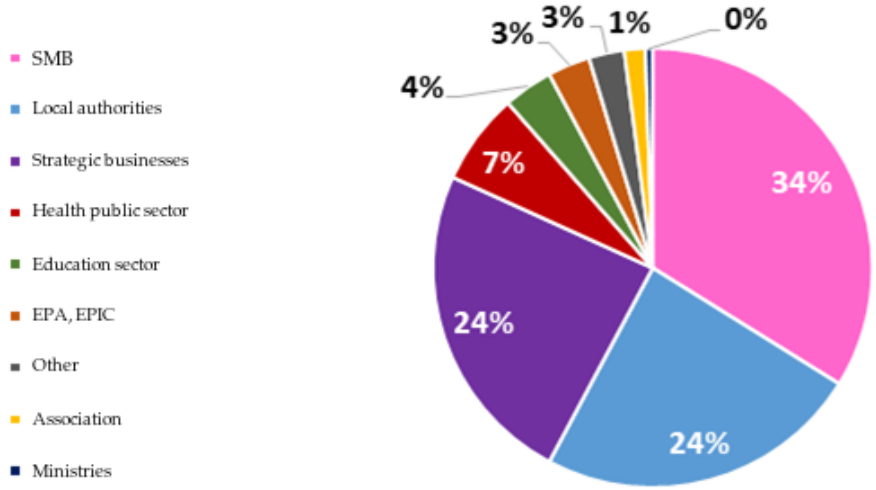

Fig. 1.3. – Breakdown of entities targeted by ransomware attacks in the context of incidents handled by the ANSSI in 2020.

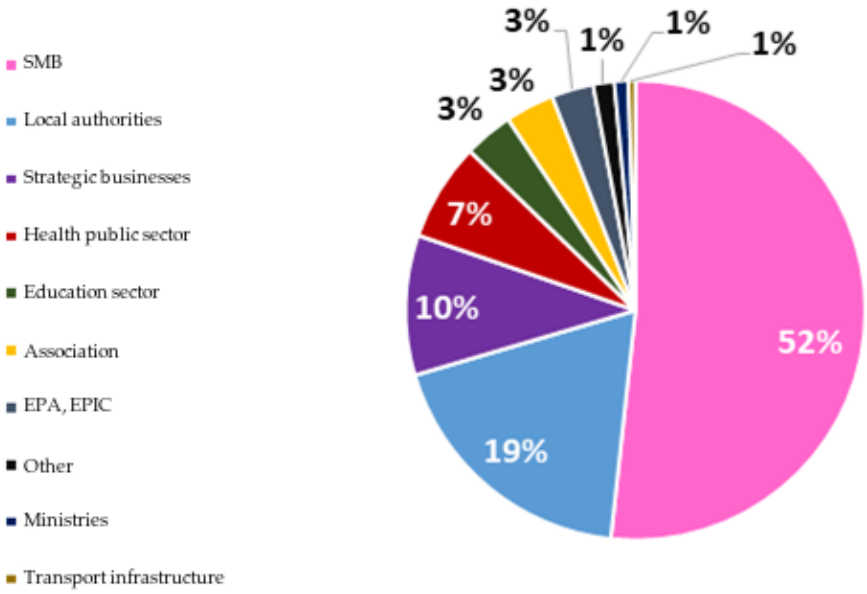

Fig. 1.4. – Breakdown of entities targeted by ransomware attacks in the context of incidents handled by the ANSSI in 2021.

The increase in the number of extortion methods and blackmail methods used by cyber criminals is also evidence of their professionalisation. These cyber criminals do not hesitate to combine the threat of disclosure of exfiltrated data with DDoS blackmail [1], telephone harassment or contacting the victim's media, partners or customers, which is similar to a form of "*Name & Shame*".

The targeting of certain groups could evolve to avoid the compromise of critical infrastructure or important public institutions. The declaration of an energy state of emergency following the compromise of the US company Colonial Pipeline by the DarkSide ransomware [8] in May 2021 and the raising of the alert level associated with ransomware to a level equivalent to terrorism in the United States [9] in June 2021 marked a turning point in the

1. The principle of threatening a victim with repeated denial of service attacks on its online services if it does not pay the ransom.

consideration of this threat on a global scale. The resources deployed by the security forces have increased tenfold and the number of hard-hitting actions has multiplied over the course of 2021: dismantling of botnets, arrest of affiliates, recovery of ransoms, etc. **The ANSSI therefore believes that only those groups of attackers able to remain out of reach of security forces, sometimes thanks to state protection, will continue to carry out this type of attack against organisations on an international scale. Other ransomware operators might in response move towards "simple" blackmail to disclose exfiltrated information.**

However, the reinvestment of the gains accumulated by cyber criminals will most likely allow them to acquire new capacities, skills and tools adapted to other technical environments where investigative capacities may be less developed, such as Linux or the *Internet of Things* (IoT).

1.2. Increasing difficulties in identifying state actors

For several years, the ANSSI has observed a convergence of methods and tools used by several profiles of malicious actors. State actors are now more commonly using non-characteristic tools, such as Cobalt Strike, widely used in the cyber criminal ecosystem. This was notably the case during the espionage campaign against French entities in 2021, involving the APT31 intrusion set [10]. This phenomenon is not necessarily organised or the result of closer relations between these two types of actors, although some intelligence services are sometimes accused of links with cyber criminals.

Another trend observed is the sharing of tools between different intrusion sets reputed to have links to states. This is particularly the case for ShadowPad [2] which is used by several attacker intrusion sets, most notably APT41 and Tonto Team [11]. This shared use of the same tool, which suggests cooperation between different attacker intrusion sets or the existence of a common supplier, by definition makes it difficult to characterise activities and attribute them to a particular attacker intrusion set. This shared use has also been observed with PlugX [12].

Like many cyber criminals, state-level attackers use the *living-off-the-land* (LotL) technique, which involves using tools already on the victim's network, including administrative tools such as PowerShell, to achieve their goals. They are therefore more difficult to detect since they use few or no tools that are characteristic of malicious activity. In addition to streamlining costs, this use of non-characteristic tools, shared or operated from the victim's network, also makes it possible to plausibly deny any involvement by not allowing activities to be characterised precisely. This is particularly the case when ransomware is used by state-run intrusion sets for profit rather than sabotage. As such, several attacker groups allegedly linked to North Korean interests are believed to use ransomware for profit, while others use such code to cover their tracks or hide their true objective.

As a result of this borrowing of cyber criminal techniques by state actors, cyber criminals are also becoming more skilled, sometimes reaching a level of sophistication comparable to that of state-level attackers. The financial gains accumulated in previous operations are believed to allow them to undertake more ambitious and longer operations. Some cyber criminal groups are also able to discover and exploit unknown or *0-day* vulnerabilities, which have historically been the preserve of so-called state groups or specialist companies [13].

This porosity between different attacker profiles can also benefit other categories of attackers, notably hacktivists. A first case of ransomware being used for hacktivism was identified in India in 2021: the Sarbloh ransomware was used as part of a protest against a government land reform [14].

1.3. Rapidly developing private capacity

The recent news related to the revelations about the targets of the customers of the Pegasus system marketed by the Israeli company NSO Group has led to a real awareness of the threat that certain private companies can represent. However, the market has been in existence for over a decade and the companies involved are as well established as they are secretive about their activities and customers.

Several service offers are possible: turnkey tools, human expertise or capacities such as *0-day* vulnerability ex-

2. Modular attack platform to open and maintain remote access to a compromised system.

ploitation methods. While these services are generally reserved for state clients in the fight against terrorism and organised crime, the latest revelations suggest a shift in the use of these tools for strategic and political espionage against other targets such as journalists, human rights defenders and senior officials [15], as well as companies holding personal data such as electronic communications operators or transport companies. These services range from the use of infected applications, through more sophisticated attack tools such as Cobalt Strike, to the exploitation of *0-day* vulnerabilities without the need for interaction with the target (*0-click*). Finally, the use of a third party, *a fortiori* private, can generate a certain feeling of impunity which may explain the unabashed targeting of certain clients.

The growth and proliferation of such companies also increases the risk that they themselves will be subject to computer attacks, leading to the disclosure and proliferation of potentially sophisticated attack tools. For the record, this was notably the case of the Italian company Hacking Team, which was the victim of an exfiltration of data and tools in 2015. These tools were exploited up until 2020 by actors reputed to have links to states and cyber criminals.

Finally, these sometimes very sophisticated services can provide new clients (state or non-state) with the means to carry out computer attacks without having to build their own capacities and skills.

2. Low-visibility attempts at espionage and sabotage, but cause for concern nonetheless

While profit-driven attacks have been in the spotlight in recent months, it is important to remember that espionage remains the primary objective, along with destabilisation attempts and computer sabotage.

2.1. Espionage remains the primary objective, particularly in France

The threat of strategic espionage remains a constant factor to be taken into account; it affects both institutional and private actors. France is a particular target of this threat, as evidenced by the attack campaigns using the Sandworm [16], Nobelium [17] or APT31 [10] intrusion sets in 2020-2021. **In 2021, of the 17 cyber defence operations handled by the ANSSI, 14 were related to computer espionage operations, 9 of which involved intrusion sets reputed to be Chinese. Similarly, of 8 major incidents, 5 involved attacker intrusion sets reputed to be Chinese.**

The misuse of foreign legal frameworks relating to cyber security can also facilitate these espionage actions aimed at capturing personal data of French citizens and/or data belonging to French companies located abroad. Although cyber security legislation is increasing worldwide, there have been several reports or suspicions of misuse of non-cyber security related legal mechanisms for espionage purposes. For example, some versions of the GoldenTax software imposed in China have embedded a backdoor allowing stealth access to the information systems of several companies [18]. Furthermore, the extraterritoriality of certain foreign national security legislation [3], a concept open to broad interpretation, poses an additional risk to data confidentiality and the availability of digital infrastructures.

This threat of misuse is likely to increase as states take on cyber issues through legislative and regulatory measures.

2.2. The targeting of critical infrastructure for sabotage remains a constant threat

Extremely critical sectors such as the water sector in Israel and the transport sector in the United States have also been subject to computer attacks for the purpose of pre-positioning and sabotage. In April 2020, several critical water and wastewater facilities in Israel were targeted in coordinated but limited attacks, later attributed to Iran [19]. In February 2021, a joint security advisory from the CISA, FBI, ISAC and EPA [20] indicated that attackers had successfully accessed the industrial system of a drinking water treatment facility in Florida. They are believed to have manipulated the level of sodium hydroxide in a potential poisoning attempt. In particular, the attackers

3. ITAR, FISA or the Cloud Act for example, or the intelligence law of the People's Republic of China.

took advantage of the weakness of the passwords used - the same ones on several interfaces and systems - and are believed to have exploited vulnerabilities in Windows 7.

The air transport sector has also experienced computer attacks for pre-positioning purposes. In August 2020, a joint CISA and FBI alert indicated that reconnaissance actions were being conducted by state-sponsored actors in the aviation sector. These pre-positioning actions included in particular vulnerability scans and attempts to recover logins and passwords.

The computer sabotage attack on the Iranian port of Shahid Rajaee in May 2020 was attributed to the Israeli authorities in retaliation for the attack on the Israeli water system in April 2020 [19]. This attack is believed to have stopped the systems regulating the flow of cargo and goods, causing traffic congestion at the port entrance for several days.

The targeting of critical infrastructure by state-level actors is likely to continue, particularly in the context of heightened geopolitical tensions. These actors are also likely to make use of cyber criminal groups in order to maintain plausible deniability.

2.3. Computer attacks for influence and destabilisation purposes

Influence and destabilisation operations are no longer limited to the simple creation of content and the search for, or even the compromise of, relays to amplify their distribution. More and more information operations rely on compromising computers in order to exfiltrate authentic documents and gain initial access to information systems. These documents and accesses are used later in operations, such as the Ghostwriter campaign attributed to Russia by Germany [21] and the European Union [22] and to Belarus by the security editor FireEye [23]. Exfiltrated documents may be released as is or modified before release. **This is not a new phenomenon, but it calls for particular vigilance in the run-up to major elections in France in 2022.**

3. Numerous weaknesses exploited

3.1. Mass exploitation of vulnerabilities by different profiles of malicious actors

Too many organisations still fail to apply patches issued by software editors in time and provide attackers with a relatively easy initial infection vector on systems exposed on the Internet. As soon as an exploitation method is made available, in the space of a few days or even a few hours, the exploitation of vulnerabilities can be industrialised, in particular through the identification of vulnerable instances by means of massive scans and serve various purposes, from computer espionage through to attacks for profit. This is particularly the case for Exchange vulnerabilities, the exploitation of which by numerous intrusion sets has been the subject of many publications. The exploitation of vulnerabilities in network devices (notably PulseSecure and Citrix) is common and regularly allows ransomware attacks.

2020-2021 has been particularly marked by some major vulnerabilities (Exchange, Log4j, PulseSecure). The ANSSI and its beneficiaries have been fully mobilised to ensure that they are corrected. It should be noted that these major vulnerabilities affected the whole world. They are therefore included in the rankings of the ANSSI's counterpart agency in the United States, the CISA. These vulnerabilities are likely to continue to be exploited in the coming months.

Most exploited CVE in 2020					
Incidents handled by the ANSSI			Incidents handled by the CISA		
1	**CVE-2019-19781**	**Citrix**	**1**	**CVE-2019-19781**	**Citrix**
2	**CVE-2019-11510**	**Pulse**	**2**	**CVE-2019-11510**	**Pulse**
3	**CVE-2018-13379**	**Fortinet**	**3**	**CVE-2018-13379**	**Fortinet**
4	CVE-2020-1472	Netlogon	4	CVE-2020-5902	F5-Big IP
5	CVE-2020-5902	F5-Big-Ip	5	CVE-2020-15505	MobileIron
6	CVE-2020-18935	Telerik	6	CVE-2017-11882	Microsoft
7	CVE-2020-15505	MobileIron	7	CVE-2019-11580	Atlassian
8	CVE-2018-7600	Drupal	8	CVE-2018-7600	Drupal
9	CVE-2017-11882	Microsoft	9	CVE-2019-18935	Telerik
			10	CVE-2019-0604	Microsoft
			11	CVE-2020-0787	Microsoft
			12	CVE-2020-1472	Netlogon

Fig. 3.1. – Most exploited vulnerabilities in 2020 in incidents handled by the ANSSI and the CISA [4].

Most exploited CVE in 2021					
Incidents handled by the ANSSI			Incidents handled by the CISA		
1	**CVE-2021-26855**	**Microsoft Exchange**	**1**	**CVE-2021-26855**	**Microsoft Exchange**
2	**CVE-2021-26857**		**2**	**CVE-2021-26857**	
3	**CVE-2021-26858**		**3**	**CVE-2021-26858**	
4	**CVE-2021-27065**		**4**	**CVE-2021-27065**	
5	CVE-2018-13379	Fortinet	5	CVE-2021-22893	Pulse
6	CVE-2021-21985	VMWare	6	CVE-2021-22894	
7	CVE-2021-22893	Pulse	7	CVE-2021-22899	
			8	CVE-2021-22900	
			9	CVE-2021-27101	Accellion
			10	CVE-2021-27102	
			11	CVE-2021-27103	
			12	CVE-2021-27104	
			13	CVE-2021-21985	VMWare
			14	CVE-2018-13379	Fortinet
			15	CVE-2020-12812	
			16	CVE-2019-5591	

Fig. 3.2. – Most exploited vulnerabilities in 2021 in incidents handled by the ANSSI and the CISA.

2020-2021 has also seen an explosion in the number of *0-day* vulnerabilities actively exploited. According to Google's *Threat Analysis Group* (TAG) in July 2021, 33 such vulnerabilities were exploited before a patch was made available, compared with 25 in 2020 and 20 in 2019. Several phenomena can explain this explosion: the improvement of detection and information sharing efforts, but also the increased technical capacities of attackers potentially supported by the development of the ecosystem of companies marketing this type of vulnerability. The misuse of China's vulnerability legislation, which requires companies to report vulnerabilities to the Chinese authorities, raises concerns about the easy identification of *0-day* vulnerabilities by Chinese attacker groups.

4. For the record, the CISA (Cybersecurity and Infrastructure Security Agency) is the US federal agency in charge of coordinating US cyber defence actions.

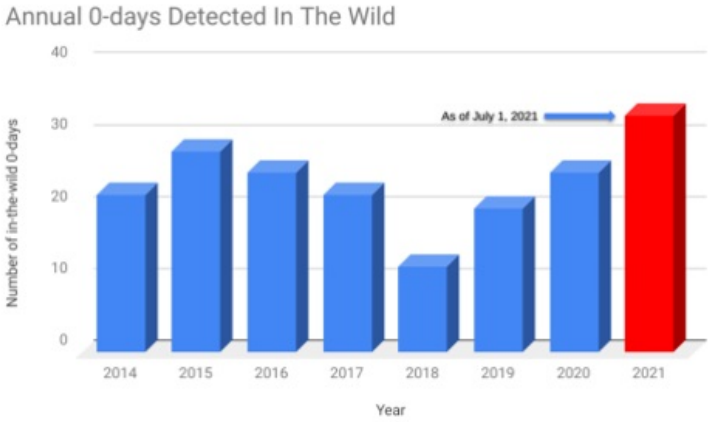

Fig. 3.3. – Evolution in the number of *0-day* vulnerabilities exploited between 2014 and July 2021, according to the Google TAG [24]

While no software or hardware product is impervious to vulnerabilities, measures exist that can complicate their task and prevent them from being exploited on a large scale. In addition to increased exchanges within dedicated communities, particularly when an exploitation method is disclosed, priority should be given to applying patches to systems exposed on the Internet, or failing that, to implementing circumvention measures.

In general, minimising the possibility of bouncing from a server hosting an application to an internal network requires strict outbound filtering and the maintaining of an up-to-date inventory of the service accounts used. These accounts should also minimise their privileges that are valid throughout the internal network. In the case of an Active Directory, this means that these accounts should not have privileges such as "Domain administrator", but should be limited:

- ideally, to standard user privileges;
- exceptionally, to local administrative privileges valid only on the servers hosting the product.

The ANSSI invites you to consult the guides "Mapping the information system" (`https://www.ssi.gouv.fr/en/guide/mapping-the-information-system/`) and "Cyber hygiene guide" (`https://www.ssi.gouv.fr/administration/guide/guide-dhygiene-informatique/`), along with the analysis of the "10 vulnerabilities most commonly observed by the agency in 2021" (`https://www.cert.ssi.gouv.fr/actualite/CERTFR-2022-ACT-008/`).

3.2. The exploitation of new digital uses such as the cloud for malicious purposes

The use of cloud services has been underway for several years and has accelerated in the last two years in the public and private sectors, with the health crisis acting as a catalyst. This widespread use automatically increases the level of threat to its users. Reports of defects in the security of data or containers are still too common. Between October 2020 and February 2021, Palo Alto detected over 2100 unsecured and easily accessible cloud instances [25].

The computing power offered by cloud instances is also a target of interest for attackers who would like to use it for their own benefit, particularly for cryptocurrency mining. The cyber criminal group "TeamTNT" has specialised in targeting cloud environments for cryptomining purposes [26], while the reputedly Chinese group "Rocke" has specialised in clandestine cryptomining on cloud servers. It therefore exploits vulnerabilities on these servers, which allow the installation of a backdoor from which attackers deploy cryptominers, terminate any previous cryptomining processes and prevent the installation of new malware [27].

The cloud also offers means of spreading within the target information system without the need for malware. Many document sharing and collaborative working services actually allow users to easily log back into their services af-

ter initial authentication. The same authentication token can be used for all of a user's devices. Access to these authentication tokens is a growing threat, with attackers attempting to gain access to them through social engineering. Once intercepted and copied by an attacker, the token can be used from another device without being detected. Another technique for token theft is to install on the target's file system a token connected to an account controlled by the attacker. When the victim automatically synchronises his or her folder in the cloud, it is with the attacker's folder and not his or her own. The attacker can thus recover the authentic token and reuse it remotely and discreetly, while erasing all traces of it having been compromised [28].

> The ANSSI invites you to consult the guides "Recommendations for multi-factor authentication and passwords" (https://www.ssi.gouv.fr/administration/guide/recommandations-relatives-a-lauthentification-multifacteur-et-aux-mots-de-passe/) and "Recommendations for securing the implementation of the OpenID Connect protocol" (https://www.ssi.gouv.fr/administration/guide/recommandations-pour-la-securisation-de-la-mise-en-oeuvre-du-protocole-openid-connect/).

The cloud can also be a source of constraints and difficulties of which users may not be aware. Lack of control over the infrastructure and a heavy dependence on the service provider, as well as sometimes opaque responsibility-sharing arrangements, can be an additional obstacle in the event of a compromise. The difficulties of intervention and investigation, detection and remediation must therefore be taken into account.

> Of course, security principles and good practices also apply to cloud technologies, especially with regard to partitioning, authentication, logging, administration and outsourcing measures. The importance of a risk management approach (such as EBIOS RISK MANAGER) in this context should also be kept in mind.

Finally, legal and contractual aspects can be an additional source of threats. The localisation of data and the extraterritoriality of certain legislation can have consequences for data protection and sovereignty. The preponderance of additional foreign players in the European market could increase the legal threat associated with the cloud. In response to these risks, in 2016 the ANSSI created the "SecNumCloud" security qualification for *cloud* service providers. In October 2021, an updated version of this requirements framework was published on the ANSSI website for comments. The future SecNumCloud qualification scheme includes in particular organisational and technical requirements aimed at protecting against extraterritorial laws that would allow a non-European country to access all or part of the data and processing hosted by a provider.

3.3. Indirect attacks via the supply chain are becoming increasingly common

This technique has been tried and tested and exploited by several state actors and cyber criminals since at least 2016. However, the cyber community as a whole is seeing a significant upward trend in the use of this indirect attack technique. According to the ENISA, between January 2020 and July 2021, 24 attacks on the supply chain were reported and documented [29]. This method presents a risk of rapid propagation of an attack which can sometimes affect an entire activity sector or a specific geographical area, particularly when the attack targets a local digital services company (DSC) or one specialising in a particular activity sector.

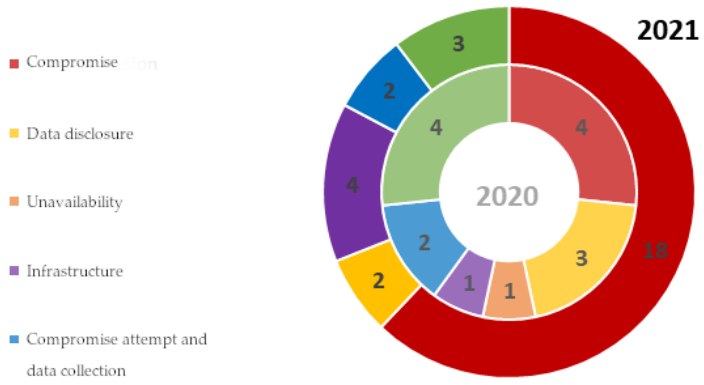

Fig. 3.4. – Comparison of the types of incidents handled by the ANSSI and affecting DSCs in 2020 and 2021.

This opportunity will continue to present itself, especially with the increasing digitisation of the supply chain. At European level, France is therefore advocating the imposition of security requirements on key digital players such as DSCs as part of the revision of the NIS (*Network and information Security*) directive in order to limit the domino effect that could result from their compromise.

3.4. Weak data security leading to massive leaks

These disclosures can be divided into four broad categories: data disclosures as part of ransomware attacks; ideologically motivated disclosures (hacktivism) [30] or as part of destabilisation operations [31]; data disclosures for resale purposes; and finally, disclosures due to negligence.

These disclosures can also be used to carry out attacks via the supply chain and to carry out phishing campaigns. They can lead to an infringement of business confidentiality or even national security, when company data (contracts, customers, *etc.*) or classified data is published. This can often have major reputational consequences.

The value placed on data by states, private companies, cyber criminals or any other category of actor will lead attackers to pursue such disclosures. Regular monitoring, similar to that carried out as part of an economic intelligence approach, can help identify these disclosures as early as possible. There are also free online services (e.g. HaveIBeenPwned) that allow you to check whether an email address, login or password has already been disclosed. However, these tools are used reactively or *post mortem* and must be complemented and preceded by raising awareness of the importance of strong passwords, the systematic use of password managers and the widespread activation of multi-factor authentication processes.

4. Conclusion

In the coming months, new opportunities will present themselves to attackers, particularly in France. The associated intentions will be varied, from destabilisation and influence to espionage and financial gain. While the exploitation of *0-day* vulnerabilities remains unpredictable, the 2022 legislative and presidential elections as well as the 2023 Rugby World Cup and the 2024 Olympic Games in France will be events that attackers will seek to exploit. There are multiple potential targets with very different levels of maturity in terms of information systems security - media, political parties, government and public organisations, think tanks, digital companies, critical operators, etc. - **calling for particular vigilance on the part of all stakeholders**.

A. Bibliography

[1] CERT-FR. *Le Code Malveillant Dridex : Origines et Usages*. May 25, 2020.
URL: https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-005.pdf.

[2] Security Affairs. *Evil Corp Rebrands Their Ransomware, This Time Is the Macaw LockerSecurity Affairs*. October 21, 2021.
URL: https://securityaffairs.co/wordpress/123661/cyber-crime/evil-corp-macaw-locker.html.

[3] CERT-FR. *Le Malware-as-a-Service Emotet*. November 2, 2020.
URL: https://www.cert.ssi.gouv.fr/cti/CERTFR-2020-CTI-010/.

[4] Krebs On Security. *Meet the World's Biggest 'Bulletproof' Hoster*. July 16, 2019.
URL: https://krebsonsecurity.com/2019/07/meet-the-worlds-biggest-bulletproof-hoster/.

[5] Krebs On Security. *Amid an Embarrassment of Riches, Ransom Gangs Increasingly Outsource Their Work*. October 9, 2020.
URL: https://krebsonsecurity.com/2020/10/amid-an-embarrassment-of-riches-ransom-gangs-increasingly-outsource-their-work/.

[6] Intel 471. *Bulletproof Hosting: How Cybercrime Stays Resilient*. February 23, 2021.
URL: https://intel471.com/blog/bulletproof-hosting-yalishanda-ransomware-banking-trojans-information-stealers.

[7] Department of Justice. *Three Members of Notorious International Cybercrime Group Fin7*. August 1, 2018.
URL: https://www.justice.gov/opa/pr/three-members-notorious-international-cybercrime-group-fin7-custody-role-attacking-over-100.

[8] Bleeping Computer. *US Declares State of Emergency after Ransomware Hits Largest Pipeline*. May 10, 2021.
URL: https://www.bleepingcomputer.com/news/security/us-declares-state-of-emergency-after-ransomware-hits-largest-pipeline/.

[9] Computerworld. *US to Give Ransomware Attacks Similar Priority as Terrorism, Official Says*. June 4, 2021.
URL: https://www.itnews.com.au/news/us-to-give-ransomware-attacks-similar-priority-as-terrorism-official-says-565470.

[10] CERT-FR. *Campagne d'attaque Du Mode Opératoire APT31 : Description, Contre-Mesures et Code*. December 15, 2021.
URL: https://www.cert.ssi.gouv.fr/cti/CERTFR-2021-CTI-012/.

[11] MITRE ATT&CK. *ShadowPad Software*. April 26, 2021.
URL: https://attack.mitre.org/software/S0596/.

[12] MITRE ATT&CK. *PlugX Software*. June 20, 2020.
URL: https://attack.mitre.org/software/S0013/.

[13] The Hacker News. *REvil Used 0-Day in Kaseya Ransomware Attack, Demands $70 Million Ransom*. July 6, 2021.
URL: https://thehackernews.com/2021/07/revil-used-0-day-in-kaseya-ransomware.html.

[14] Bleeping Computer. *New Sarbloh Ransomware Supports Indian Farmers' Protest*. March 8, 2021.
URL: https://www.bleepingcomputer.com/news/security/new-sarbloh-ransomware-supports-indian-farmers-protest/.

[15] Le Monde. *Comment les services de renseignement français ont traqué Pegasus après les révélations du « Monde »*. November 19, 2021.
URL: https://www.lemonde.fr/pixels/article/2021/11/19/comment-le-renseignement-francais-a-traque-pegasus-apres-les-revelations-du-monde_6102638_4408996.html.

[16] CERT-FR. *Campagne d'attaque Du Mode Opératoire Sandworm Ciblant Des Serveurs Centreon*. February 15, 2021.
URL: https://www.cert.ssi.gouv.fr/cti/CERTFR-2021-CTI-004/.

[17] CERT-FR. *Campagnes d'hameçonnage Du Mode Opératoire d'attaquants Nobelium*. December 6, 2021.
URL: https://www.cert.ssi.gouv.fr/cti/CERTFR-2021-CTI-010/.

[18] Trustwave. *The Golden Tax Department and the Emergence of GoldenSpy Malware*. June 25, 2020.
URL: https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/the-golden-tax-department-and-the-emergence-of-goldenspy-malware/.

[19] The Washington Post. "Cyberattack on Iranian Port Is Attributed to Israel". May 18, 2020.
URL: https://www.washingtonpost.com/national-security/officials-israel-linked-to-a-disruptive-cyberattack-on-iranian-port-facility/2020/05/18/9d1da866-9942-11ea-89fd-28fb313d1886_story.html.

[20] CISA. *Compromise of U.S. Water Treatment Facility*. February 11, 2021.
URL: https://www.cisa.gov/uscert/ncas/alerts/aa21-042a.

[21] Infosecurity Magazine. *Germany Accuses Russia of Election Meddling Through Cyber-Attacks*. September 7, 2021.
URL: https://www.infosecurity-magazine.com/news/germany-russia-election-meddling/.

[22] Conseil européen. *Declaration by the High Representative on Behalf of the European Union on Respect for the EU's Democratic Processes*. September 24, 2021.
URL: https://www.consilium.europa.eu/en/press/press-releases/2021/09/24/declaration-by-the-high-representative-on-behalf-of-the-european-union-on-respect-for-the-eu-s-democratic-processes/.

[23] FireEye. *Ghostwriter Update: Cyber Espionage Group UNC1151 Likely Conducts Ghostwriter Influence Activity*. April 28, 2021.
URL: https://www.fireeye.com/content/dam/fireeye-www/blog/pdfs/unc1151-ghostwriter-update-report.pdf.

[24] Google TAG. *How We Protect Users from 0-Day Attacks*. July 14, 2021.
URL: https://blog.google/threat-analysis-group/how-we-protect-users-0-day-attacks/.

[25] Palo Alto - Unit42. *Unsecured Kubernetes Instances Could Be Vulnerable to Exploitation*. April 23, 2021.
URL: https://unit42.paloalonetworks.com/unsecured-kubernetes-instances/.

[26] Intezer. *Intezer - Attackers Abusing Legitimate Cloud Monitoring Tools to Conduct Cyber Attacks*. September 8, 2020.
URL: https://www.intezer.com/blog/cloud-workload-protection/attackers-abusing-legitimate-cloud-monitoring-tools-to-conduct-cyber-attacks/.

[27] Palo Alto Networks. *Malware Used by "Rocke" Group Evolves to Evade Detection by Cloud Security Products*. January 17, 2019.
URL: https://unit42.paloaltonetworks.com/malware-used-by-rocke-group-evolves-to-evade-detection-by-cloud-security-products/.

[28] Help Net Security. *Beware the Man in the Cloud: How to Protect against a New Breed of Cyberattack*. January 21, 2019.
URL: https://www.helpnetsecurity.com/2019/01/21/mitc-attack/.

[29] ENISA. *Threat Landscape for Supply Chain Attacks*. July 29, 2021.
URL: https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks.

[30] actu.fr. *Cyberattaque de l'AP-HP à Paris : un étudiant mis en examen, les données publiées sur internet*. October 11, 2021.
URL: https://actu.fr/ile-de-france/paris_75056/cyberattaque-de-l-ap-hp-a-paris-un-etudiant-mis-en-examen-les-donnees-publiees-sur-internet_45576995.html.

[31] Ars Technica. *NSA Employee Who Brought Hacking Tools Home Sentenced to 66 Months in Prison*. September 25, 2018.
URL: https://arstechnica.com/tech-policy/2018/09/nsa-employee-who-brought-hacking-tools-home-sentenced-to-66-months-in-prison/.

1.9.1 - March 9, 2022

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI - 51 boulevard de la Tour-Maubourg, 75700 PARIS 07 SP
www.cert.ssi.gouv.fr / cert-fr.cossi@ssi.gouv.fr

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
SGDSN