CERT-IST

INDUSTRIE | SERVICES | TERTIAIRE

Cert-IST annual report on attacks and vulnerabilities in 2022

Released in February 2023

Contents

1 Introduction

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

The report begins with a summary of the major security events in 2022 (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 cyberthreat landscape and the challenges companies will face in 2023.

➢ About CERT-IST

Cert-IST (**C**omputer **E**mergency **R**esponse **T**eam – **I**ndustry, **S**ervices and **T**ertiary) 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 2022

The table below gives a summary of the key events in 2022. These events are significant because they received a lot of media attention, or because they are indicators of cyber threat evolution.

January 2022	The Russian FSB arrests members of the **REvil** group. The FSB probably acted in response to pressure from the United States. It was likely a political manoeuvre to show Russian goodwill. It marks the end of this ransomware group, which had perpetrated the ColonialPipe and Kaseya attacks in 2021. It had already been partially neutralised in October 2012.
	Lapsus$, a cybercriminal group likely made up of 14 to 18-year-olds, successfully hacked into a series of major companies, among them Nvidia, Microsoft, Samsung, T-Mobile and Uber. The attacks were not particularly advanced, but the attackers were bold and do not hesitate to call their victims on the phone and persuade them to visit fake websites.
February 2022	$325 million was stolen in an attack on the **Wormhole cryptocurrency platform**. It was one of the largest-scale incidents of the year. But the record for 2022 was the **Ronin** incident in March ($625 million), which is attributed to the North Korea-based Lazarus group. And when **FTX filed for bankruptcy** (in November 2022), $477 million disappeared. **Globally in 2022, more than $2 billion was stolen in the cryptocurrency market**.
	24/02/2022: Russia declared war on Ukraine.
	Data breach at **CONTI**: After Russia declared war, a dispute broke out between the group's Russian and Ukrainian members. A large amount of internal data was made public. It shows that CONTI functions like a company, with about 100 employees, an HR department, etc. This data breach is detailed in §3.3.2.

February 2022	**Microsoft announced it was blocking macros** by default in Office documents downloaded from the web (there would no longer be a button to unblock them in the macros security message). But in early July, Microsoft backtracked. Then at the end of the month, it re-enabled blocking. Discussions turned to how to bypass **MOTW** (Mark of the Web), which Microsoft uses to determine whether a document has been downloaded from the internet, or other methods of circumvention (see Follina below, in May).
March 2022	**Spring4Shell:** After Log4Shell (vulnerability in the Log4J library), another vulnerability was identified in Java libraries. This time it affects the Spring.io framework. Fewer attacks were observed than Log4Shell (probably because the library is less widely used) but the Mirai botnet seems to have used it in April. In October, a third Java vulnerability was reported in the media. **Text4Shell** targets the Apache Commons Text library. To our knowledge, there have been no successful attacks via this vulnerability, because it is only found in certain very specific configurations.
	Okta announced that it too had been a victim of the Lapsus$ group. The attack took place in January at a subcontractor that provides technical support for Okta customers. The incident highlights the risk of attacks on outsourced activities (see § 3.6).
	CISA reported that it had observed **attacks targeting internet-connected UPS** (uninterruptible power supply) equipment with default passwords. This alert came a few weeks after the publication of a study by Armis called **TLStorm**, which revealed TLS/SSL vulnerabilities in UPS devices from APC. Apart from the type of equipment targeted, there is no connection between the two announcements.
April 2022	**PIPEDREAM:** This is the name given by Dragos (Mandiant called it **Incontroller**) for attack tools (probably Russian) targeting industrial systems (SCADA, OT, etc.). This discovery is hugely important and comparable to Stuxnet (see § 3.5).
	Costa Rica fell victim to a series of attacks using the CONTI ransomware. The ensuing chaos led the country's President to declare a state of emergency in early May.
May 2022	**ms-msdt** Office vulnerability (aka **Follina**). A researcher showed that it is possible to trigger code execution using a malicious Word document with the ms-msdt: handler. This vulnerability was widely publicised (perhaps because the attack is perpetrated without a macro) and attacks would later be observed.
	The **Raspberry Robin** malware was discovered by Red Canary. It was prevalent throughout the year. It spreads (among other ways) by infecting USB memory drives. This method, which was seen a lot in the past, had almost disappeared. According to the latest analysis, Raspberry Robin is a type of pay-per-install botnet. It installs malware on demand on the machines it has infected.
June 2022	**OT:ICEFALL:** Forescout published a study identifying 56 vulnerabilities impacting 10 SCADA vendors. In our opinion, this is one of the key events of the year in industrial system security (see § 3.5.1).
July 2022	A data theft **affecting a billion Chinese citizens** was discovered. On the Breach Forums hacker platform, a user going by the alias of ChinaDan put 23 TB of information up for sale relating to almost a billion Chinese people, for the price of 10 bitcoin.
	Zimbra Collaboration (webmail software) fell victim to a series of attacks in July and August exploiting the CVE-2022-27925 and CVE-2022-37042 vulnerabilities. In October fresh attacks were reported, this time using the CVE-2022-41352 vulnerability. **Pig Butchering scam:** The FBI warned against this type of scam, which involves convincing victims to join a group of cryptocurrency investors.

August 2022	**LastPass** (an online password vault service) announced that it had been breached and that source code had been stolen. Then in late December, LastPass announced that the hackers had come back and stolen user data (encrypted data but offline attacks are possible). LastPass did not provide much detail, which led many users to criticise the tool and call for its discontinuation.
	Log4J: CISA published the CSBR report on Log4J. The Cyber Safety Review Board was created by the US government after the SolarWinds attack in 2020 to analyse major attacks. Log4J vulnerability was discovered in December 2021 and was highly active in 2022 (see § 3.1.1) with mostly state-sponsored attacks.
	TLP 2.0: Version 2 of the TLP protocol was released by FIRST. TLP is a protocol that defines the distribution rules for a document. Note: another protocol widely used in the CERT community is PAP. It defines what a user is allowed to do with information they receive. TLP defines authorised distribution; PAP defines authorised use.
September 2022	**ProxyNotShell** vulnerabilities in Exchange. After ProxyLogon and ProxyShell in 2021, this third set of vulnerabilities was discovered in 2022. We discuss it (briefly) in § 3.1.1.
	MFA fatigue attack: An **Uber** employee was targeted using a new attack technique called MFA fatigue. We discuss it in § 3.8.1.
	Deadbolt: This ransomware appeared in January 2022 and specifically attacks **QNAP** NAS servers (and ASUSTOR) exposed on the internet. It was widely discussed throughout the year, especially in September.
	Optus, one of the main telecom operators in Australia announced it had suffered a data breach (10 million customer accounts). The theft was due to a **lack of protection of APIs**. The attackers demanded a hefty ransom to keep the data from being published. But in the end they gave up, probably for fear of prosecution.
	Edward Snowden was granted Russian citizenship. He received his Russian passport in December. Since his revelations about the NSA in 2013, Snowden has been a refugee in Russia.
October 2022	**Fortinet** was affected by several critical vulnerabilities. In October it was the CVE-2022-40684 vulnerability. It concerned the Fortinet administration interface, which should never be exposed on the internet, but ShadowServer reported that 17,415 devices were exposed. In December, the CVE-2022-42475 vulnerability was discovered in the highly sensitive SSL VPN service. Fortinet was criticised for having only released the information to its premium customers, leaving other customers unaware of the vulnerability for a significant period of time (which attackers could exploit).
	BlueBleed data breach at Microsoft. **SocRadar.io** discovered that Microsoft had improperly secured a cloud storage space (Azure Blob Storage), which it uses to store customer data. It could have allowed a third party to illegally access this data.
November 2022	**Opera1er:** GroupIB and Orange revealed the existence of a group of French-speaking hackers targeting banks in Africa. They had allegedly stolen more than $30 million in 30 attacks from 2019 to 2021.
December 2022	**ChatGPT** demonstrated the capabilities of an AI engine. AI has many possible uses, and some worry it could be used to write malware.

3 Analysis of the most significant phenomena in 2022

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

- The main **vulnerabilities**
- **Infostealer** malware dominates the news
- A year of stabilisation for **ransomware**?
- **Russian-Ukraine** war redefines the role of cyber in a conflict
- **SCADA** threat increases with PIPEDREAM malware
- **Supply chain** attacks also target outsourced activities
- Rise of **hackers-for-hire** and offensive products for states
- Other phenomena observed:
  - Attacks on MFA
  - Attacks on satellites?
  - BruteRatel and the new offensive tools
  - Windows: Bring Your Own Vulnerable Driver
  - Fewer exploits published before attacks

3.1 The main vulnerabilities

3.1.1 At a glance

The most notable attacks in 2022 were on these products:

- **F5 BIG-IP:** CVE-2022-1388 vulnerability, which triggered the CERT-IST/AL-2022.006 amber alert in May.
- **Atlassian Confluence Server:** CVE-2022-26134 vulnerability (CERT-IST/AL-2022.008 amber alert in June).
- **Fortinet:** CVE-2022-40684 vulnerability (CERT-IST/AL-2022.012 amber alert in October), then CVE-2022-42475 (CERT-IST/AL-2022.015 yellow alert in December).
- **Zimbra Collaboration**. CVE-2022-27925 and CVE-2022-37042 vulnerabilities (in August) and CVE-2022-41352 (in October). Note: this product was added to the Cert-IST list of monitored products in late October and has therefore not given rise to any Cert-IST alerts. However, we issued the **INFO-2022.019** message.

Some of the vulnerabilities we reported in 2021 remained highly prevalent in 2022:

- **Microsoft Exchange:** After ProxyLogon and ProxyShell in 2021, a third set of vulnerabilities called **ProxyNotShell** was discovered in 2022. These vulnerabilities were used in 0-day attacks starting in July 2022 by state-sponsored (probably Chinese) hackers. Microsoft patches have been available since October, but attacks increased in late 2022 after an exploit program was released.
- **Log4J:** This vulnerability was discovered in December 2021 but had ceased to be in the news by late January. However, it continued to be used in attacks after this, with for example state-sponsored attacks reported by Ahnlab (a South Korean company) in May, US-CERT in June and Microsoft in August.

3.1.2 Other attacks in 2022

The table below details the 16 alerts issued by Cert-IST in 2022.

Alert	Reference	Description	Date
Yellow	CERT-IST/AL-2022.001	Attacks expected against Linux/Unix systems (vulnerability in pkexec tool of **Polkit package**)	26 Jan. 22
Yellow	CERT-IST/AL-2022.002	Attacks expected against **SAP Applications** using the Internet Communication Manager (ICM) component	10 Feb. 22
Yellow	CERT-IST/AL-2022.003	Attacks expected with **"Dirty Pipe"** against Linux systems (CVE-2022-0847)	10 Mar. 22
Yellow	CERT-IST/AL-2022.004	Attacks for **VMware Workspace ONE Access and Identity Manager** (CVE-2022-22954)	14 Apr. 22
Yellow	CERT-IST/AL-2022.005	Attacks expected for **Microsoft** RPC (CVE-2022-26809)	15 Apr. 22
Amber	CERT-IST/AL-2022.006	Ongoing attacks against **F5 BIG-IP** (CVE-2022-1388)	9 May 22
Yellow	CERT-IST/AL-2022.007	Attacks expected for **VMware Access, vIDM, vRA, and vRealize Suite Lifecycle Manager** (CVE-2022-22972)	27 May 22
Amber	CERT-IST/AL-2022.008	On-going attacks against **Confluence** servers (CVE-2022-26134)	3 Jun. 22
Yellow	CERT-IST/AL-2022.009	On-going attacks using the Windows MSDT **"Follina"** vulnerability (CVE-2022-30190)	8 Jun. 22
Yellow	CERT-IST/AL-2022.010	Attacks expected for **VMware Access, vIDM, vRA, and vRealize Suite Lifecycle Manager** (CVE-2022-31656, CVE-2022-31659 and CVE-2022-31660)	11 Aug. 22
Yellow	CERT-IST/AL-2022.011	0-day attacks against **Microsoft Exchange** (ProxyShell variant)	30 Sep. 22
Amber	CERT-IST/AL-2022.012	On-going attacks against devices running on **FortiOS** (CVE-2022-40684)	17 Oct. 22
Amber	CERT-IST/AL-2022.013	On-going attacks against **Adobe Commerce** (formerly Magento Commerce) with CVE-2022-24086	16 Nov. 22
Yellow	CERT-IST/AL-2022.014	Attack expected for **F5 BIG-IP** (CVE-2022-41622)	22 Nov. 22
Yellow	CERT-IST/AL-2022.015	On-going attacks on devices running on **FortiOS** (CVE-2022-42475)	13 Dec. 22
Yellow	CERT-IST/AL-2022.016	Attacks against **Citrix Application Delivery Controller (ADC) and Citrix Gateway** (CVE-2022-27518)	14 Dec. 22

3.2 Infostealer malware dominates the news

3.2.1 *At a glance*

Several times in 2022, media reports showed that some attacks on companies were perpetrated without exploiting vulnerabilities:

- Hackers purchase stolen authentication data from the website of an initial access broker (IAB).
- They then use this data to gain access to a company. Depending on the case (and the level of protection), they enter the company (via theft of a VPN account) or simply an outsourced cloud service (for example a private GitLab or GitHub space).

These attacks work well because remote access has become widespread (with homeworking, the cloud and de-perimeterisation) and attacks against MFA have been developed (see § 3.8.1). They are generating growing demand on the IAB market, driven by a type of malware called infostealers.

An infostealer is a malware designed to steal authentication data on the victim's computer (saved passwords, session cookies, etc.), cryptocurrencies and some related technical data. The best known infostealers are **Racoon** and **RedLine**.

In 2022, we observed a massive increase in attacks using infostealers.

Note: after infostealers, **the other significant class of malware of the year is Wiper**, which has been used constantly in cyberattacks by Russia against Ukraine (see § 3.4.1).

3.2.2 *Infection chain: from web browser to botshops*

Here is a typical sequence of events when a machine is infected by an infostealer:

- The victim downloads a piece of "cracked" software. These programs almost always contain malware, often an infostealer.
- The infostealer steals the account information and passwords the user has stored in their web browser. If the user has activated synchronisation of web data between browsers, the data for their work accounts can sometimes be found on their personal device(s) as well.
- The stolen accounts are sent by the malware to the hacker, who then offers them for sale on a merchant site called a **botshop** or **logshop**. The most famous is Genesis. These "stores" sell the complete dataset harvested from the infected machine. This batch of data is called a "log". It contains login details, cookies and the technical characteristics of the machine (screen resolution, CPU, RAM). This array of information allows the hacker to impersonate the victim's computer and thus bypass anti-fraud protections (tools that detect bots and fake clicks).

3.2.3 How do I stay protected?

We have not seen any specific studies that suggest solutions to these types of infostealer attacks, but the guidelines below should be considered:

- Educate users about the dangers of software downloaded from the internet (at home and at work). In addition to pirated software (which is illegal), users should be careful when they download software, because some sites offer malicious versions of original free software. So, always look for the official website (for example via its Wikipedia page) rather than downloading from the first website in a Google search.
- Avoid saving logins and passwords in a web browser, because many malware programs can steal them from here. It is better to use a password safe or vault (like KeePass), which are much less exposed to this type of attack.
- Never sync your work accounts between multiple devices. And never use your company account passwords for other accounts or for non-company websites.
- Investigate the possibility of monitoring whether company-related accounts are being offered for sale in IAB marketplaces.
- When an infostealer infection is detected, determine which accounts have been compromised and have the passwords changed.

3.3 A year of stabilisation for ransomware?

3.3.1 At a glance

Below is the headline article of our December 2022 monthly bulletin, which outlines the trends we observed. Overall, in 2022:

- There was a drop in the number of ransomware attacks in the first half of the year. At the same time, Blackmail attacks with data theft accounted raised.
- But ransomware attacks were back in force from September.

Headline article of the Cert-IST monthly bulletin for December 2022 (published in January 2023):

Since the beginning of 2023, many articles has been published about the future evolution of ransomware. Without making any predictions, following are some trends we saw during our activity.

- 2022 was a year of stabilization, while 2021 was the year of explosion of the number of attacks disclosed. According to French journalist Valérie Reiss-Marchive (from LeMagIT), who spoke at our Forum 2022 event in December (see our article later in this Bulletin), there were in France in 2022 almost the same number of attacks as in 2021 (see LeMagIT article).

- There have been many attacks on healthcare organizations. However, it is not certain that this sector of activity is more targeted than the others and the explanation may be that more attention is paid to these attacks.

- At the beginning of 2022, "true" ransomwares were rather on the decline in favour of data theft attacks (and blackmail to disclose stolen data). These latter incidents are often referred to as "data-leak extortion". True ransomware came back in force later, especially from September 2022 onwards.

- We should find another word to replace “ransomware", because nowadays this word is used both for real ransomware and for data-leak extortion. The word ransomware tends to be used for any cyber-criminal intrusion that leads to blackmail.

- An increasing number of states are using ransomware attacks. (cf. TheRecord.media) Sometimes it is to hide a sabotage action (it is made to look like a ransomware, but the goal is to block the computers and there is no ransom negotiation). This was seen in 2022 for instance in Russian attacks against Ukraine or in Iranian attacks against Israel. Other times it is an attack to capture currency, especially for embargoed countries. North Korea has been practicing these attacks for several years, and Iran seems to be doing so since 2021.

Note: Here are some articles on this subject, in addition to those cited above: TheRecord.media 2, Trend Micro, EMSI soft, BlackFog.

3.3.2 The unexpected effects of the Russia-Ukraine war and the CONTI leak

Many cybercriminal groups are based in Russia and satellite countries. It is therefore possible that the drop in ransomware attacks in the first half of 2022 is related to the Russian invasion of Ukraine and the suspension of activities by some cybercriminals. This is only a theory, but it is believed that various cybercriminals were arrested when they left Russia's area of influence because of the conflict. Examples may include the author of the Zeus malware and the author of the Racoon malware.

The CONTI ransomware group disbanded at the start of the war because some members were pro-Russia and others were pro-Ukraine. A huge amount of internal data was made public when the group broke up, including new information about its structure. CONTI was one of the most significant ransomware groups. The leaked data showed it had a team of 80 to 100 people and a company-like structure, with its own HR department, teams responsible for infrastructure and a substantial budget for buying services (e.g. to obtain financial information about target companies) and software (e.g. to buy adversary software like Cobalt Strike).

3.3.3 The fight against ransomware groups is intensifying

Ransomware groups continued to be highly active in 2022. But the fight against these groups also continued. For example, members of the REvil and Lapsus$ cybercriminal groups were arrested in 2022 and the HIVE group was neutralised in early 2023.

Since May 2021, with the Colonial Pipe incident in the United States, governments have stepped up their fight against ransomware. This was one of the key phenomena we identified in our 2021 report. This effort clearly continued in 2022.

3.4 Russian-Ukraine war redefines the role of cyber in a conflict

3.4.1 At a glance

Russia’s invasion of Ukraine is the first example of cyber playing a full part in an armed conflict. Russia has high levels of expertise in this weapon and has been carrying out large-scale cyberattacks against Ukraine since 2015.

We probably don’t know the full extent of the cyberattacks perpetrated by Russia and Ukraine. But we note the following:

- There has been no “cyber Armageddon” (i.e. complete chaos caused by an all-out cyberattack). Cyber weaponry seems to be more about reconnaissance and destabilisation than total destruction.
- The Russian attacks we know about are mostly wipers (software designed to erase data on infected computers and disable them). Apart from wipers, the most notable attack was on KA-SAT satellite modems (used by the Ukrainian military to access the internet). See § 3.8.2.
- In addition to the state-sponsored attacks, there has been a significant mobilisation of hacktivists, who perpetrate pro-Ukrainian or pro-Russian attacks. These types of attacks have been encouraged by both states (which have published lists of targets). These attacks have caused real but limited damage. They have created disorder, but not given any significant advantage to either side. Civilians have also been called on to perform defensive actions, such as reporting overflying drones.
- American companies Microsoft and Amazon have been playing an important defensive role by migrating and hosting data for Ukrainian government agencies in the cloud. This move of data abroad raises questions, because it is widely considered that the control and hosting of data is a key issue of sovereignty.
- The “hunt forward” approach performed by the USA (pre-emptive defensive actions, see below) had not been previously documented and will undoubtedly be used by others.

3.4.2 Hunt forward

Headline article from Cert-IST monthly bulletin, May 2022

At the beginning of Russia's war against Ukraine, Russian state-sponsored cyberattacks seemed be rather less severe than might have been feared (see the Headline section of our February bulletin). […] If the effect of these operations has been rather limited (according to what has been disclosed), it is perhaps because of the 'Hunt Forward' operations that the US has announced it has carried out. These operations consist of anticipating possible cyber crises by sending experts to analyse the situation on the ground. We imagine that they look for traces of compromise (looking for dormant implants) or give recommendations to enhance security or facilitate recovery after an attack (backups, DRP, etc.). The United States has indicated that it has conducted 9 "Hunt Forward" operations in Ukraine and mentions in particular a 2-month operation that began at the end of 2021. This type of operation has existed for 4 years and 28 missions in 16 countries have been carried out.

Note: this is only a theory. But a likely good illustration of the principle of pre-emptively anticipating an attack in a hunt forward approach is the Pipedream malware (see § 3.5.1). It is rumoured that the United States proactively set out to steal the malware from the attacker, rather than waiting for it to become known in an actual attack (see § 3.5.2).

3.5 SCADA threat increases with Pipedream malware

3.5.1 At a glance

One of the key events of 2022 was the discovery of the Pipedream attack toolkit. Pipedream is a piece of malware specially designed for attacking industrial facilities. Its discovery is as important as the discovery of Stuxnet in 2010 because it shows that attacks are now designed to circumvent the current defences (zoning) of industrial networks.

Pipedream is probably a Russian tool. Russia is the most active perpetrator of attacks on industrial systems. It is likely of course that other countries are envisaging this type of attack. China, the United States and other advanced countries in the cyber domain are undoubtedly also developing these skills, but much more discreetly.

Another key event of the year was the **publication in June by Forescout of a study called OT:ICEFALL**. This study identified 56 vulnerabilities that affect devices from 10 vendors (among them Honeywell, Siemens and Yokogawa). Most of these vulnerabilities are caused by insecure-by-design practices and show the security weaknesses that are still found in industrial systems (Forescout likens securing industrial systems to climbing Everest and the name “Icefall” refers to one of the first stages of the Everest climb). The last part of the study shows how to use these vulnerabilities in attack scenarios (with attack on a gas pipeline, wind turbines and a manufacturing plant). In contrast to the highly sophisticated Pipedream toolkit, OT:ICEFALL shows that in some cases planning an industrial attack does not have to be complicated.

Note: Cert-IST issued the **INFO-2022.013** message to inform our community about the OT:ICEFALL study.

3.5.2 *The Pipedream / Incontroller toolkit*

Cert-IST monthly bulletin, April 2022:

In mid-April, the US CISA, as well as the companies Dragos and Mandiant, published the description of a new malware (or rather a toolkit of several malwares) designed to attack industrial systems (ICS). It has been named **PIPEDREAM** (by Dragos) and **INCONTROLLER** (by Mandiant). This malware is considered to be a new "big" ICS malware to be compared with Stuxnet (2010), Industroyer (2016) and TRITON (2017). It also follows the announcement a few days earlier of an attempted Industroyer2 attack in Ukraine. **These two events show that the threat of attacks on industrial systems is growing at an alarming rate.**

The origins of PIPEDREAM are mysterious. Dragos said that the malware was given to it by a trusted source and that it has not been used in any real attacks. Rumour says that PIPEDREAM was stolen by the US Secret Service from Russian research institutes (possibly the TsNIIKhM which was accused of developing TRITON). With the increasing sophistication of attacks against industrial systems, and the potentially catastrophic impact of this type of attack, one can indeed imagine that an offensive approach was chosen, which consists in stealing the malware from the attacker rather than waiting for found it during an attack.

Publicly disclosing this malware:

- forces the attacker to change his malware (and thus delay planned attacks),
- warns potential victims and advise them to protect themselves.

To help victims protect themselves, SANS has published a webcast detailing the offensive capabilities of this malware and proposing a global approach for ICS security: PIPEDREAM and Countering ICS Malware (free SANS account required).

3.6 Supply chain attacks also target outsourced activities

Attacking via the supply chain was one of the major developments we identified last year in our 2021 annual review. In 2022, this threat remained a major concern. As a reminder, we broke it down into three categories:

- *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 will have been previously compromised, without the vendor's knowledge.*

• Attacks on software continue

In 2022, the most widely observed attacks involved cases of compromised libraries (such as **NPM**, **PyPi** and **Ruby**). This comes under the last of the three categories above.

We also noted an attack targeting Travis.CI, which shows that an attack on development environments (in this case CI/CD) is still a growing threat (this was one of our major observations in 2021).

• Attacks on outsourced activities are emerging

The most interesting case is the attack by the Lapsus$ cybercriminal group on OKTA in January 2022 (made public in March). To steal OKTA login details, Lapsus$ attacked a company in charge of OKTA customer technical support. This company (Sitel) therefore had access to the tools needed to reset OKTA accesses. This is a particular case of supply chain attacks via a provider (the second category in our list above), but it could be a category in its own right: attacks on business processes that have been outsourced (business process outsourcing, or BPO).

Note: we published the INFO-2022.004 message about this attack.

3.7 Rise of hackers-for-hire and offensive products for states

- The Pegasus case continues

In the summer of 2021, it emerged that the Pegasus spyware tool sold by NSO Group has been misused. Pegasus can be covertly installed on the mobile phones of people deemed to be dangerous. Designed to fight terrorism, it has also been used by some states for surveillance of journalists and opponents. This "dirty market" for surveillance tools has been known since at least 2015, but 2021 showed that their misuse was more widespread than previously thought.

In 2022, awareness of the phenomenon continued to grow. In Europe, for example, there is evidence of the use of Pegasus in Spain (disclosed in April) and an equivalent spyware program (called Predator) in Greece. In March, the European Parliament set up the PEGA Committee to investigate this phenomenon of misuse. In the United States, the House of Representatives held a public hearing on the subject in late July 2022. Google, Microsoft and CitizenLab.ca gave evidence.

Pegasus is not the only software in this category. We also know about **Candiru** (from the Israeli company of the same name), **Predator** (from Macedonia-based company **Cytrox**) and **Hermit** (from Italian companies RCS Lab and Tykelab). It is likely that there are others.

- Hackers for hire

There is clearly a demand from states for offensive tools. Google reported in 2022 that it had identified more than 30 companies in the market for selling 0-day and offensive cybersecurity tools to states. Google more recently cited the Spanish company **Variston**, which offers an attack tool in this category called **Heliconia**.

There is also a trend of using hacking-for-hire companies to handle the approach and attack targets. In late 2021, Facebook published a report identifying seven companies that offer these services to varying degrees. Six of these companies are named in the report: Cobwebs, Cognyte, Black Cube, Bluehawk, BellTroX and Cytrox.

- A market that is gradually becoming available to companies

The tools and services developed for states are also gradually being made available to a wider market. Hacking for hire is being offered to companies with varying levels of sophistication. It can be ordinary spear-phishing attacks, as described in a Reuters article in June 2022 about a service offered by Indian companies and mainly targeting law firms. Attacks can also be more sophisticated, using 0-day vulnerabilities, as described in the Microsoft Knotweed report in July 2022 about **DSIRF**. This Austria-based company advertises that it offers "advanced" information gathering and analysis services for international companies.

Cyber-mercenary groups identified by Cert-IST as part of our attack and IOC monitoring service

- **Bahamut (CERT-IST/ATK-2017-068):** Mercenary organisation carrying out cyber espionage in the Middle East and South Asia.

- **Dark Basin (CERT-IST/ATK-2020.066):** Group of mercenary hackers who have targeted thousands of individuals around the world. Citizen Lab attributes Dark Basin's activities to employees of an Indian company called **BellTroX InfoTech Service**.

- **DeathStalker (CERT-IST/ATK-2020.090):** Group of mercenary hackers targeting the financial and legal companies.

- **CostaRicto (CERT-IST/ATK-2020.126):** Cyber espionage campaign conducted by a group of mercenary hackers offering APT-style attacks.

- **Void Balaur (CERT-IST/ATK-2021.131):** Group of Russian-speaking cyber mercenaries selling mailbox copies and other private data (also known as **Rockethack**).

- **KNOTWEED (CERT-IST/ATK-2022.082):** Hacking-as-a-service group from the Austrian company **DSIRF**.

3.8 Other phenomena observed

3.8.1 Attacks on MFA

With the growing use of MFA, hackers are forced to develop new attack techniques. In 2022, two new techniques were observed:

- MFA fatigue
- Pass the cookie

We describe these types of attacks in the box below. Of course, just because of these attacks we should not abandon MFA.

Cert-IST article published in our September 2022 monthly bulletin

Attacks targeting MFA

As the use of multi-factor authentication (MFA) becomes more widespread to strengthen access security, hackers are also making progress in this area and developing new ways of attacking some of these MFA systems. In the summer of 2022, two such attacks were reported in the media:

- **OKTA** users were targeted by a large-scale phishing campaign (via SMS messages asking them to log into their OKTA account). It affected sites like **Twilio**, Cloudflare, Klaviyo, MailChimp and Doordash. We posted an article on this attack.
- An **Uber** employee was targeted by an MFA fatigue attack. His phone was swamped by MFA notification messages and he ended up accepting one of them, which allowed the hacker to gain access to Uber's network.

We published an article in 2018 about the SIM swap attacks that were targeting MFA via SMS messages at that time. Here is a broad overview of known attack techniques against MFA systems.

The various MFA techniques:

Here are the four MFA techniques currently being used:

1. **MFA by SMS:** A secret passcode is sent by SMS to the user's phone when they attempt to log onto a website.
2. **MFA via an authenticator app:** A secret code is generated every 30 seconds by an app on the user's phone. These apps (such as Google Authenticator, Authy, Duo or Microsoft Authenticator) use a T-OTP algorithm to generate a one-time passcode.
3. **MFA by push notification:** A popup window appears on the user's phone when they log onto a site. They use this popup to confirm that they allow access.
4. **MFA via a FIDO2 key:** A cryptographic algorithm is used to perform authentication via the FIDO2 protocol. This type of algorithm is implemented by Ubikey hardware keys, for example.

Whatever the MFA technique used, to avoid asking for full authentication at every login attempt, an **authentication cookie** mechanism is often implemented. If the user already has a valid (non-expired) cookie, then the new login is accepted without any further authentication (thus, there is no MFA). This is the "remember me" function found on many websites.

Known attacks

Here are the known attacks:

- **SIM swap** (targets mechanism 1): The attacker impersonate the victim and calls the victim's phone operator to get a new SIM card. With this SIM, the attacker now receives the SMS sent by the MFA system. The attack is quite complex (the operator has to be convinced) and used for high-value targets, for example to steal the user's cryptocurrency wallet.
- **Phishing MFA** (targets mechanisms 1 and 2): The attacker lures the victim to a fake website that relays the data exchanged during the login attempt, including the MFA code, to the real website. This is a MITM (man in the middle) attack. It works for SMS and authenticator type MFAs. There are tools for implementing this type of attack (such as the EvilProxy paid service and the evilgophish open-source project).
- **Theft of authentication cookies** (targets mechanisms 1, 2, 3 and 4): If a piece of malware (like Infostealer) has infected a victim's computer, it can steal their authentication cookies. If they have not expired, it can sign in without authentication (and therefore without MFA). This type of attack has been gaining popularity since early 2022, probably due to illegal BotShop services like Genesis (discussed in our May 2022 article), which sell the data stolen by infostealers.
- **MFA fatigue** (targets mechanism 3): This is the most recently documented attack technique, which we describe at the beginning of this article for the attack against Uber. It is likely to become quickly obsolete as push notification popups are improved (e.g. by including a user-activated "Mute" function that blocks these popups for a set period of time, such as half an hour).

Conclusion

Despite being under attack, MFA mechanisms are still an important advance in authentication security and efforts to deploy them should continue. For hackers, they have become a common pitfall they have to deal with when attacking well-defended targets. It is therefore logical to see bypass attempts and attacks against MFAs.

For more information

- MFA fatigue (and possible solutions):
  https://www.bleepingcomputer.com/news/security/mfa-fatigue-hackers-new-favorite-tactic-in-high-profile-breaches/
  https://www.securityweek.com/high-profile-hacks-show-effectiveness-mfa-fatigue-attacks
- MFA techniques:
  https://jumpcloud.com/blog/push-notification-mfa

3.8.2 Attacks on satellites?

The Russian attack on the KA-SAT satellite (operated by ViaSat) is one of the most significant cyber events of the war against Ukraine. It was not an attack on the satellite itself, but on the service provided (internet connectivity via satellite). Nonetheless, this event is part of a broader trend where satellites have become the target of attacks in recent years:

- In 2018, France announced that it planned to defend its satellites against attacks by satellites operated by other countries. Since September 2019, France has a Space Command. In late 2019, the United States created the US Space Force (USSF), the sixth branch of the American military.
- Tests of missile launches against satellites have been carried out for many years. The most recent was by Russian in November 2021.

In this context, cyberattacks against satellites is an increasingly likely prospect. Note that since 2020, the US Air and Space Force has run an annual competition called Hack A Sat to explore this threat.

3.8.3 BruteRatel and the new offensive tools

Two years ago, we reported that Cobalt Strike (a commercially available tool for performing attack drills) had become the most widely used tool for actual attacks, typically in ransomware cases, but also sometimes in state-sponsored attacks (such as the SolarWinds attack).

In 2022, a similar tool began to make the news: **BruteRatel C4**.

This tool has already been used in real attacks (see for example the analysis published in July 2022 by Palo Alto Networks). Several analysts believe that this phenomenon will grow.

Other similar tools have been cited (but seem less popular at the moment):

- **Sliver**: open-source tool from Bishop Fox, available on GitHub and described by Microsoft in August 2022
- **Havoc**: open-source tool available on GitHub
- **Manjusaka** and **Ninja**: open-source tools available on GitHub and cited by Kaspersky
- **Nighthawk**: commercially available tool from MDSec

The C2 Matrix project has identified over 100 projects offering such offensive tools.

3.8.4 Windows: Bring Your Own Vulnerable Driver

The **BYOVD** (Bring Your Own Vulnerable Driver) attack technique was widely discussed in 2022. It allows an attacker who has already obtained system privileges on a Windows machine to execute code in the Windows kernel.

Access to the kernel ("kernel mode") is protected (only code signed with a Microsoft-approved signature is allowed to run in the kernel). To bypass this protection, the BYOVD technique works as follows:

- It installs an authentic driver (for example a driver developed by Dell or Avast) that is signed, but for which there is a known vulnerability.
- It then exploits this vulnerability to force this driver to execute malicious actions.

BYOVD attacks were seen several times in 2022, making it a fairly common technique by now.

To counter BYOVD, Microsoft has compiled a list of known vulnerable drivers and has a function that blocks the installation of these drivers. Unfortunately, this mechanism was not properly implemented for Windows 10 and Windows Server, which has further fuelled the conversation about BYOVD.

3.8.5 Fewer exploits published before attacks

For a given vulnerability, the threat typically evolves in stages:

1	Targeted or limited attacks (e.g. 0-days)
2	Private exploit announced (e.g. video)
3	Public PoC (proof of concept)
4	Technical reports
5	**Public exploit**
6	Isolated attacks
7	Use of the vulnerability by a malware
8	Massive attacks

Not every step necessary happens every time. But step 5 (exploit published on the internet) is used by many as an indicator of the need to patch the vulnerability quickly. This is because attacks will now multiply and affect more victims than the initial 0-day attacks.

This indicator is changing and it is now not uncommon to see more and more attacks without a publicly available exploit. Take this case for example:

- For the **ProxyNotShell** vulnerability in Microsoft Exchange (**CERT-IST/AL-2022.011** alert dated 30-Sep-2022), the exploit was released only two months later (on 30-Nov-2022).
- The CVE-2022-24086 vulnerability in **Adobe Commerce (formerly Magento Commerce)**. This vulnerability was patched by Oracle in February 2022 (without having been exploited as a 0-day). To our knowledge, there is still no public exploit. However, there has been a progressive increase in attacks since September 2022, which prompted us to publish the **CERT-IST/AL-2022.013** alert

on 16-Nov-2022. It is likely that a private exploit program (i.e. not made public) has been circulating in the cybercriminal world.

It is important to be aware of this development, because if this observation is confirmed, the procedures for triggering alerts and prioritising security patches will need to be updated.

4 Cert-IST activity in 2022

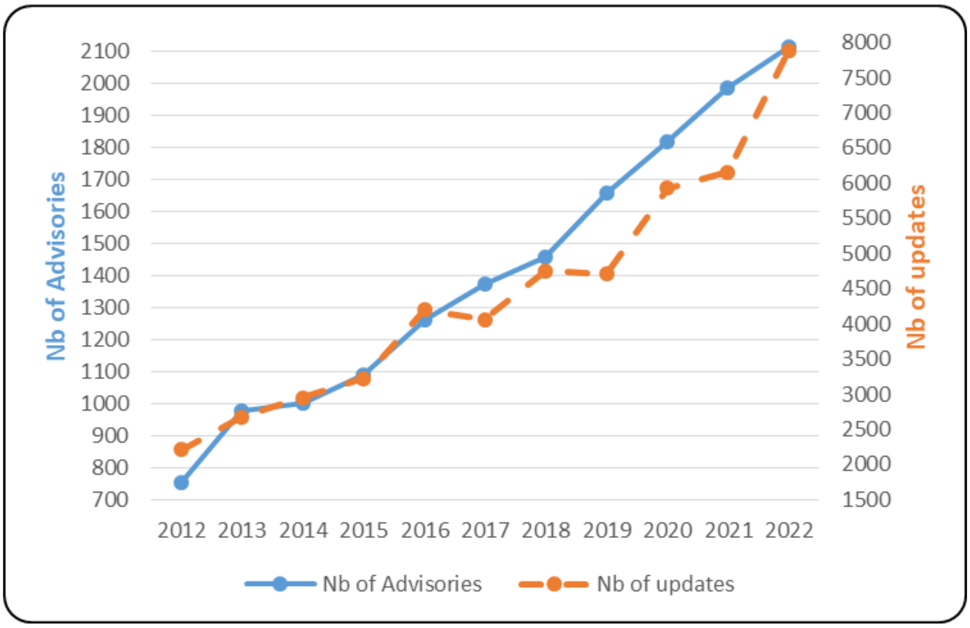
4.1 Vulnerability and threat feeds

As part of our monitoring of 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.

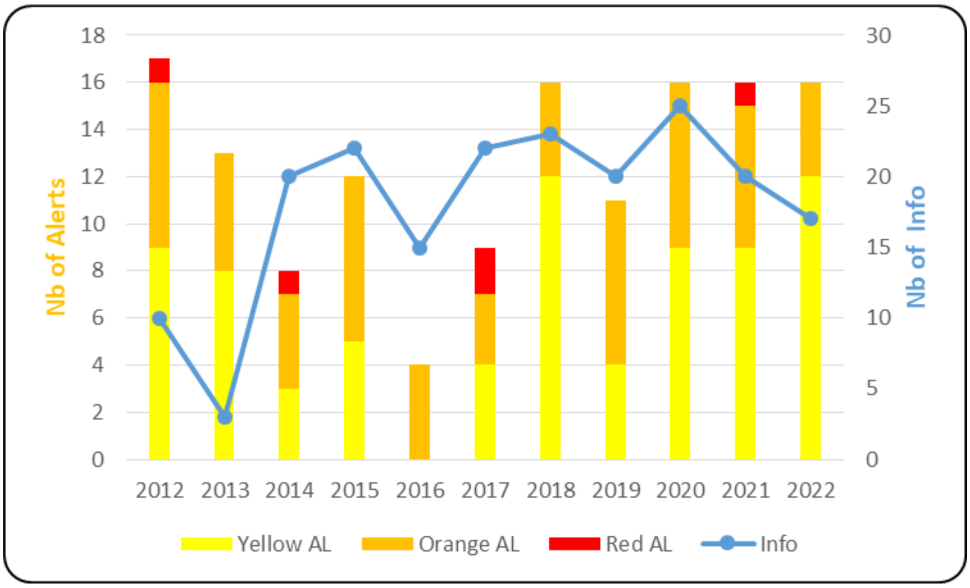
Cert-IST produces various types of publications:

- **Security Advisories (AV)**, which describe any newly discovered vulnerabilities in the 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 attacks, 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).
- **The Attack Reports (ATK)** and **indicators of compromise (IOC).** ATKs describe major attacks and hacker groups. The corresponding IOCs are made available in a MISP database. Both covers all kind of threats, including recurrent threats (malspam, exploit kits, ransomware), cyberespionage incidents (APT attacks) and the most significant ransomware.

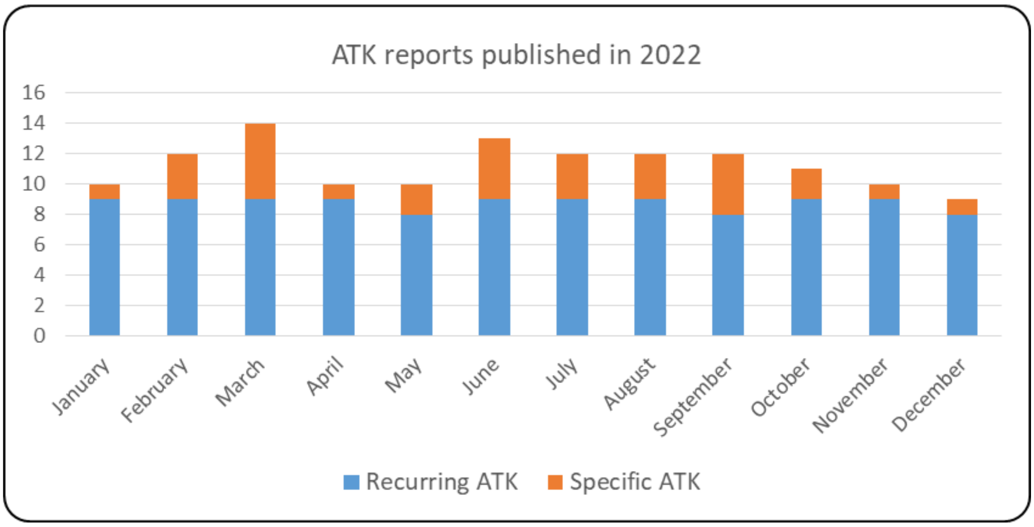
The graphs below show the number of Cert-IST alerts, reports, etc. over the last few years.



Number of security advisories (and updates) published per year



Number of security alerts published per year



Number of ATK reports published per month

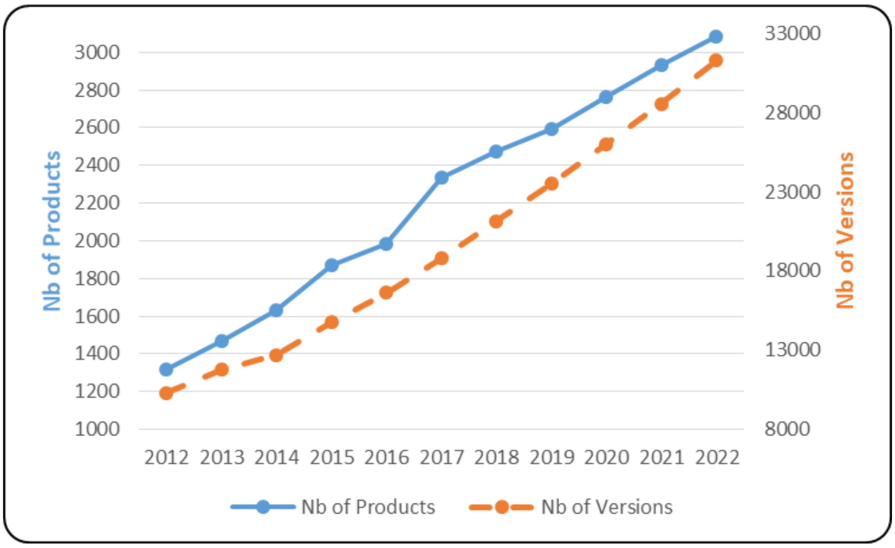
In 2022, Cert-IST published:

- **2,115** security advisories (including **120** SCADA advisories), **7,875** minor updates and **170** major updates.
  The number of advisories has been constantly growing in recent years (see graph), with a **6%** rise in 2022 compared to 2021. 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 **17** info messages. There were no red alerts last year. The previous red alerts were issued in 2021 (Exchange) and 2017 (WannaCry and NotPetya). From year to year, activity in this

category has fluctuated widely, but since 2018 the number of alerts per year has stabilised (with the exception of 2019).

- **135** attack reports (ATK) were published in 2022. **3,765** enriched events were added to the Cert-IST MISP database with **855,717** indicators (IOCs) added this year. In total, there are **6.2 million** IOCs in the Cert-IST MISP database.

Regarding the catalogue of products monitored by Cert-IST, as of 31 December 2022, Cert-IST was tracking **3,080** products and **31,281** versions. The graph below shows the evolution of the number of products and versions monitored by Cert-IST.



Number of products and product versions in Cert-IST's catalogue

4.2 Technology monitoring

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

Attacks targeting identities are becoming increasingly common.

Since 2020 (and the SolarWinds attack), it is known that advanced attackers look for weaknesses in authentication systems, with SAML, OAuth or PKI attacks.

We saw in 2022 that cybercriminals are targeting user accounts, stealing them using infostealer malware (such as Racoon or RedLine, see § 3.2) and bypassing MFA authentication using new techniques (see § 3.8.1).

These two phenomena show that some attackers prefer to impersonate real users, rather than exploiting vulnerabilities to gain entry without a valid account. This is what we see in post-attack analysis. Of course, the search for vulnerabilities continues (see below) but the **theft of passwords (or other authentication data such as cookies, etc.) is one of the most significant phenomena of the year**.

With the rise of Zero Trust Architecture (ZTA) solutions, identity attack is a critical risk: if a hacker can trick the ZTA with a false identity, the protection collapses.

Attacks on equipment exposed on the internet continue to increase.

In the 2010s, attacks were mostly aimed at the user’s workstation by exploiting vulnerabilities in the software installed on it (Flash, Java, PDF, etc.).

By 2015, attacks were aimed at the user, tricking them to open a compromised document (with the return of macro attacks) or reveal passwords (phishing attacks).

Since 2019, attackers have also increasingly been exploiting vulnerabilities discovered in exposed devices on the internet (VPNs or exposed appliance attacks). This phenomenon continued in 2022. Further, the number of intrusions via stolen passwords (the first phenomenon identified above) combined with intrusions via vulnerabilities on exposed equipment is likely greater than the total number of intrusions performed by direct infection of a workstation via compromised emails or websites.

Works on major topics are on-going.

Developments in 2022 show that companies should continue their works on do the following topics:

- Prepare for a potential ransomware attack or blackmail for stolen data. This can be achieved through crisis exercises, for example, and/or analysis of resilience in the event of a cyberattack.
- Be aware of potential attacks via the supply chain, and work on two topics: with suppliers to enhance supplier’s defences, and with developers to evaluate the security of software development environments (see our discussion of this in our 2021 annual report).
- Continue to secure industrial systems (SCADA, OT, etc).

Threat and attack monitoring remains an important part of cybersecurity

There were many developments in 2022, the most important of which is undoubtedly the Russia/Ukraine war. From a cyber perspective, what we have seen there, especially for defensive measures and resilience will likely have a tangible influence on the future of cyber-defence.

More broadly, the increase in the number of attacks and vulnerabilities, combined with the rapid pace of technological change, makes it crucially important to constantly monitor threats.

Here, Cert-IST is the partner of choice for companies today.

Cert-IST

290 Allée du lac
31670 Labège
France

info@cert-ist.com

https://www.Cert-IST.com

+33 5 34 39 44 88