CertIST

Industrie Services Tertiaire

Annual report on Attacks and Vulnerabilities seen in 2021

Released in February 2022

Contents

1 Introduction

Each year, Cert-IST publishes a report on the vulnerabilities, attacks and trends of the previous year to highlight the general tendencies and threat evolution, and help the community protect itself more effectively.

The report begins with a summary of the major security events in 2021 (see § 2), followed by an analysis of the key trends (see § 3). We also offer a brief review of Cert-IST's activity during the year (see § 4).

In the conclusion (see § 5), we give a summary of the current cyber-threat landscape and the challenges companies will face in 2022.

➢ **About Cert-IST**

Cert-IST (Computer Emergency Response Team – Industry, Services and Tertiary) is a computer attack alert and response centre for businesses. Set up in 1999, Cert-IST helps its members identify threats by continuously analysing new vulnerabilities, their severity and the protection measures needed. In the event of a security incident affecting one of its members, Cert-IST can assist with the investigation and the return to normal operations.

2 What happened in 2021

2.1 The Top 8

In this section, we bring you a summary of all the news from 2021. But first, here are the events we think were the most significant.

- **ProxyLogon** and **ProxyShell** attacks on Microsoft Exchange.
- Apache **Log4J** vulnerability.
- **PrintNightmare** vulnerabilities.
- Return of **NTLM relay** attacks (PetitPotam).
- REvil attack on **Kaseya**.
- **Pegasus** attack and **zero-click** vulnerabilities aimed at Apple (ForcedEntry).
- **Codecov.io** attack in CI/CD environments.
- Increasing focus on vulnerabilities in **Microsoft Azure**.

We discussed this last item in the headline article of our September 2021 monthly bulletin, reproduced below.

Headline article from Cert-IST monthly bulletin, September 2021:

In just one month, from 30 August to 29 September 2021, we published three information messages about issues affecting Microsoft's Azure cloud computing service: **INFO-2021.023** about Azure Cosmos, **INFO-2021.026** about OMI and **INFO-2021.027** about the brute force attack on Azure passwords. In each case, it was researchers who warned Microsoft following their work on Azure. And these announcements will undoubtedly prompt other researchers to look into this issue as well. **We should therefore expect an increase in the number of vulnerabilities discovered in Azure (and Microsoft 365).**

The SolarWinds incident in late 2020 showed that state-sponsored hackers (in this case, probably Russia) were already working of these issues, with attacks targeting Azure and Microsoft 365 authentication (Golden SAML attacks). The fact that security researchers now also publishes on these topics is therefore beneficial, since it will help highlight (and fix) problems that may already be known 0-days for some state-sponsored hackers.

These recent publications show that the search for vulnerabilities in the cloud is changing, with a greater focus on more technical issues than what was previously known. Until now, we were essentially talking about poor infrastructure configuration, such as weakly protected AWS buckets, for example, which anyone could browse. Now, however, researchers are also focusing on the underlying protocols and the way security mechanisms are implemented. This is a step forward in the maturity level of the research for vulnerabilities in cloud solutions.

2.2 Key events in 2021

The table below gives a summary of the key events in 2021. These events are significant because they received a lot of media attention, or because they are indicators of cyber threat evolution.

January 2021	**Emotet dismantled, NetWalker arrest.** Anti-cybercrime operations began in January and have continued throughout 2021: • Against ransomware actors: NetWalker (January), Egregor (February), Clop (June) and REvil (October). Some groups decided to suspend their activities: DarkSide (May), Avaddon (June) and BlackMatter (November). • Against certain mass malware: Emotet (January and April). • Against infrastructure: shutdown of DoubleVPN (June), dark web Operation Dark HunTor (October). Of course, it is a never-ending battle: Trickbot was back in February and Emotet in November. And when a ransomware stops operating, it often re-emerges in another form: in 2021, REvil was replaced by DarkSide, then BlackMatter, then BlackCat (ALPHV).

January 2021	**Baron Samedit:** A vulnerability discovered by Qualys in the "sudo" command in Linux and Unix allows a user to obtain "root" privileges. It is a simple escalation of privileges, but the vulnerability is easy to exploit (with an exploit program) and affects a huge number of Linux distributions, as well as Solaris, AIX and macOS.
January 2021	**SonicWall** had a difficult start to the year, with 0-day attacks on its **SMA** VPN product in January and February, then **Email Security** in April, then **SMA** and **SRA** in June. We reported on these developments in our **INFO-2021.003**, **INFO-2021.010** and **INFO-2021.017** messages. **Zyxel** (another VPN vendor) also announced critical vulnerabilities in its products in January and then in June.
February 2021	A **water treatment plant in the city of Oldsmar, Florida**, was hacked, and the level of sodium hydroxide was increased to a dangerous level. The investigation showed that an employee's computer had been breached, which gave access to the water treatment system (via TeamViewer on a computer). Disaster was avoided because the operator in charge of the station noticed the unusual level of chemical.
February 2021	**Dependency confusion.** A researcher described an attack technique that takes advantage of the way code generation tools (or package installers) fetch their dependencies (linked libraries or packages). The problem was illustrated again in June when a researcher accidentally hacked the website of Microsoft's Halo game. We discuss this dependencies issue in § 3.6.1, which deals with the software supply chain.
February 2021	**France: Russian attacks (Sandworm) on Centreon.** ANSSI, France's national agency for information system security, published a report on the attacks (from 2017 to 2020) targeting old versions of Centreon's IT monitoring software. The attacks were probably perpetrated by the Sandworm group. *(We published message **INFO-2021.006** for this event).*
March 2021	**Accellion FTA:** Cybercriminals used 0-days in Accellion's FTA software to steal documents and blackmail the company's user customers. The victims included Singapore Telecommunications (in February), then Qualys and Shell (in March).
March 2021 Top news	**ProxyLogon attack on Exchange**. This attack was used occasionally in January by the Hafnium group, then massively from March by various types of hackers. We discuss this attack in § 3.1.
March 2021	**France: Fire at the OVHcloud datacentre** in Strasbourg. The fire was an accident, probably caused by an electrical fault.
March 2021	**France:** The **Pierre Fabre laboratory** was affected by **ransomware**. It was one of hundreds of victims in France in 2021. Others included **Manutan** (attacked in February). Manutan shared its experience about the crisis, which was greatly appreciated. Internationally, **Accenture** was also affected by a ransomware attack in August. The scale of the incident was apparently much smaller than claimed by the LockBit group (behind the attack). Below, we also mention the **Colonial Pipe** (May) and **Kaseya** (June) attacks.
April 2021	**Attack on a nuclear facility in Natanz, Iran.** A report claimed this was a cyberattack, but to our knowledge the facts have not been clearly established.

April 2021 Top news	**Codecov.io Bash Uploader attack:** A hacker modified the Bash Uploader script in Codecov.io's cloud environment, and for two months (February and March) was able to retrieve data about software developed by third parties (such as Rapid7 and IBM) in CI/CD mode. We discuss this attack in § 3.6.2, which deals with the software supply chain.
April 2021 Top news	**NTLM relay attacks:** Already known to specialists, NTLM relay attacks made a conspicuous return in 2021: - In April with the **RemotePotato0** attack. - In July with the **PetitPotam** attack. - And in January 2022 with the **ShadowCoerce** attack. **PetitPotam** is considered the most dangerous attack because it can be combined with the ESC8 attack, which was discussed in June in the study: Certified Pre-Owned: Abusing ADCS. It allows an attacker without an account (but already on the company's internal network) to take control of the Microsoft PKI (ADCS). *(We published message INFO-2021.018 about this attack.)*
April 2021	**21Nails**: This is a series of 21 vulnerabilities in Exim (mail server under Linux/Unix) discovered by Qualys. We issued a yellow alert **CERT-IST/AL-2021.007** for the most serious one (CVE-2020-28018), but no massive attacks were observed subsequently**.**
April 2021	**BadAlloc vulnerability in RTOSs** (real-time operating systems): Microsoft published a series of 25 vulnerabilities after a study of real-time OSs used in the automotive sector and medical equipment, for example. The OS most cited by the press was BlackBerry QNX.
May 2021	**Colonial Pipeline** was hit by a ransomware attack conducted by the DarkSide group. After this attack, the White House declared the fight against ransomware a national priority. The issue was also discussed at the G7 summit in June 2021.
May 2021	**FragAttack WiFi vulnerability.** A researcher published a series of 12 vulnerabilities in the fragmentation and aggregation functions (hence the name FR-AG) of WiFi frames. *(We published message INFO-2021.012 about this news.)*
May 2021	**Vulnerabilities in Nagios**. Since the SolarWinds Orion attack in 2020, monitoring software (such as Nagios) has come under scrutiny by researchers. - In May, skylightcyber.com published a first report on 13 vulnerabilities in Nagios, as well as an attack tool called **SoyGun**. - In October, Synacktiv.com reported five vulnerabilities. - In November, grimm-co.com reported 11 vulnerabilities.
June 2021	**Interception of ANOM phones by the FBI and the Australian Federal Police** led to the arrest of hundreds of suspects. These secure phones had been sold to criminals in an underground market. This operation is reminiscent of the infiltration in 2020 on **EncroChat** phones by police in France and the Netherlands.
June 2021	**ALPACA:** A new TLS attack technique. The vulnerability was discovered by a group of academics, and for now the attack seems difficult to carry out. It highlights the danger of wildcard TLS certificates (such as *.my-company.com). *(We published message INFO-2021.015 about this news.)*
June 2021	**Death of John McAfee** in a Spanish prison. Nefarious and capricious character who created the famous antivirus, he apparently committed suicide in the prison where he was being held.

June 2021 Top news	**PrintNightmare:** The saga around the vulnerabilities in Microsoft's Print Spooler started in June with the (accidental?) publication by researchers of a PoC for a supposedly fixed vulnerability. It continued for much of the summer, with publication of an urgent patch after a week, which was immediately circumvented, then publication of new fixes, which caused printing problems.
June 2021 Top news	**Kaseya attack:** because of a flaw in Kaseya's VSA solution, the REvil group managed to infiltrate MSPs and infect their clients. Nearly 1,500 companies were infected. The REvil group demanded $70 million, but Kaseya obtained a decryption key on 23 July from an undisclosed source. The incident had begun on 2 July. *(We published message INFO-2021.020 about this news.)*
July 2021 Top new	**Pegasus:** A consortium of journalists revealed that misuse of the NSO spyware (originally designed to help combat terrorism) was much more widespread than previously known. The United Nations requested a moratorium on the sale of this type of software (in August). The Israeli government subsequently banned the export of Pegasus to 65 countries (in November).
July 2021	**SeriousSAM vulnerability** in Windows. This was one of the Windows vulnerabilities reported in the media in July (along with PrintNightmare and PetitPotam) and undoubtedly the least serious. SeriousSAM is a vulnerability in the Windows registry and allows attacks on the Security Account Manager (SAM).
August 2021	**Data breach at T-Mobile:** The breach exposed the personal information of 50 million customers of the telecoms operator. This was the fourth known data leak at T-Mobile, after August 2018, November 2019 and March 2020. A fifth breach was also announced in December 2021.
August 2021	**Linux turned 30**. And apparently, the **computer password turned 60**.
September 2021	**BrakTooth vulnerabilities in Bluetooth.** A series of 16 vulnerabilities was published by academic researchers. And in November, a proof-of-concept program was made available. This was not an exceptional event, since Bluetooth vulnerabilities are discovered every year.
September 2021	**Zoho Manage Engine's** products were the focus of a series of (possibly Chinese) cyber espionage attacks that successively targeted **ADSelfService Plus** (revealed in September), then **ServiceDesk Plus** (revealed in December), and then **Desktop Central** (also in December).
September 2021	**ForcedEntry / Apple zero-click vulnerabilities:** Apple published a fix for the most infamous zero-click vulnerabilities (used by Pegasus since mid-2020).
September 2021 Top news	**OMIGOD vulnerability** (pronounced "Oh My God!") **in Microsoft Azure**: Researchers at Wiz.io discover a critical vulnerability in the Open Management Infrastructure (OMI) component that is automatically installed by Microsoft in some Linux VMs deployed in Azure.

October 2021	**LightBasin attack on 13 telecoms operators**. CrowdStrike published a report on this attack and showed the level of sophistication that can be achieved by an attack designed specifically for a particular business domain. Telecoms operators are a frequent target of cyber espionage attacks. Examples in 2021 include: Operation Diànxùn (March), DeadRinger (August) and Operation GhostShell (October).
October 2021	**Cyberattack 64411 in Iran**. In October, a mysterious attack (unexplained) paralysed petrol station pumps with the message "Cyberattack 64411". 64411 is the phone number of Iranian Supreme Leader Ali Khamenei. This number had already been displayed during an attack in early July that paralysed the rail service.
November 2021	**Meris DDoS botnet.** A new botnet (discovered in June) is breaking records and taking its place alongside the traditional Mirai family botnets.
November 2021	**CISA launches KEV catalogue:** KEV stands for known exploited vulnerabilities. The Cybersecurity and Infrastructure Security Agency (CISA) has launched a database of KEVs that American federal agencies must act on (by applying patches). It supplements the National Vulnerability Database (NVD).
December 2021 Top news	**Log4j:** The **Log4Shell** (CVE-2021-44228) vulnerability in the Apache Log4j library has caused companies to work hard to identify and protect vulnerable installations.
December 2021	**iLOBleed rootkit targeting HP iLO** discovered by an Iranian company. This rootkit is highly sophisticated and the analysis by the Iranian company remarkable.

3 Analysis of the most significant phenomena in 2021

In this section, we analyse the most significant phenomena of the year:

- **Exchange ProxyLogon:** the major attack of 2021.
- **Ransomware:** attacks continue.
- Other **blackmails targeting companies**.
- **Cryptocurrencies:** rise in attacks on platforms and assets.
- **Supply chain** attacks.
- **Source code:** a **new target** of attacks.
- Rise in the **number of vulnerabilities**.
- **Log4j:** what we learned from it.
- **Geopolitics** and state-sponsored attacks.

3.1 Exchange ProxyLogon: the major attack of 2021.

3.1.1 At a glance

The ProxyLogon (March 2021) and ProxyShell (August 2021) attacks against on-premise Exchange servers are, in our opinion, the most significant attack of 2021. They served as entry points for intrusions by state actors (APT attacks) as well as cybercriminals (ransomware attacks).

When looking back: in 2020, the most common intrusion vector was vulnerabilities in VPNs and appliances (BIG-IP, Citrix, Palo Alto Networks, Pulse Secure). In 2021, it was Exchange vulnerabilities. And in 2022, perhaps it will be attacks using Log4j vulnerabilities.

3.1.2 Focus on ProxyLogon and ProxyShell

Microsoft Exchange (on-premise) was the target of two series of attacks in 2021:

- **ProxyLogon** in March 2021, for which we issued a **red alert** **CERT-IST/AL-2021.003**. It is very rare for Cert-IST to use this level of alert (previous cases were in 2017 with WannaCry and NotPetya). The box below explains this crisis in more detail.
- **ProxyShell** in August 2021, for which we issued an amber alert **CERT-IST/AL-2021.010**.

As a result of these attacks, a large number of Exchange servers that were not fixed immediately after the release of the Microsoft patches were compromised throughout 2021.

Excerpt from the Cert-IST monthly bulletin about ProxyLogon:

On 2 March 2021, Microsoft released “out-of-band” patches (without waiting for the next monthly patches) for seven critical vulnerabilities affecting Exchange Server. Two of these vulnerabilities (CVE-2021-26855 and CVE-2021-27065) were first used in isolated attacks in early January 2021 (attacks by the Hafnium group, described by Microsoft and Volexity) and then on a larger scale around 27 February, which is almost certainly what prompted Microsoft to release the “out-of-bound” patches.

From 3 March 2021, the attacks further increased in number, and since no exploit programs were released on the internet before 11 March, it can be assumed that the attack programs were circulating in closed circles. None of the following has been confirmed, but it is possible that there were two successive leaks about these attacks:

- The official discoverer of the two vulnerabilities (Taiwanese company DEVCORE) may have had its discovery stolen in late December 2020 by the Hafnium group, which used it in early January (or alternatively, Hafnium and DEVCORE discovered these vulnerabilities independently).
- One of the participants in the Microsoft MAPP programme may have had the PoC (that Microsoft released in MAPP) stolen in mid-February 2021. This could explain the wave of attacks that began on 27 February.

For this Exchange crisis, Cert-IST published on 3 March 2021:

- Security advisory **CERT-IST/AV-2021.0339** to describe the vulnerabilities and available patches.
- Attack report **CERT-IST/ATK-2021.029** to describe the **Hafnium** group.
- Alert **CERT-IST/AL-2021.003** (at yellow level).

On 4 March 2021, a blog was created in the Crisis Hub (HdC) to track the development of this threat (11 articles posted via this blog in March). On the same day, we raised the alert level to red when we saw the rapid increase in attacks on Exchange.

3.1.3 Other attacks in 2021

The table below details the 16 alerts issued by Cert-IST in 2021.

Alert	Reference	Description	Date
Yellow	CERT-IST/AL-2021.001	Attacks expected against **Sudo** on Linux/Unix systems (CVE-2021-3156)	31 Jan. 21
Amber	CERT-IST/AL-2021.002	Ongoing attacks against **VMware vCenter** Server (CVE-2021-21972)	25 Feb. 21
Red	CERT-IST/AL-2021.003	Ongoing attacks targeting **Microsoft Exchange Server (ProxyLogon)**	3 Mar. 21
Yellow	CERT-IST/AL-2021.004	Attacks expected against **SAP** Solution Manager	11 Mar. 21
Yellow	CERT-IST/AL-2021.005	Attacks expected against **F5 BIG-IP** (CVE-2021-22986)	22 Mar. 21
Amber	CERT-IST/AL-2021.006	Ongoing attacks against **Pulse Connect Secure** (CVE-2021-22893)	21 Apr. 21
Yellow	CERT-IST/AL-2021.007	Attacks expected against **Exim on Linux/Unix** (CVE-2020-28018)	19 May 21
Yellow	CERT-IST/AL-2021.008	Ongoing attacks targeting **VMware vCenter** Server (CVE-2021-21985)	3 Jun. 21
Amber	CERT-IST/AL-2021.009	Attacks against Microsoft Windows Print Spooler (**PrintNightmare**)	1 Jul. 21
Amber	CERT-IST/AL-2021.010	Attacks targeting **Microsoft Exchange Server (ProxyShell)**	13 Aug. 21
Yellow	CERT-IST/AL-2021.011	Ongoing attacks on **Atlassian Confluence** (CVE-2021-26084)	2 Sep. 21
Yellow	CERT-IST/AL-2021.012	Ongoing attacks targeting **VMware vCenter** Server (CVE-2021-22005)	27 Sep. 21
Yellow	CERT-IST/AL-2021.013	Attacks expected against **Apache web servers** (CVE-2021-41773)	6 Oct. 21
Yellow	CERT-IST/AL-2021.014	Attacks targeting **ManageEngine ADSelfService Plus** (CVE-2021-40539)	5 Nov. 21
Yellow	CERT-IST/AL-2021.015	Attacks targeting **GitLab servers** (CVE-2021-22205)	5 Nov. 21
Amber	CERT-IST/AL-2021.016	Attacks against Apache **Log4j** (CVE-2021-44228)	10 Dec. 21

3.2 Ransomware attacks continue

3.2.1 At a glance:

Ransomware attacks targeting businesses (and local authorities) have been widespread since September 2019. They continued in 2020 and then in 2021 at an ever-increasing rate. The two main phenomena of 2021 were:

- Governments fighting back and making unprecedented efforts to stop the most massive attacks, with infrastructure takedowns, cryptocurrency seizures and arrests. The United States has been particularly active on these issues following the Colonial Pipe (May 2021) and Kaseya (July 2021) attacks, but the effort is international.
- Insurance companies are reducing the level of cover in the case of claims and increasing their prices.

3.2.2 Are you prepared for a ransomware attack?

If a company falls victim to a ransomware attack, it will have to manage a crisis on multiple fronts:

- Which parts of the company are compromised? And how to isolate them?
- What IT resources can be used during the crisis?
- How long have the attackers been on the network?
- Are backup and recovery plans adequate for this type of crisis?
- Who to inform? How to communicate: internally, externally, with the hackers?
- What outside help can be called on: insurance, service providers, others?
- Should we pay the ransom?
- Etc.

Some of these questions can only be answered after a crisis has begun, since they will depend on the exact circumstances. But others can be anticipated. And it is wise to have a response plan in place before such a crisis occurs.

A lot of guidance has been published on this issue, especially by government agencies.

- Canada: https://cyber.gc.ca/en/guidance/ransomware-playbook-itsm00099
- France: https://www.ssi.gouv.fr/entreprise/guide/attaques-par-rancongiciels-tous-concernes-comment-les-anticiper-et-reagir-en-cas-dincident/ and https://www.ssi.gouv.fr/administration/guide/crise-dorigine-cyber-les-cles-dune-gestion-operationnelle-et-strategique/
- New Zealand: https://www.cert.govt.nz/it-specialists/guides/how-ransomware-happens-and-how-to-stop-it/
- United Kingdom: https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks
- USA: https://www.cisa.gov/stopransomware

3.3 Other types of blackmail targeting companies

Ransomware attacks are not the only type of cyber blackmail that companies face. Overall, there has been an increase in blackmail.

3.3.1 *Data disclosure blackmail (data leak):*

In this case, the hacker steals data but does not attempt to lock the victim's computers (as ransomware would). The hacker may not even have infiltrated the internal networks of the target company, but has stolen the data from an exposed system on the internet, or from a partner company of the victim. This type of attack increased in 2021 and will no doubt continue to do so in 2022. For example, Qualys was targeted in March 2021 following the Accellion FTA attack.

3.3.2 *DDoS attacks (ransom DDoS):*

The hacker threatens to block internet access if a ransom is not paid and makes a show of strength by conducting an initial short-lived attack. This type of attack, which already existed in the 2010s for online betting sites, returned in September 2019, this time targeting any type of business. Since then, the phenomenon has remained largely under the radar but regularly continues to target new victims. These ransom DDoS (RDDoS) attacks now appear in a dedicated section in the quarterly reports of almost every anti-DDoS protection vendors (which shows that this is an established threat).

3.3.3 *Soon, information attacks?*

In the future, companies might need to deal with a new category of threats: information attacks (dissemination of false information via social media, or even cyberattacks designed to harm a company's image). For now, these types of attacks is mostly used by state-sponsored attackers, and does not specifically target companies. But as we know, state-sponsored attacks often serve as a model for other attacks on a wider scale. For example, APT attacks started as a military tactic, were then used more widely for economic motives, and are now also used by cybercriminals.

3.4 Cryptocurrencies: attacks on platforms and assets increased

Attacks on cryptocurrencies, security issues with exchange platforms and attacks on specific decentralised finance (DeFi) protocols were covered more than ever in the IT media in 2021. **It was a record year for theft and misappropriation of cryptocurrencies**, whether conducted by fraud or cyberattacks. In total, the amounts stolen are estimated to be around $14 billion — almost double compared to the previous year.

Misappropriation of cryptocurrencies can take different forms, depending on whether the attacker is targeting the end user, an investment company or a trading platform, or directly targeting the implementation of a protocol. Note also that DeFi protocols / platforms can also be used for money laundering, although it is currently difficult to obtain precise figures on this.

3.4.1 Attacks on trading platforms and DeFi protocols

These are the most high-profile events ($2.2 billion in 2021 according to ChainAnalysis), although they do not necessarily account for the bulk of the money stolen. The most regularly targeted DeFi protocols are, in order, Ethereum, Binance, Polygon and Avalanche. These attacks often exploit the fact that online platforms (see the incidents at Grim Finance, AscendEX, Vulcan Forged, BitMart, Badger, etc.) do not properly implement a smart contract. *Note: A smart contract is a computer protocol often implemented via a blockchain that facilitates, verifies and executes the negotiation or execution of a contract*.

In 2021, the largest theft was suffered in August by the PolyNetwork platform for $600 million. In this particular case, 99% of the stolen money was returned shortly afterwards by the hacker, who mainly wanted to expose a vulnerability in a smart contract managing the exchange of liquidity from one blockchain to another.

However, it is also common for theft from trading platforms to be carried out via a more conventional intrusion. For example, a developer at the bZx platform fell victim in November 2021 to a spear phishing email with a malicious Word attachment, leading to the theft of a cryptocurrency wallet and the loss of $55 million for the company.

The trading platform / DeFi sector is ultimately subject to the same problems as the banking sector. It is targeted to an extreme extent because of the opportunities for gains for the attackers. But the new technologies they implement, especially the codes for smart contracts, will need to be the subject of special attention and investment in terms of security (code security, encryption, data protection, staff awareness, etc.).

3.4.2 Scams

Scams of all kinds are believed to account for just over half of all cryptocurrency misappropriations in 2021 ($7.8 billion). Currently, the so-called “rug pull” crypto scams seem to be the most effective and widespread. Taking advantage of the gullibility of some first-time investors, malicious individuals lay the groundwork for a bogus cryptocurrency project, but credible enough at first glance, in order to gather a "pool" of investors. These projects are often backed by a huge marketing campaign aimed at influencers on social networks. The fear of missing out on a promising investment attracts more and more people. This drives up the initial price of the token, which in turn generates even more expectation. Once enough funds have been collected, the scammers shut down or simply abandon the platform and disappear with the cash. The most well-known case of this type of scam in 2021 is Thodex, a Turkish cryptocurrency trading platform, whose CEO and founder disappeared in April after siphoning off $2 billion.

In the near term, in the absence of any regulation, only a massive effort to raise user awareness would help bring down these figures. In the longer term, the industry may have to take more drastic measures to prevent tokens associated with potentially fraudulent or dangerous projects from being listed on the major exchanges (systematic audits, pentests, etc.).

3.4.3 *Outright theft from users*

Many attacks are simply aimed at the end user / small holder with the purpose of stealing their cryptocurrency wallet, or making them transfer funds without their knowledge. These attacks are carried out using relatively unsophisticated malware, yet they generate millions of dollars. They can be categorised as follows:

- **Stealers** (for example, Redline and Cryptbot): This type of malware steals the cryptocurrency wallet itself. They retrieve addresses they find in the clipboard. Then they scan the system for associated passwords, or install a keylogger module to retrieve these passwords more directly.
- **Clippers** (for example, Hackboss and MyKings): This malware replaces the cryptocurrency wallet addresses it finds in the clipboard with the address of a wallet owned by the hacker. Because addresses are long, random strings of numbers and letters, the victim may not realise when transferring funds.

3.4.4 *Cryptojacking, still a safe bet*

Cryptojacking refers to an attack that consists of utilising the processing power of a compromised system to mine cryptocurrencies (usually Monero XMR) without the machine owner's knowledge. It is hard to gauge the amount of profits generated by this type of threat, but according to ChainAnalysis they account for three-quarters of the sums in cryptocurrency from malware, excluding ransomware.

Around 2018, it became apparent that cryptojacking was gradually moving away from the average user's desktop and toward servers and thus businesses. In early 2021, Cisco even estimated in a report that 69% of its customers had been affected by cryptojacking in 2020. In 2021, cryptojacking seemed to generate more and more profits by compromising servers through known vulnerabilities in applications such as Microsoft Exchange (ProxyLogon, ProxyShell), Oracle WebLogic, Atlassian Confluence, ElasticSearch and Docker. The threat is taking on an increasingly industrial dimension in the form of botnets of several thousand compromised machines, which continually scan the internet for new vulnerable targets. The most active of these in 2021 include TeamTNT, LemonDuck, Z0Miner, Kinsing, Sysrv, Freakout and Glupteba.

3.5 Supply chain attacks

3.5.1 *Several types of attacks*

Since the SolarWinds Orion attack, revealed in late 2020, attacks through suppliers (supply chain attacks) have become a concern for many companies.

This is a complex problem that includes several categories of attacks. There is no definition of what falls under “supply chain attacks” (see § 3.5.3 below), but the main categories are:

- Attack via an MSP (managed services provider): An MSP with access to a company’s network is attacked. Its privileged access is then used by the hacker to infiltrate the target company.
- Attack via another provider or partner (other than an MSP).
- Attack via software or hardware supplied by an official vendor. The software (or hardware) will have been previously compromised, without the vendor’s knowledge.

Note: there are other categories that may or may not (depending on the viewpoint) be added to these three categories. For example “attack via a cloud service”, which may be considered as a special case of an attack via an MSP, or as a category in its own right.

The category of attacks via software or hardware tends to attract the most interest in the security community. Some even think that these are the only real “supply chain attacks”, which is a bit simplistic. We discuss this category in more detail below (in § 3.6).

3.5.2 *Mitigation solutions already exist*

Here are two examples of measures to limit the risk of attacks via suppliers:

- Organisational solution: Identify your key suppliers, inform them of your concerns about the risk of a supply chain attack and ask them to implement measures to reduce the risk and impact.

  This is a conventional approach already adopted by many companies in the field of IT security and which leads, for example, to the addition of specific contractual clauses.

- Technical solution: Limit the computer access granted to MSPs (e.g. for remote maintenance) and ensure they are strictly managed and monitored.

  This type of measure is already widely applied and is often accompanied by specific equipment (such as jump hosts) to monitor and control remote access.

3.5.3 Is there a definition of “supply chain attack”?

• According to the Mitre Att&ck model

In the Att&ck matrix, Mitre defines two distinct techniques:

- **T1195 – Supply chain compromise**
  This technique includes all attacks aimed at manipulating software or hardware prior to receipt by the victim. Interception of a package during shipping is part of it.
- **T1199 – Trusted relationship**
  This technique includes all attacks that utilise (unknowingly) an authorised access granted to a provider.

Because of this distinction, the Att&ck project clearly considers that only T1195 attacks (the third category in our analysis in § 3.5.1) are supply chain attacks.

• According to ENISA

In July 2021, the European Union Agency for Cybersecurity (ENISA) published a report (entitled: Threat Landscape for Supply Chain Attacks) that analyses 24 recent supply chain attacks. The types of attacks are varied, and ENISA uses a broader definition than the Mitre Att&ck framework. In the taxonomy it proposes, ENISA considers that a supply chain attack occurs whenever the hacker follows two steps. First, it targets the supplier. Then second, it exploits the advantage gained on the supplier side to attack the final victim (who is a customer of the supplier and the original intended target of the overall attack).

3.5.4 A difficult attack for the perpetrators as well

At the BruCON security conference in September 2021, Joe Slowik presented an original perspective by asking the question: How hard is it to carry out a supply chain attack?

If the attacker does not have a specific target, attacking via the supply chain is not especially difficult — it can be an effective way to reach a large number of victims by compromising a single component (such as a popular software library).

But if the attacker is targeting a specific victim or business sector, then devising a supply chain attack becomes much more complex because two parameters must be controlled:

- The scope of distribution of the attack. Does the attacker take the risk of unlimited distribution, which is bound to be detected by at least one victim, or control the distribution?
- The level of control over the final target. Can the attacker establish a direct channel of communication with the final target, or must he continue to act through the supplier to perform actions at final target side? Does the attacker choose an autonomous (worm) or a managed attack code?

Overall, except in the case of an attack with no specific target, carrying out a supply chain attack is a complex task and is only of interest to hackers if a conventional attack (not via a supplier) is too difficult.

3.6 Source code: a new target of attacks

In 2021, there was a lot of talk about supply chain attacks targeting development environments and developed software. In this case, the "supplier" is the developer of the source code and the final victim is the company that uses the developed code. In this dedicated section, we deal with this particular case of attacks via the supply chain.

3.6.1 Attacks aimed at source code

Attacks on source code are still relatively low-profile phenomenon, but they gained significance in 2021, and this trend is likely to continue. It takes two forms:

- Theft of source code.
- Insertion of malicious code.

Theft of source code has been observed in several security incidents. Microsoft and MimeCast, for example, said that, when they were hit in 2020 by the SolarWinds attack, one of the actions of the (allegedly Russian) hackers was to access the source code of some of their products. We also know of at least one other non-public case of a similar incident (separate from SolarWind).

This is a weak trend (little discussed), but it should be taken seriously. It can be summarised as follows: some hackers are keen to steal the source code of products, probably to look for vulnerabilities, or maybe to gauge the possibility of inserting malicious code.

Insertion of malicious code is a widespread phenomenon and it increased in 2021 with attacks such as:

- Direct compromise of open-source libraries (e.g. through poorly protected or stolen access rights). This type of attack has been ongoing for several years and mainly affects code sharing repositories such as NPM (JavaScript), Maven Central (Java), NuGet Gallery (.net), RubyGems (Ruby) and PyPI (Python).
- **Dependency confusion attacks** (discovered in February 2021) that take advantage of dependency search rules during software generation and utilise these (often poorly understood) rules to have malicious libraries used instead of legitimate ones.

So far, attacks of this type have mostly been for relatively trivial malpractices such as installing a cryptominer or stealing Discord credentials. But there have also been cases where the attack was designed to steal Amazon AWS access keys. It is also theoretically possible to use these attacks to drop a backdoor inside companies that use one of the compromised open-source libraries.

Techniques for software supply chain attacks
From an article in the December 2021 Cert-IST monthly bulletin and based on a report from NIST and a report from Sonatype.

List of techniques cited by NIST:

- Manipulation via the update mechanism.
- Theft of the electronic signature of binaries.
- Compromise of open-source code.

For compromise of open-source code, Sonatype cites the following techniques:

- Attack by dependency confusion.
- Typosquatting.
- Malicious code injection.

For malicious code injection, Sonatype cites the following techniques:

- Theft of a developer account.
- Publication of a compromised fork of the legitimate project.
- Submission of manipulated contributions.
- Compromise of a developer's workstation.

3.6.2 Beware of DevOps and CI/CD attacks

Evolving technologies have led to significant advances in the world of software development in recent years, with DevOps (unification of application development and operations) and CI/CD (continuous integration, continuous delivery).

These approaches have resulted in undeniable progress. But in 2021, we noted that **DevOps and CI/CD security issues were the topic of many talks at conferences**. This shows that these technologies have reached a level of maturity that is prompting some to search for their weaknesses and vulnerabilities. Examples of the warnings issued by these researchers include:

- Beware of ghost instances: With CI/CD, the environments are very dynamic and Docker instances are automatically launched after each successful application generation. But it is not uncommon that, due to malfunctions, some Docker instances are not properly terminated and continue to run as a ghost. This raises concerns, such as: Do you know exactly which Docker instances are running? Are they all legitimate? Do you know how to identify a pirate instance that has been added to legitimate instances?
- Beware of rights granted to developers: If the developer can change the application generation rules, they can also take control of the production environment. Separation of duties and peer review of changes are important security concepts to protect against these types of internal attacks. They need to be translated into the DevOps world.
- Do you know who has modified a given source code? In the event of a security incident, it will need to be investigated to identify when the intrusion occurred. To do this, it is probably necessary to digitally sign the changes (commits) in the source code.

Another significant event in 2021 was the **Codecov.io attack**. Codecov.io is a company that offers continuous integration tools for the test phase (between the build and release phases of the DevOps cycle). In late January 2021, an attack on Codecod.io allowed a hacker to modify one of its tools (Bash Uploader). And for two months (before the attack was discovered in early April), a modified version was run by all of Codecov.io's customers using this tool. This allowed the hacker to gain illegal access to the development spaces of Codecov.io customers. For example, IBM and Rapid7 reported that they had been affected. This is an example of a cascading supply chain attack:

- The initial attack targeted Codecov.io.
- It enabled the hacker to attack Codecov.io customers (for example, IBM and Rapid7).
- And eventually to compromise the code developed by these customers, so that the hacker could then attack the customers of those customers.

3.6.3 Securing development environments: a long-term effort

Attacks on source code and the software supply chain highlight the need to strengthen the security of development environments. This is especially true since in recent years we have moved from a traditional segmented model (with a clear boundary between development, delivery and operation) to a continuous model (DevOps), which is much more dynamic and is often directly connected to Cloud services (SaaS) on the internet.

The problem is complex and has multiple dimensions:

- How to manage vulnerabilities in the libraries (dependencies) used by the project?
- Do the CD/CI tools used create security issues?
- How to reconcile a continuous DevOps approach with a security need for separation of roles?

It is clear that this is a long-term endeavour. But the attacks observed in 2021 show that it is important to start thinking about this issue now.

3.7 Rise in the number of vulnerabilities

3.7.1 Patch strategy and management of urgent fixes

With the increase in the number of vulnerabilities discovered and, in turn, the number of patches released by vendors, companies are faced with the increasingly difficult task of deploying these patches. Most companies distinguish between two processes:

- Routine deployment of regular patches (during scheduled maintenance slots).
- Management of urgent patches.

And the increase in the number of vulnerabilities mainly affects (in terms of workload):

- The upstream triage operation (before these two processes) to decide which patches are urgent (vs regular).
- Deployment of the urgent patches. Conversely, adding patches in the “routine patches” category has little impact, because this process deals with a (usually large) set of patches has a single batch to be tested and deployed.

The general principle for defining urgency is fairly well established: a vulnerability is urgent if it is severe and an exploit program exists. But assessing severity is too often influenced by the amount of discussion about a vulnerability (the hype about the vulnerability).

• Beware of media hype

In 2021, there were several high-profile vulnerabilities in the media (such as PrintNightmare and SeriousSAM) that are “just” escalation-of-privilege attacks: a hacker who has already gained access to a company uses this flaw to gain higher-level privileges. The fact that it is an internal attack (the hacker must already have access to the company) reduces the risk and thus the severity of such vulnerability. It seems to us that the hype surrounding these vulnerabilities is due more to the interest of researchers in the problem raised (with a series of patches and circumvention of them) than the actual severity of the vulnerability.

To limit these “hype” effects, it is important to define in advance the “urgency” rules that will be used to triage new vulnerabilities. For example, decide whether an escalation-of-privilege vulnerability should (or should not) prompt an urgent deployment.

• Vendors need to design more reliable software

The number of security patches released each year is constantly increasing. While we cannot complain that vulnerabilities are being fixed, we sometimes wonder about the quality and reliability of the code. We also know that when a vulnerability is fixed, researchers will be interested in the problem raised — either to find a way to circumvent the fix, or to find a similar problem elsewhere. So, it is important to be extra vigilant when fixing a vulnerability, to avoid incomplete fix.

Since code quality has been a long-standing issue and there does not seem to be enough improvement on this front up to now, some people now think that only a legal requirement will lead to significant improvement.

3.7.2 2021: Annus horribilis for Microsoft?

Microsoft had some hard times about security in 2021, with in particular:

- The Exchange ProxyLogon (March 2021) and ProxyShell (August 2021) attacks. The wave of ProxyLogon attacks in March may have been due to details released by Microsoft to its partners under the MAPP programme.
- PrintNightmare (July 2021), with many twists and turns (waiting for patches, then incomplete patches) and malfunctions caused by the patches released by Microsoft.
- PetitPotam and NTLM relay attacks. This type of attack was already known and shows the weaknesses of NTLM authentication in Windows. It was discussed a lot in 2021 with the PetitPotam vulnerability. NTLM is considered obsolete by Microsoft, but it still has a strong footprint in the Windows environment (difficult to do without it). And its successor (Kerberos) is also known for its weaknesses (Golden Tickets and DCSync attacks).
- OMIGOD: A critical vulnerability in an open-source component developed by Microsoft (Open Management Infrastructure, OMI) that is automatically installed by Microsoft in some Linux VMs deployed in Azure.

Other Microsoft vulnerabilities were reported in the media in 2021, such as **SeriousSAM** (a privilege escalation via the Windows registry). But it is a conventional vulnerability which, on its own, has nothing unusual about it.

Concerning vulnerability tracking, Microsoft changed its security bulletins in 2021 (much to our regret), which now contain (mostly) no description except a CVSS note. After the discontinuation of the famous “Microsoft Security Bulletins” in 2017 (MS17-023 was the last one), with a level of detail always cited as exemplary, the Microsoft bulletins are getting worse and worse.

3.8 Log4j: what we learned from it

The Log4j vulnerability (announced in December 2021) has caused companies to work hard to identify and protect vulnerable installations. It is one of the most significant vulnerabilities of the year. After a massive wave of all-out attacks in December (conventionally referred to as “spray and pray” — i.e. “spray” randomly and “pray” the attack works in a few places), more selective attacks (targeting specific applications) will likely continue throughout 2022. This issue is not closed and the application of patches on all vulnerable systems must be continued.

The most striking aspect of this vulnerability is that it impacts a large number of applications, and identifying these applications is a complex task. It is therefore advisable for companies to have a **software map**, which indicates for each application which external components (libraries) are used. This corresponds to the concept of a **Software Bill of Materials (SBOM)**, which the United States is actively promoting:

- For example, the CISA considers an SBOM as a way to combat the VBOS phenomenon (vulnerability below the OS, i.e. vulnerabilities in low-level components such as the UEFI, see this presentation at the RSA 2021 conference).
- It is also a way to remediate software supply chain attacks more quickly.
- SBOM mapping was mentioned in an Executive Order in May 2021 signed by the US President as a way to improve security. Of course, it was not the only recommendation in this document, which also discusses concepts such as zero trust, EDRs, etc.

Building a software map is a huge task if conducted on a company-wide scale. We already know that it is difficult to identify all the machines and applications used in an organisation (due to shadow IT and legacy systems). Compiling an SBOM is an additional challenge. Nonetheless, in light of the Log4j crisis and the phenomenon of software supply chain attacks, SBOM mapping is a vital undertaking in the years ahead. A first step might be to request an SBOM for new systems installed at the company.

3.9 Geopolitics and state-sponsored attacks

Our analysis of attack reports, government alerts and indicators of compromise made public in 2021 does not show any dramatic change in terms of which countries are most reported as the source of attacks. Unsurprisingly, the bulk of attacks were attributed to China, North Korea, Iran and Russia. Out of habit, we tend to distinguish between cybercrime (for financial motives) and cyber espionage (traditionally associated with nation states). Today, however, we have to deal with state-sponsored threats that often combine both these aspects.

Attacks in 2021 were also influenced by the COVID-19 pandemic. Most cyber-offensive countries either attempted to spy on their counterparts to see how they were managing the crisis (vaccine development, treatments, infection rates, etc.) or simply used COVID as a theme for phishing campaigns. In fact, beyond governments, the pharmaceutical and medical sectors were especially widely targeted during the year.

3.9.1 China

The most active actor, based on the number of reported attacks, China was cited a huge number of times as the source of threats in CTI reports and at conferences in 2021. Its progress and presence in the cyber domain, including on the defensive side, is impressive. Anecdotally, but indicative of this progress, we had to process a large number of attack reports written in Chinese in 2021, which was rarely the case before.

Beyond the purely offensive aspect (the Chinese actor most mentioned in OSINT reports in 2021 was the meta-group APT41/Winnti linked to the Ministry of State Security), we also note that China is becoming increasingly independent from the rest of the world:

- For several years, China has been compiling its own catalogue of vulnerabilities (the CNVD, equivalent to America's NVD database).
- In 2018, China banned its citizens from taking part in international 0-day vulnerability contests such as Pwn2Own and created a Chinese equivalent called the Tianfu Cup.
- This year, China made it mandatory for its citizens to report any 0-day vulnerabilities they discover to the Chinese government and forbids them to disclose vulnerabilities to anyone other than the affected vendor. This also gives the Chinese government a clear advantage in terms of attacks.

3.9.2 North Korea

Noted in 2020 for its "Dream Job" campaigns, North Korea remained active in terms of social engineering and cyber espionage in 2021. These operations, which combine phishing emails and solicitations via social networks, typically targeted employees of technology companies with supposed job offers. In 2021, some of these attacks specifically targeted security researchers via fake Twitter and LinkedIn profiles.

But the North Korean threat (the cyber community divides it into two major groups: Lazarus and Kimsuky) is characteristic because of the economic restrictions on the country and its isolationist policy.

2021 showed once again that the country's government is ramping up offensives aimed at retrieving cash, through targeted ransomware attacks, various forms of extortion and, increasingly, theft of cryptocurrency. The country is believed to have generated $400 million in just seven successful attacks in 2021 against centralised cryptocurrency exchange platforms and investment companies. This does not include the large number of campaigns we have observed that directly target small holders by means of fake crypto trading apps. The UN recently stated in a report that North Korea was investing the proceeds from cybercrime (nearly $2 billion a year) in the development of nuclear weapons and other military technologies.

3.9.3 Iran

Known for their social engineering attacks via smartphones and social networks, as well as phishing campaigns targeting universities around the world, Iranian actors stepped up their offensive in 2021. For example, Microsoft noted a clear increase in brute force attacks (scanning and exploitation of VPN or Exchange server vulnerabilities, password spraying on Office365), with the aim of deploying ransomware or destructive malware (cf. the PAY2KEY, AGRIUS, Black Shadow, N3TW0RM and MosesStaff groups / operations). From political espionage and destabilisation (especially in Israel) to generation of financial profit, Iranian groups / modes of operation abound. It is reasonable to assume that for-profit attacks (i.e. ransomware) are used to finance larger cyber-espionage operations (such as this campaign against the telecoms sector).

On the cyberdefence side, we have seen that the level of technical expertise in some reports from Iranian cybersecurity companies (in particular the analysis of the iLOBleed rootkit targeting the iLO mechanism on HP servers) is remarkable, suggesting increased investments in this sector of activity.

3.9.4 Israel

In 2021, the most significant event was **Pegasus** (spyware theoretically sold to help combat terrorism but in reality widely used also to target civilians and opponents). Pegasus had been known since 2015, with misuse in some countries (United Arab Emirates, Mexico, Morocco, etc.). The revelations in the summer of 2021 show that these abuses are much more widespread than previously thought.

3.9.5 Russia

Russia has been highly advanced for several years in attacks against critical infrastructure (especially in Ukraine) and in manipulation (information attacks and supposed collusion with Russian cybercriminal actors).

2021 was a rather exceptional year because a lot of reports were published in order to analyse in detail and draw lessons from the supply chain attack conducted around the world via the SolarWinds Orion software. The US officially attributed the SolarWinds attack to the Russian intelligence services as part of a series of sanctions against the country announced on 15 April 2021.

One of the surprising elements in the second half of 2021 is that we observed several cases of ransomware attacks targeting Russia, which until then was considered as a no-go and dangerous for Russian hacker groups.

3.9.6 United States

There were no high-profile offensive actions in 2021 attributed to the United States. We well imagine that there must have been some, but to date they have remained secret. The most remarkable effort is on the defensive side, with an **active fight against ransomware groups** and exemplary measures to strengthen infrastructure security with, for example, the **launch of the Known Exploited Vulnerabilities (KEV) catalogue**, which lists exploited vulnerabilities that must be fixed by US government agencies. The FBI and the Department of Justice are increasingly communicating publicly with, for example, alerts on ongoing threats, public attributions and indictments of Chinese, Russian and Iranian hackers.

3.9.7 And France?

France still remains low profile on the offensive front (no publicly known attacks since Babar and Animal Farm, revealed in 2015). Developments in 2021 include the creation of the L2I doctrine (for "*lutte informatique d'influence*", or cyber influence warfare, which supplements the 2018 "LID" defensive and 2019 "LIO" offensive doctrines) and the creation of specific CERTs for the healthcare, maritime, aviation and space sectors and regional CERTs.

4 Summary of Cert-IST activity in 2021

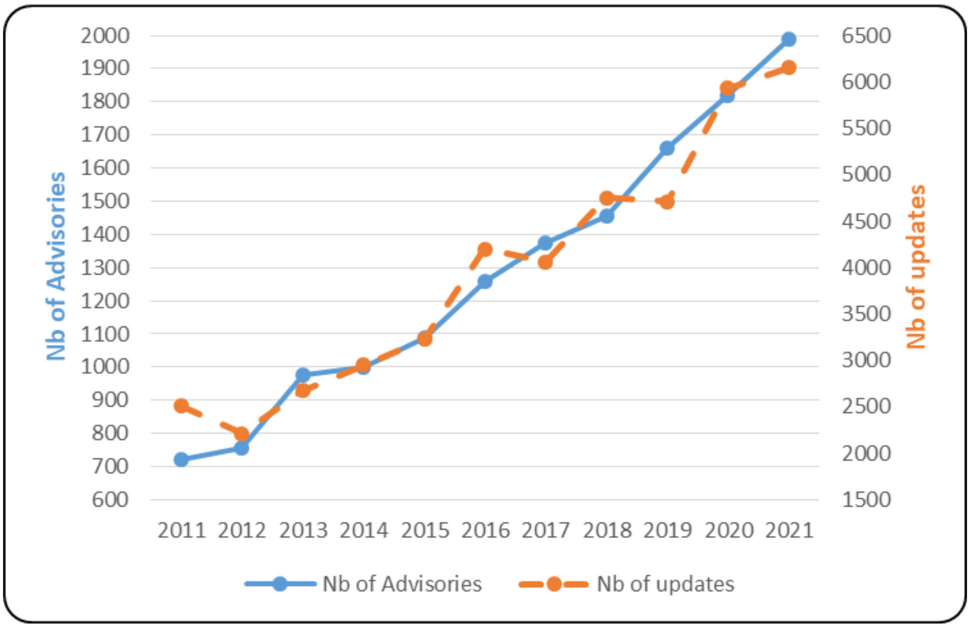
4.1 Vulnerability and threat feeds

As part of its monitoring activity on vulnerabilities and threats, Cert-IST continuously tracks various sources for information (vendor announcements, security blogs, mailing lists, communications between CERTS, etc.) in order to stay informed of new vulnerabilities. Every day, this data is analysed to provide our members with sorted, qualified and prioritised information.

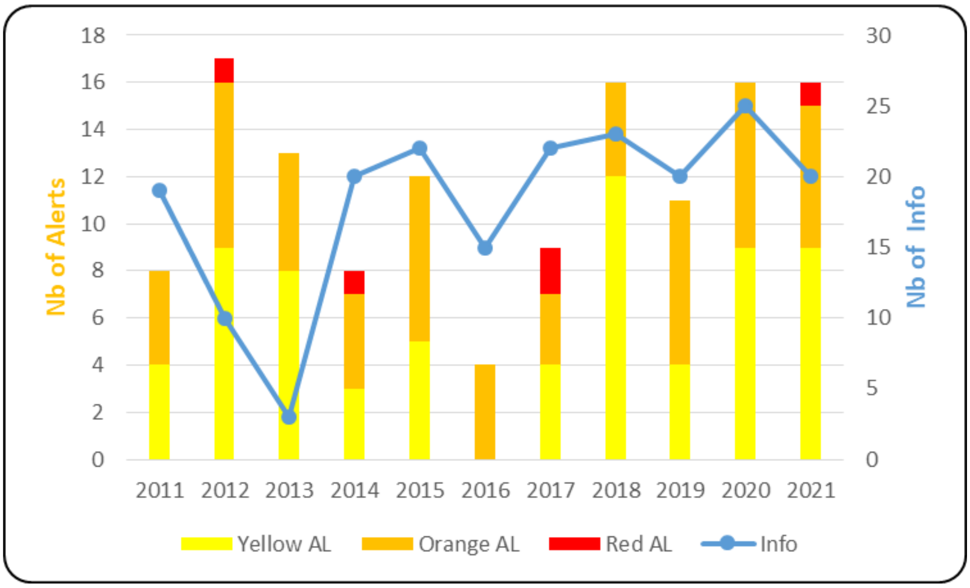
Cert-IST produces various types of publications:

- **Security Advisories (AV)**, which describe any newly discovered vulnerabilities in products monitored by Cert-IST. These AVs are continuously enriched with minor and major updates. The latter typically correspond to situations where exploits are publicly disclosed.
- **Alerts (AL)**, which are issued when there is a particular risk of attack, and **INFO messages**, which provide an analysis of particular vulnerabilities (often reported in the media) but of lower immediate danger level. These two categories focus on the attack risks, while security advisories systematically identify all vulnerabilities (regardless of their probability of being used in attacks).
- **Attack reports (ATK)** and **indicators of compromise (IOC)** via a shared MISP database. These list major attacks, whether they are recurrent threats (Malspam, Exploit Kits, Ransomware) or cyber-espionage incidents (APT attacks).

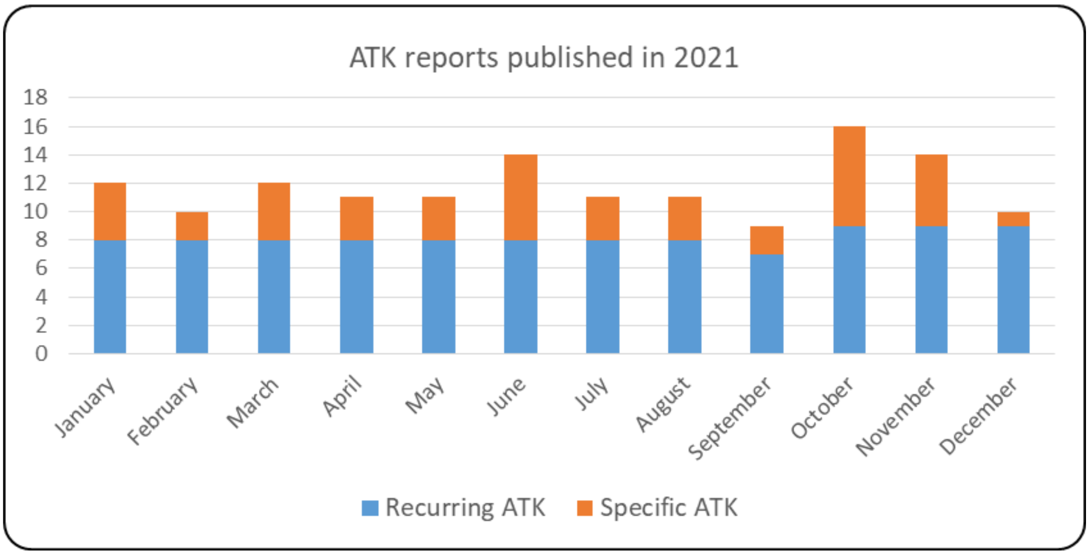
The graphs below show the number of Cert-IST alerts, reports, etc. over the last few years.



Number of security advisories published per year



Number of security alerts published per year



Number of ATK reports published per month

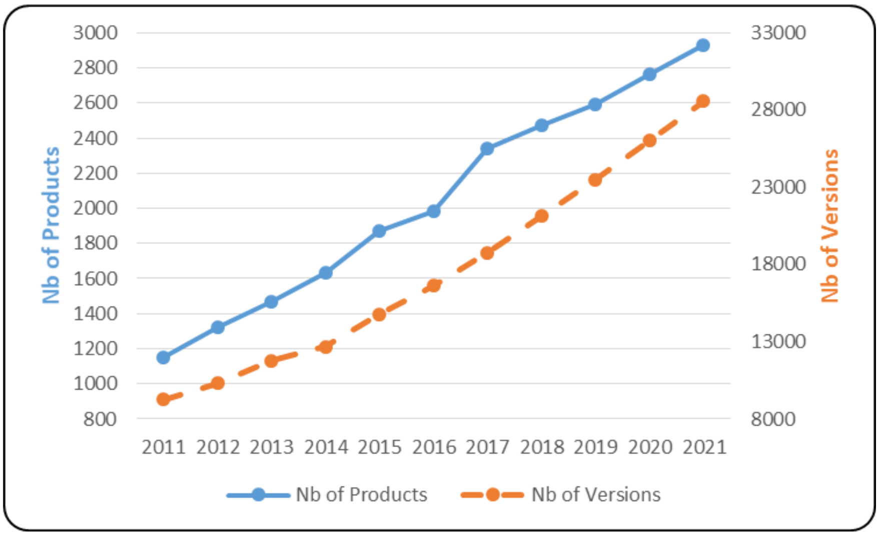
In 2021, Cert--IST published:

- **1,987** security advisories (including **79** SCADA advisories), **5,982** minor updates and **173** major updates.
  The number of advisories has been constantly growing in recent years (see graph), with a **9%** increase in 2021 compared to 2020. This steady increase shows that discovering vulnerabilities is an ever-growing phenomenon. Maintaining an adequate level of security still depends on the constant application of security patches for products in the information system.
- **16** alerts and **20** Info messages. In 2021, we issued a red alert for the ProxyLogon Exchange attacks. The previous red alerts were issued in 2017 (WannaCry and NotPetya). From year to year,

activity in this category fluctuates and there is no overall trend. It has remained relatively stable since 2018.

- **140** attack reports (ATK) were published in 2021, **3,453** have been enriched in the MISP database, and **793,185** indicators (IoCs) were added (there is a total of **5.5 million** in the database).

Regarding the catalog of tracked products monitored by Cert-IST, at the end of 2021 Cert-IST Cert-IST was tracking **2,930** products and **28,561** versions. The graph below shows the evolution of the number of products and versions monitored by Cert-IST over the year.



4.2 Technology Watch

In addition to vulnerability tracking, Cert-IST also produces technology watch reports:

- A **daily media watch bulletin (press review)** listing the most relevant articles about security issues posted on French and English language websites.
- A **monthly SCADA watch bulletin** providing a summary of current events related to the security of industrial systems.
- A **monthly general bulletin** summarising the month’s developments (in terms of vulnerabilities and attacks) and addressing current events through articles written by the Cert-IST team.
- A **monthly bulletin on attacks and IOCs**, which summarises the most significant events in the attack landscape.

5 Conclusions

The attacks on Exchange (ProxyLogon in March and ProxyShell in August) were among the major events of 2021. They confirm two trends that had already begun in previous years:

- Hackers are using all means at their disposal to gain access to companies. For a long time, the vector of choice was end users (with attacks via malicious emails) and their passwords (attacking weak passwords or stealing them by phishing). In the last two years, however, attacks targeting servers have been increasing.
- Cybercriminals are using this type of attack as much as cyber espionage groups. Gone are the days when infiltration attacks (APTs) were the preserve of the latter.

More generally, the line between state sponsored actors and cybercriminals is becoming ever more blurred:

- They use the same tools, such as PowerShell and Cobalt Strike. Of course, state-sponsored hackers have specific and more advanced tools, but for all the more mundane actions they use the same tools as cybercriminals.
- Some states (North Korea and possibly Iran) sometimes engage in cybercriminal behaviour and conduct attacks for the purpose of generating financial revenue.

Ransomware was still the most prevalent threat this year, and no company is immune to being attacked. If measures are not already in place, it is important to be prepared and study the various aspects of this type of crisis (see § 3.2.2).

Similarly, the security of computers used by people working from home is another urgent issue, if it has not already been addressed. Here, there are probably only two safe solutions (in terms of security): conventional full VPN access (as opposed to split VPN), which sends all traffic to the company, or a Zero Trust type solution, which natively addresses the issue of users at home and on the move.

In 2021, we saw a development in attacks targeting the Cloud, especially Azure and Microsoft 365. Vulnerabilities in Azure Cosmos, OMI (OMIGOD vulnerability) and brute force attacks on Azure passwords show that the search for vulnerabilities in the cloud is changing, with a greater focus on more technical aspects than previously thought. We can expect these Azure vulnerabilities to become more significant in the future.

Supply chain attacks continue to be a growing concern. The issue is complex because it covers several categories of attacks that would perhaps be better treated separately (see § 3.5.1). Part of the answer already exists, at least from a functional point of view (identifying suppliers, raising awareness of stakeholders, etc.) and best practices (limiting access by third parties, etc.). Protecting against supply chain attacks is clearly a difficult but important task, which must begin now.

Lastly, protection of development environments is a new concern. They are a target — for stealing source code, accessing related data or launching an attack on a third party (software supply chain attack). Evolving development methods with continuous integration (CI/CD), DevOps and the use of cloud-based tools (SaaS) increase the exposure of development environments to cyberattacks. Securing these environments is a long-term task, but it is important to be aware of this problem now and start acting to address it.

Cert-IST

290 Allée du Lac
31670 Labège
France

info@cert-ist.com

https://www.cert-ist.com

+33 (0)5 34 39 44 88