CERT-IST

INDUSTRIE | SERVICES | TERTIAIRE

CERT-IST annual report on attacks and vulnerabilities in 2023

Released: February 2024

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 an analysis of key security events throughout the year (see § 2). We also offer a brief review of CERT-IST's activity during the year (see § 3).

In the conclusion (see § 4), we give a summary of the current cyberthreat landscape and the challenges companies will face in 2024.

➢ **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 Analysis of the most significant phenomena in 2023

This report begins by discussing the most significant phenomena of the year for companies:

- The four most significant attacks of the year: **Barracuda ESG** (CVE-2023-2868), **MOVEit Transfer** (CVE-2023-34362), **3CX** (CVE-2023-29059) and **Citrix NetScaler** (July and October)
- The increase in zero-day attacks
- Attacks on edge devices
- New criminal cyberattacks (in addition to ransomware and BEC attacks): MOVEit-style attacks, advanced social engineering and credentials hunting (ATO)
- And other observations, including: Pro-Russian DDOS attacks, use of RMM tools, attacks on VMware ESXi and phishing attacks conducted through OneNote and Teams.

We then move on to a review of other key topics:

- Cryptocurrencies, a favoured target for many attackers
- Cyber-warfare and the growing importance of cyber weaponry for states
- China's continued dominance in the cyber-offensive space
- Pegasus and Predator: the abuse of surveillance tools continues.

2.1 Significant events for companies

2.1.1 *The most notable attacks of 2023*

Attacks reviewed below are listed in order of importance, starting with the most noteworthy. At the end of this chapter, we summarise in a table all alerts issued by CERT-IST throughout 2023.

May 2023: Attack on **Barracuda ESG** equipment (CVE 2023 2868)

At a glance: In May 2023, Barracuda discovered that a zero-day vulnerability had enabled a China-based attacker (the group UNC4841, according to Mandiant) to compromise the Barracuda Email Secure Gateways (ESG) appliances of 5% of their customers. The attack started in October 2022. When Barracuda analysed the attack in May 2023, they realised that the perpetrators had profoundly altered the compromised systems and Barracuda then recommended to replace affected ESG rather than repair them.

Key takeaways: Besides this unprecedented recommendation (which had never been made before to the best of our knowledge), this attack is notable because it had many characteristics that were typical of attacks observed throughout the rest of the year (which we will further discuss later):

- It was a **zero-day** attack (see § 2.1.2) ...
- ...which targeted edge devices (see §2.1.3) and **profoundly compromised them** (concealing backdoors, countering disinfection attempts and wiping logs) ...
- ...and was committed by a Chinese state actor (see § 2.2.3).

May 2023: **MOVEit Transfer** attack (CVE 2023 34362)

At a glance: Cybercriminals affiliated with the group Cl0p exploited a zero-day vulnerability in MOVEit Transfer (a tool used to share files with third parties) to steal as many documents as possible from companies that use that tool. They then blackmailed the targets, threatening to release the documents.

Key takeaways: This attack affected a striking number of victims, with 2,600 companies reportedly being impacted. Some were direct victims who used the MOVEit Transfer product, and others were indirect victims whose data were stolen from direct victims.

The exploitation of zero-day vulnerabilities by cybercriminals is a new trend, as they had previously favoured already known vulnerabilities (known as one-days or *n*-days) to organise massive attack campaigns. These criminal zero-day attacks were observed as early as January 2021, when one such attack targeted Accellion FTA. However, they became more widespread in 2023 with attacks on Aspera Faspex (January), GoAnywhere MFT (February) and PaperCut (April).

April 2023: “Double supply chain attack” on 3CX softphones (CVE-2023-29059)

At a glance: In April 2023, EDR alerts indicated that 3CX, a desktop telephony application, had been compromised at 3CX side (in a software supply chain attack). The investigation showed that the attack had initially targeted MacOS (before Windows) and that 3CX had been compromised several months earlier when an employee downloaded a financial application (X_TRADER) which had itself been compromised by another supply chain attack, probably in February 2022. Both attacks have been attributed to a group affiliated with the North Korean government.

Key takeaways: This attack is most notable for being a double supply chain attack. Besides this, it exhibits well-known motivations and methods: North Korea often targets cryptocurrencies, so it is not surprising that it would have compromised a piece of financial software. And like many advanced attackers, North Korea demonstrated here that it is able to gain information and spread from one target to the next over the course of several years.

July and October 2023: Attacks on **Citrix NetScaler**

At a glance: Citrix NetScaler was targeted by two massive attacks in 2023, compromising a large number of systems. These were conventional attacks (nothing new in the techniques used) where the majority of breaches occurred despite patches being available.

Key takeaways: The July attack was not a zero-day, but was launched just two days after patches were announced. This short elapsed time can most likely be attributed to the fact that massive attacks targeting the same type of systems had already occurred in January 2020, meaning that the attackers knew their targets well and were able to deploy attacks at lightning speed. On many systems, patches were deployed too late: a backdoor had already been created and was not detected when the patches were applied.

On the other hand, the October attack *was* a zero-day, the first breaches having occurred in August, but the majority occurred a full two weeks after patches had been released. The timeline of these events was ordinary:

- the vulnerability was disclosed and patches released
- ...then technical details and an exploit appeared a few days later...
- ...and finally, numerous different actors rushed to carry out attacks.

The vulnerability in question makes it possible to remotely steal memory fragments containing unencrypted session tokens, allowing attackers to access the vulnerable device. It was nicknamed **CitrixBleed** in reference to the famous HeartBleed vulnerability in OpenSSL that came to light in 2014, also a memory leak issue that revealed critical data (cryptographic keys).

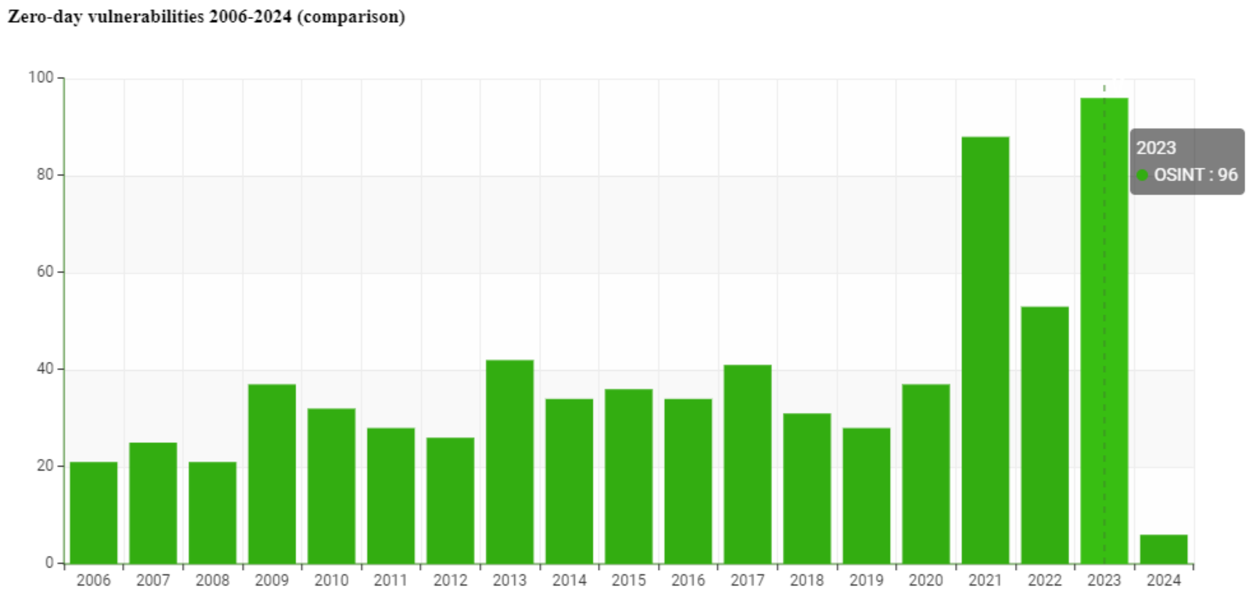
Other attacks in 2023

The table below details the 20 alerts issued by CERT-IST in 2023. In addition to the attacks discussed above, the year’s most notable attacks included ones targeting **Fortinet**, **Outlook**, **Ivanti EPMM**, **Atlassian Confluence** and **Cisco IOS XE**.

Alert	Reference	Description	Date
Yellow	CERT-IST/AL-2023.001	Ongoing attacks using **SugarCRM** vulnerability (CVE-2023-22952)	12 Jan. 23
Yellow	CERT-IST/AL-2023.002	Ongoing attacks against **Cacti** (CVE-2022-46169)	17 Jan. 23
Orange	CERT-IST/AL-2023.003	Ongoing attacks against **ManageEngine** products (CVE-2022-47966)	20 Jan. 23
Orange	CERT-IST/AL-2023.004	Ongoing attacks targeting **VMware ESXi** (ESXiArgs ransomware)	6 Feb. 23
Yellow	CERT-IST/AL-2023.005	Attack expected for **Fortinet FortiNAC** (CVE-2022-39952)	22 Feb. 23
Yellow	CERT-IST/AL-2023.006	Attacks detected for **Barracuda** Email Security Gateway (CVE-2023-2868)	31 May 23
Yellow	CERT-IST/AL-2023.007	Ongoing attacks against devices running **FortiOS** (CVE-2023-27997)	13 Jun. 23
Yellow	CERT-IST/AL-2023.008	Ongoing attacks with vulnerability targeting **Microsoft Office/Outlook** (CVE-2023-36884)	13 Jul. 23
Orange	CERT-IST/AL-2023.009	Ongoing attacks against **Netscaler** Application Delivery Controller (ADC) and Netscaler Gateway (CVE-2023-3519)	19 Jul. 23
Yellow	CERT-IST/AL-2023.010	Ongoing attacks against **Ivanti Endpoint Manager Mobile** (EPMM) (CVE-2023-35078, CVE-2023-35081)	25 Jul. 23
Orange	CERT-IST/AL-2023.011	Ongoing attacks against **Ivanti Sentry** (CVE-2023-38035)	25 Aug. 23
Orange	CERT-IST/AL-2023.012	Ongoing attacks against **Juniper Junos** (CVE-2023-36844 to CVE-2023-36847)	28 Aug. 23
Yellow	CERT-IST/AL-2023.013	Ongoing attacks against **Apple iOS** (CVE-2023-41061, CVE-2023-41064)	8 Sep. 23
Yellow	CERT-IST/AL-2023.014	Attacks expected for **Microsoft SharePoint** (CVE-2023-29357 and CVE-2023-24955)	29 Sep. 23
Yellow	CERT-IST/AL-2023.015	Ongoing attacks against **Confluence** servers (CVE-2023-22515)	12 Oct. 23
Orange	CERT-IST/AL-2023.016	Ongoing attacks against **Cisco IOS XE** (CVE-2023-20198 and CVE-2023-20273)	17 Oct. 23
Orange	CERT-IST/AL-2023.017	Ongoing attacks against **Netscaler** Application Delivery Controller (ADC) and Netscaler Gateway (CVE-2023-4966)	24 Oct. 23
Yellow	CERT-IST/AL-2023.018	Ongoing attacks against **F5 BIG-IP** (CVE-2023-46747 and CVE-2023-46748)	6 Nov. 23
Yellow	CERT-IST/AL-2023.019	Ongoing attacks against **Apache ActiveMQ** (CVE-2023-46604)	7 Nov. 23
Yellow	CERT-IST/AL-2023.020	Attacks expected against **Apache Struts 2** (CVE-2023-50164)	14 Dec. 23

2.1.2 *Increase in zero-day attacks*

According to zero-day.cz, 2023 saw the discovery of 96 zero-day vulnerabilities, breaking the record set in 2021 (with 88 zero-day vulnerabilities discovered).



Number of zero-day vulnerabilities identified by www.zero-day.cz (maintained by Cybersecurity-Help)

On a longer timescale, the curve of this graph shows a clear development in 2021: while the annual frequency of zero-day attacks had until that point hovered around 40, it spiked to over 80.

We believe that this rise is due to three factors:

- An increase in **Pegasus-type zero-days** targeting iPhones and Android smartphones: around 20 iOS/iPhone zero-days were discovered in 2023.
- **Chinese state-sponsored attacks**: according to Recorded Future, since 2021, China has exploited about ten zero-day vulnerabilities each year in massive attack campaigns.
- The exploitation of **zero-days by cybercriminals.**

The last two categories consist of cases where the vulnerability was used to target a large number of victims in an attack campaign, while in the past, zero-days were reserved for attacks with a smaller number of high-value targets. This means that for ordinary organisations (non-"high-value" targets), the risk of falling prey to a zero-day attack is increasing.

Is this increase a cause for concern?

Yes and no, as zero-day attacks have always posed a risk. However, in addition to the pressure that this trend places on operational teams (as zero-days often require patches to be rapidly deployed), the increase in zero-day attacks demonstrates that the most important thing is not just to prevent them, but to know how to regain control over the situation when they do happen. This requires two skills:

- Detection: realising that you have been infected, which is not easy when attackers know how to cover their tracks
- Recovery: knowing how to clean impacted systems or, if this is not possible, how to replace them.

2.1.3 Attacks on edge devices

Since 2019, attacks targeting edge devices (typically VPN gateways and internet-exposed appliances) have been on the rise. This trend continued in 2023, with eight of our 20 alerts pertaining to this type of product: **Fortinet** (twice), **Barracuda**, **Citrix Netscaler** (twice), **Juniper**, **Cisco IOS XE** and **F5 BIG-IP**.

We already noted this trend in our 2020 report and described some of these systems as “hard on the outside, and weak inside”. In addition to this, three new and significant factors associated with these attacks became apparent in 2023:

- Deep compromises
- The difficulty of monitoring devices
- The difficulty of disinfecting them.

Deep compromises and the difficulty of monitoring devices

Article published on the front page of the monthly CERT-IST monthly bulletin for March 2023

Several recent examples have shown that some attackers are able, after exploiting a vulnerability, to deeply modify the equipment they have compromised, in order to stay on that equipment for a long time and not be detected. Mandiant describes this on a SonicWall SMA firewall and Fortinet on a FortiGate firewall. They observed the following:

- techniques for surviving a version upgrade,
- replacing system libraries,
- installing network filters that trigger a backdoor when a particular ICMP packet is received,
- erasing logs,
- etc.

Both are appliances based on systems such as Linux or FreeBSD, which offers great flexibility. And the attackers are obviously very familiar with the operation of these platforms. Mandiant also points out that these appliances are difficult to monitor (no EDR, no detection of operating anomalies, no antivirus) and that the underlying OS is hidden, which can make it difficult to detect an abnormal process or even to collect logs.

These findings are worrying. Perhaps the appliances need to be improved. But it is also essential to activate the monitoring features that exist (Fortinet says that it was the integrity check of the FIPS mode that allowed the compromise to be discovered), and to monitor the anomalies that are detected. Of course, the security patches must also be scrupulously applied and a complete reinstall of the device is required if an attack has succeeded.

Difficulty of disinfecting them

With experienced attackers, it can be difficult to identify all the changes made, and thus restore the system to a healthy state. It has become common for attackers to implement mechanisms to withstand version updates. More rarely, there have been cases where an attacker modifies low-level software (e.g. UEFI attacks or infections of network adapter firmware). There are many other possibilities, including attacks on motherboard BMCs, but no accounts of real-world attacks of this type. Since 2021, CISA in the United States has grouped these attacks under the umbrella of VBOS (vulnerability below the OS) and raised awareness about protective measures.

VBOS attacks are exceptional cases, only perpetrated by advanced state actors. On the other hand, the example of Barracuda ESG in 2023 (see § 2.1.1) demonstrates that situations where “it’s better to replace than to repair” could become commonplace.

Note: There is no element to believe that the Barracuda incident included a VBOS attack.

Replace rather than repair?

Barracuda’s recommendation raised eyebrows, but this is undoubtedly the only approach that guarantees a clean slate. Indeed, financial considerations aside, we might ask ourselves why we don’t use this solution more often.

Replacing edge equipment is a delicate task.

- Its availability is often critical; and
- Its configuration (in terms of settings) must be perfectly documented so that it can be reproduced on replacement equipment without having to copy over the contents of the infected equipment and risk reinfection.

However, with proper preparation (including having an clean copy of the equipment’s configuration to hand), it can be accomplished without any major difficulty.

Just as “make backups” is a common advice when making recommendations to protect against ransomware attacks, we believe that “develop device replacement procedures” is an equally important advice to protect against edge device attacks.

2.1.4 Attacks by cybercriminals

2.1.4.1 Ransomware and BEC remain the leading threats

As we describe new trends in the following sections, it is important to remember that, for companies, most cyberattacks still take the form of:

- Ransomware: originally limited to attacks rendering enterprise computers inoperable *en masse*, this term now also includes blackmailing victims with threats to disclose stolen data.
- Business email compromise (BEC) attacks: this term is often used in a broad sense to refer to all attempts at financial fraud made via email, such as posing as a third-party company to place a fraudulent order or tricking users into making bank transfers.

2.1.4.2 MOVEit-like attack campaigns

The MOVEit Transfer attack (see § 2.1.1) demonstrated that cybercriminals are relentless in searching for new ways to attack companies, and therefore to steal documents and sow disruption in the company.

In 2023, their tools of choice included:

- Managed file transfer (MFT) software, including MOVEit. Other attacks we have already mentioned (in § 2.1.1) targeted **Accellion FTA**, **Aspera Faspex** and **GoAnywhere MFT**. And we can add to this list attacks on Hitachi Vantara's **HCP Anywhere** (with the French AP-HP incident in September 2021), SolarWinds's **Serv-U** (in October 2021), **Citrix ShareFile** (August 2023).
- The enterprise printing solution **PaperCut** (attacked in April 2023). Currently, this is the only software of this type to have been attacked.

What will future attacks look like?

It is hard to say. However, we have observed a new tactic which is likely to become more common: **targeting customer-facing support resources**.

In October 2023, Okta suffered an intrusion into its customer support services by an actor who stole .HAR files that customers had sent to the company's technical support team. These debug files contain session tokens that the attacker was able to use to access affected customer's accounts.

This incident indicates that customer support channels represent an attractive target for attackers, as they contain customer data which can be used for blackmail. To limit the impact of this type of attack, it is important to limit the retention period for the data stored in these systems.

2.1.4.3 Advanced social engineering attacks

Article published on the front page of the monthly CERT-IST monthly bulletin for November 2023

In November, CISA issued an alert about the **Scatter Spider** group. This group is believed to be the one that attacked two Las Vegas casinos and hotels in early September: the MGM Resorts and then the Ceasar Palace. It is one of the few groups known to practice highly advanced social engineering attacks.

It can, for instance:

- Search LinkedIn for a system's engineer working for a targeted company,
- Then gather personal information (date of birth, etc.) about him on the Internet,
- Steal his account and passwords with phishing attacks, either by e-mail or SMS,
- Call the company's technical support (Help Desk) pretending to be him, and reset his Okta tokens.

In addition to its in-depth technical knowledge of authentication methods, the group is known for its ability to manipulate its victims. This starts with audacity (it can, for example, start a WhatsApp conversation with its victim to convince him to perform an action), but it can also go up to threaten physical retaliation, as demonstrated in this Microsoft report. Similar behaviours were also seen in early 2022 with the **Lapsus$** group with attacks such as the "MFA fatigue" one against Uber, or also the Twilio/Okta attack.

These advanced social engineering attacks are becoming more and more frequent, critical and successful. Over the summer, Okta published 2 articles on this matter (on July and on August), indicating that these attackers have repeatedly succeeded in convincing Help Desk teams of victim companies to give them access to Okta administrator accounts.

Note: Scatter Spider is known by multiple names (see our **CERT-IST/ATK-2023.010** attack sheet): **Octo Tempest** for Microsoft, **0ktapus** for Group-IB, **Scatter Swine** for Okta, **Muddled Libra** for Palo Alto Networks, **UNC3944** for Mandiant. It's not entirely certain that all these names refer to the same group. In fact, some CTI analysts say they have trouble defining the shape of some groups, which they describe as **fluid** (see this presentation from the SLEUTHCON 2023 conference).

2.1.4.4 Hunting for credentials (password, Okta, etc.)

Hackers have long attempted to steal authentication data (like passwords, session tokens and so on) in order to take control of users' accounts. Attacks like these are usually called account takeovers (**ATO**).

Some ways of performing them have long been common knowledge:

- Guessing passwords (with "brute force" and "password spraying" attacks among others)
- Asking the user (phishing).

More recently, other methods have appeared:

- Stealing a user's password (with **infostealers**)
- Circumventing MFA (**SIM swap**, **MFA fatigue**, **pass-the-cookie**).

In 2023, two new trends emerged:

- Theft from authentication solutions providers like **Okta** (in October) and from the **1Password** password manager. In 2022, **LastPass**, another password manager, had suffered a major attack. Vulnerabilities in **KeePass** were also much discussed in 2023. None of these is anything new, but 2023 showed us how common and varied this type of attack is becoming. For some cybercriminals, stealing passwords is their main line of business, and they attempt to access those passwords wherever they are stored.
- Calls to company helpdesks with the goal of taking over an account. This includes the advanced social engineering attacks discussed above.

2.1.5 What about state-sponsored attacks?

State-sponsored attacks comprise a significant proportion of the current threat landscape. In fact, states are the most dangerous and advanced attackers. They are able to use attack techniques that are unknown or unavailable to other attackers, and their methods are sometimes mimicked by cybercriminals.

2023 saw a significant number of state-sponsored attacks, including some carried out by China, Russia, Iran and even the US (suspected to be behind the so-called “Operation Triangulation” iPhone attack in Russia).

However, we did not observe events in 2023 which are a cause for concern for companies, and that were not already covered in other parts of this report.

Note: Some points in section 2.2 expand on this analysis of state-sponsored attacks.

2.1.6 Other notable trends

Below are a few notable techniques observed in 2023.

2.1.6.1 DDoS attacks such as NoName057 and Anonymous Sudan

First observed in March 2022, in the early stages of the Russia-Ukraine war, DDoS attacks by the pro-Russian hacktivist group **NoName057** (and other such groups including **Killnet**) continued in 2023. The group **Anonymous Sudan** (not initially directly linked to the Russia-Ukraine war but close to pro-Russian groups) attracted particular attention, having orchestrated several attacks targeting France in late February and even knocking out some of Microsoft’s Azure and Outlook cloud services in June.

To the best of our knowledge, these DDoS attacks have not had serious consequences. However, they have rendered target sites unavailable for several hours and added pressure and workload to operational teams deployed to respond to them.

2.1.6.2 Use of RMM tools

In 2023, CISA published several advisories (such as this one in January and this one in June) warning that some legitimate remote monitoring and management (RMM) tools are often used by attackers to remotely control compromised workstations. For example, remote access software such as **AnyDesk** or **ScreenConnect** (now called **ConnectWise Control**) is often used in fraud operations targeting the general public (e.g. Microsoft technical support scam) or even companies. **TeamViewer** is also frequently used.

CISA therefore recommends that companies monitor whether this type of tool appears on their internal network and launched an initiative in conjunction with manufacturers and MSSPs to prevent criminal use of RMM tools.

2.1.6.3 Attacks on VMware ESXi

VMware's virtualisation solutions are widely used by companies and are therefore attractive targets for attackers.

- VMware is often targeted by ransomware, as encrypting an ESXi hypervisor makes it possible to encrypt all of the VMs that it hosts all at once. The year started with Recorded Future announcing that the frequency of this type of attack had increased threefold in 2022. VMware itself has a page on its website dedicated to describing protective measures against ransomware.
- Attackers (whether state-sponsored or cybercriminal) have a keen awareness of the well-worn attack paths used to target vSphere: attack vCenter, then take control of the ESXi servers and finally the VMs. For examples, see this presentation from Typhooncon 2023 or this Chinese attack using CVE-2023-20867.
- In February 2023, a vulnerability in the SLP service resulted in thousands of ESXi servers being infected with a specific ransomware dubbed **ESXiArgs**. Many were unsecured servers installed on "bare metal" infrastructure (bare servers requiring the installation of an OS) hosted by OVH.

2.1.6.4 Phishing via OneNote and Teams

On a smaller scale, two new phishing techniques emerged in 2023:

- OneNote phishing: early in the year, a wave of email attacks used ".one" attachments (the extension used for Microsoft OneNote notebooks) to infect victims.
- Teams phishing: in September, several attacks of this type were reported. Victims were sent a Teams chat message with a malicious attachment. The attack exploits a vulnerability disclosed in June, and a tool named TeamPhisher had been published to exploit it a month later.

2.2 Other, non-enterprise-focused developments

2.2.1 *Cryptocurrencies, a favoured target for many attackers*

As discussed in our 2021 annual report, cryptocurrency theft presents an attractive prize for cybercriminals as well as states such as North Korea and Iran. In 2023 we saw for instance (see § 2.1.1) that 3CX attack was linked to a North Korea-sponsored attack targeting the financial sector. Moreover, it has long been known that SIM swapping originated in 2016 with attacks on cryptocurrencies.

Much like the Banker Trojans (malware designed to steal money from victims' bank accounts) seen around 2015, today we see many attacks attempting to siphon money from cryptocurrency wallets. According to Intel 471, these **crypto drainers** were the best-selling type of malware on the black market in the first half of 2023.

This threat primarily concerns individuals and companies who own crypto or who work in the decentralised finance (DeFi) sector.

2.2.2 *Cyber-warfare and the growing importance of cyber weaponry for states*

The Russia-Ukraine war has demonstrated that cyberattacks are a true part of the war weaponry, especially useful for intelligence gathering, destabilisation and influence operations.

This reality makes it more important than ever for states to possess both Cyberdefence and Cyberoffense tools. Consequently, cyber-armament is rising:

- Following the "hunt-forward" operations described in our 2022 annual report, the watchword in 2023 was **Active Cyber Defence**.
- China's **Volt Typhoon** attack on the United States was read by many analysts as a pre-positioning operation to install backdoors in facilities in Guam (an Island in Pacific where US has important military installations), with the goal of being able to disrupt internet communications in the Pacific region should a conflict break out.
- Analyses exploring what a cyberwar looks like and how it would impact civilians are now being presented at conferences. For example, at Hack.lu 2023, sessions were organised entitled "Introduction to Cyberwarfare" and "Eight Rules for Civilian Hackers".

2.2.3 *China's dominance of cyberoffence continues*

Since 2021, China has been found responsible for many cyberattacks. In 2023, the most notable events were:

- The ESG Barracuda attack (see § 2.1.1)
- The Volt Typhoon attack
- The theft of cryptographic keys from Microsoft by the group **Storm-0558** (see this article from TheRecord.media, published in July 2023, and Microsoft's followup announcement in September).

In 2023, Mandiant and RecordedFuture also identified China as the perpetrator of the **Fortinet, VMware** (CVE-2022-41328 and CVE-2023-20867), **Citrix NetScaler** (CVE-2023-3519, July 2023) and **Atlassian Confluence** (CVE-2023-22515, October 2023) attacks.

2.2.4 Pegasus and Predator: the abuse of surveillance tools continues

In July 2021, a group of journalists revealed that the cybersurveillance tool Pegasus had been widely abused. Despite the actions taken at the time (the prosecution of NSO, the European Parliament's PEGA commission, etc.), new abusive uses of the tool were uncovered in 2023:

- New zero-click attacks using Pegasus were discovered, targeting iOS: **PWNYOURHOME** in April and **BLASTPASS** in September
- In October, a journalistic investigation dubbed "Predator Files" was published concerning the **Predator** malware (a Pegasus equivalent), attributed to the **Intellexa** consortium.

3 CERT-IST activity in 2023

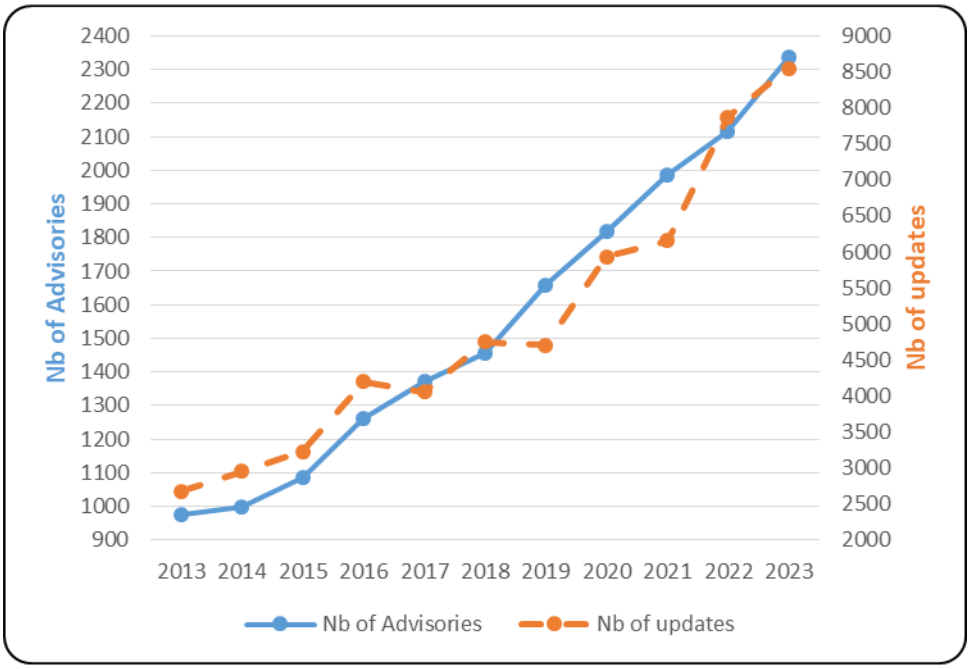
3.1 Vulnerability and threat feeds

As part of our monitoring of vulnerabilities and threats, CERT-IST continuously tracks various sources for information (vendor announcements, security blogs, mailing lists, communications within the cyber community, etc.) in order to stay informed. Every day, this data is analysed to provide our members with sorted, qualified and prioritised information.

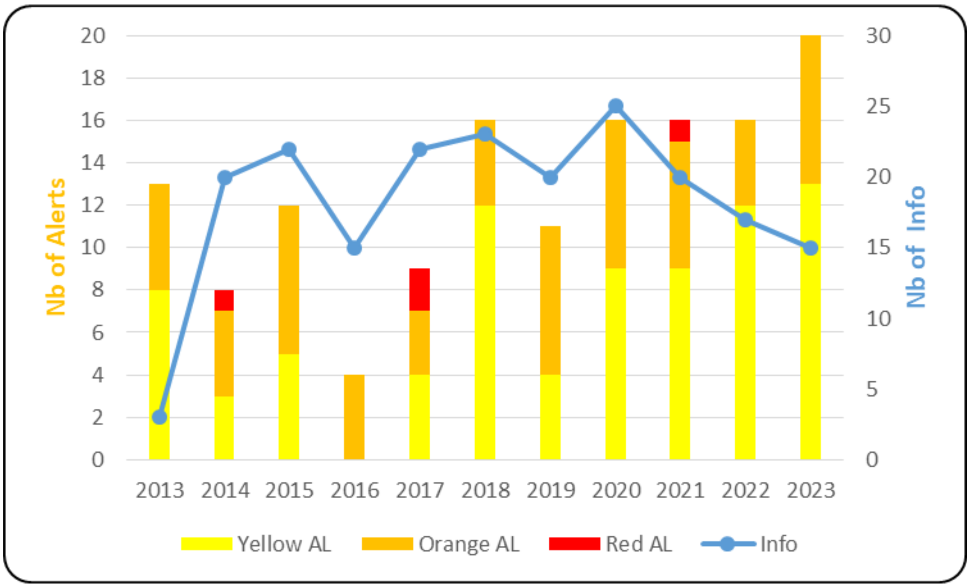
CERT-IST produces various types of publications:

- **Security Advisories (AVs)**, which describe any newly discovered vulnerabilities in the products we monitor. These AVs are continuously expanded with minor and major updates. The latter typically correspond to situations where exploits are publicly disclosed.
- **Alerts (ALs)**, 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).
- **Attack Reports (ATKs)** and **indicators of compromise (IOCs)**. 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, botnets, 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

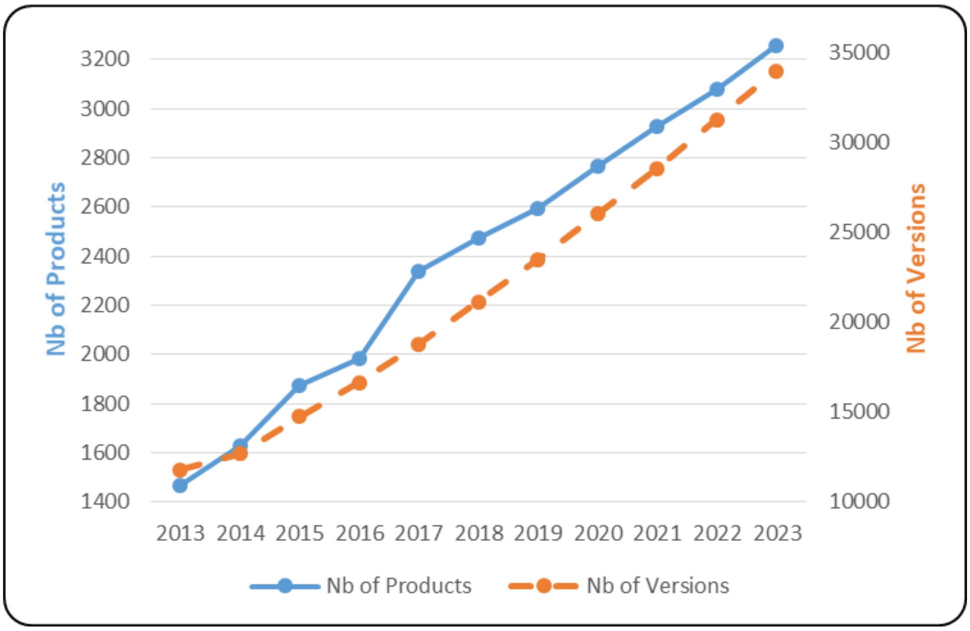
In 2023, CERT-IST published:

- **2,338** security advisories (including **136** SCADA advisories), **8,544** minor updates and **166** major updates.
  The number of advisories has been constantly growing for many years (see graph), with a **10%** rise in 2023 compared to 2022. This **steady increase** shows that discovering vulnerabilities is an ever-growing phenomenon. Maintaining an adequate level of security, therefore, still depends on the constant application of security patches for products in the information system.

- **20** alerts and **15** Info messages. There was no red alerts last year. The previous red alerts were issued in 2021 (Exchange) and 2017 (WannaCry and NotPetya). Over the last few years, the number of alerts has remained more or less stable, but rose in 2023, jumping from 16 to 20 alerts over the course of the year.

- **138** attack reports were published in 2023, with **7,181** enriched events added to the Cert-IST MISP database and **400,000** indicators (IOCs) added this year. In total, there are **7.5 million** IOCs in the CERT-IST MISP database.

Regarding the catalogue of products monitored by Cert-IST, Cert-IST was tracking **3,258** products and **34,004** versions as of 31 December 2023. The graph below shows the change in the number of products and versions monitored by CERT-IST.



Number of products and versions monitored by CERT-IST

3.2 Technology monitoring

In addition to vulnerability tracking, CERT-IST also produces technology monitoring 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.

4 Conclusions

Replace rather than repair?

Of all the developments observed in 2023, we believe that the most significant for companies is the fact that more attacks are deeply compromising edge devices. Attackers do not stop at controlling the device, they infiltrate it with the aim of remaining there for as long as possible. This was seen in particular with the Barracuda ESG attack as well as the attack targeting Ivanti Connect Secure in early 2024. In these cases, rather than simply cleaning and applying patches, it becomes necessary to completely rebuild the system. This practice (rebuild the system using a master image) has long been applied to individual computers, but going forward and apply it to infrastructure equipment, especially devices exposed on the internet will probably be required.

The leading cybercriminal threats remain ransomware and BEC scams

Nonetheless, 2023 has also seen:

- A rise in social engineering attacks (e.g., hackers posing as company employees and requesting helpdesk to reset MFA tokens)
- An endless hunt for credentials (with the continuation of 2022's Infostealer attacks and a rise in attacks on Okta and password managers).

Opportunities for improvement

Reducing the number of systems exposed to the Internet. Every new critical vulnerability brings new attacks on poorly secured, internet-exposed systems, begging the question: did these systems really need to be visible for all the world? This is not a new issue, but has apparently worsened with the widespread adoption of cloud infrastructure and its access-from-anywhere model. There is no silver bullet against this problem, but there are protective measures that can be taken:

- Consider an internet-exposed system as being critical. For example, it must be possible to apply updates extremely quickly in case of a critical failure and appropriate procedures must be in place to do so.
- Do not expose administrator functions directly. They should only be accessible from specific access points (e.g. bastion hosts, jump hosts, etc.)
- Implement an upstream access control mechanism (IAM), separate from the application itself. Access control is a critical function, meaning that it should ideally be managed by a dedicated solution, such as an application gateway or an authentication reverse-proxy.

Dealing with extreme complexity of cloud environments (such as Azure, AWS and GCP). These cloud solutions are technically complex and very dynamic, making them difficult to manage. There is likely no true solution besides noting that the security robustness of these solutions largely depends on the capability of the cloud service supplier. You expect that the supplier has a good design and will be able to deal with security issues diligently and effectively. This trust requires transparency and commitment of the supplier as well as a clear statement on the responsibilities of both client and supplier.

It should, however, be noted that the use of cloud solutions (as opposed to implementing internally the entire technical stack, from infrastructure to application) strengthens security, as the cloud provider takes in charge the security maintenance for its products. Again, clear statements on responsibilities and service commitments enables each party to concentrate on the part of the work for which it is responsible.

An ever-evolving sector

Like every year, 2023 has been eventful in terms of new vulnerabilities and attacks. Staying up to date and identifying trends remain critical to maintain control over cyberdefence. Here, CERT-IST is the partner of choice for companies today.

Association Cert-IST

290 Allée du lac
31 670 Labège
France

info@cert-ist.com

https://www.cert-ist.com

+33 (0) 5 34 39 44 88