almond

CWATCH

Edition 2024/2025

Threat Landscape Overview

Europe has seen an acceleration of attacks over the past 18 months

TLP:CLEAR

CONTENTS

PROJECT TEAM

Almond would like to thank all the experts who made this Threat Landscape possible.

Chloé
GRÉDOIRE

Cyber Threat Intelligence
Analyst

Manon
GUEGUEN

Cyber Threat Intelligence
Analyst

Mathias
GARCIAU

SOC / CERT / CTI CWATCH
Manager

Mélodie
CELIN

Communication & Marketing
Manager

This Threat Landscape 2024-2025 was written entirely by humans, and no IAs were mistreated in the process!

FOREWORD

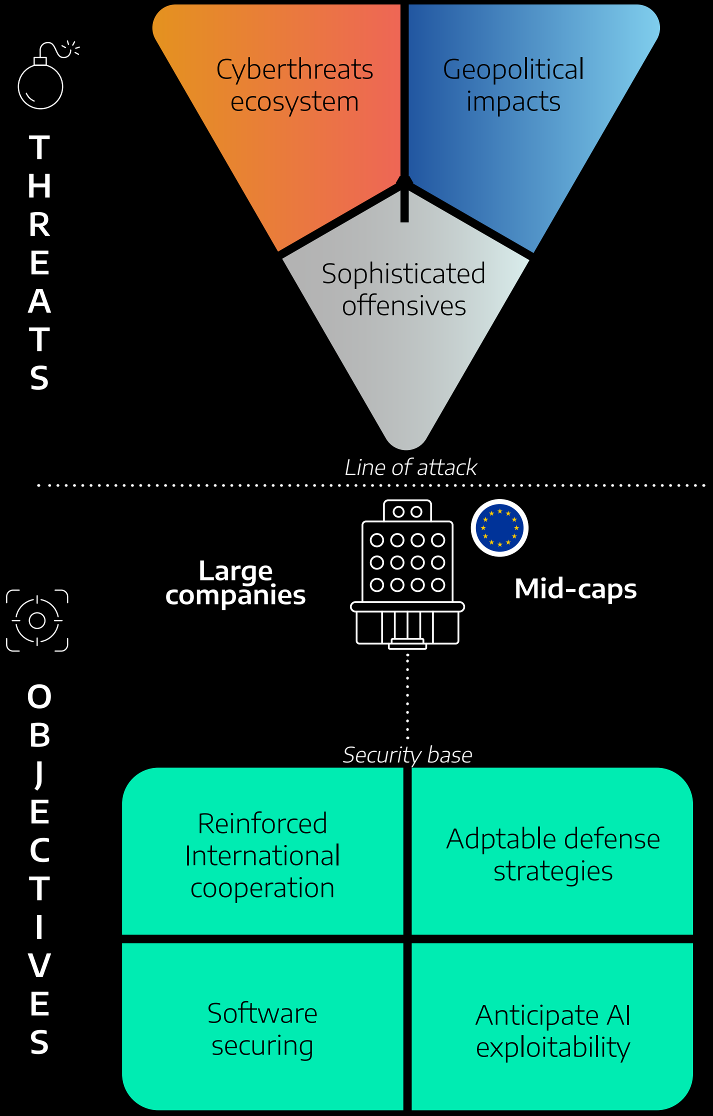
The New Face of Cyberthreat: challenges and imperatives

As the cyber threat landscape evolves, it does so at a dizzying pace, shaped by an unprecedented geopolitical context and cutting-edge technological advances. These factors are radically transforming the nature of attacks, requiring constant vigilance and adaptation.

At the heart of current geopolitical tensions, Europe finds itself on the front line, a prime target for cybercriminals who are refining their methods at an alarming rate. We are witnessing the emergence of unprecedented tactics, including hyper-volumetric DDoS attacks and the sophisticated exploitation of artificial intelligence, which are redefining the digital battlefield.

These new approaches are particularly challenging for large and medium-sized companies. The complexity of their information systems, combined with a certain organizational inertia, makes them particularly vulnerable to increasingly refined attacks. Faced with this growing threat, the Paris 2024 Olympic Games illustrate a real awareness and increased preparation, making this event a case study in security cooperation.
In this difficult context, it is becoming imperative to establish enhanced cooperation, both at European and international level, to effectively combat these threats. Furthermore, the responsibility of software publishers in securing digital environments must be clearly asserted and integrated into cyber defense strategies.

It’s time to mobilize: together, let’s strengthen our defenses and anticipate tomorrow.



01.

RANSOMWARE: THE INVASION CONTINUES

The number of victims worldwide rose by almost 29% between 2023 and 2024.

In France, there was an increase of almost 82% (vs. 2023, 155 victims listed).

In 2024, the median threat detection time (MTTD) observed by CERT Almond was two days.

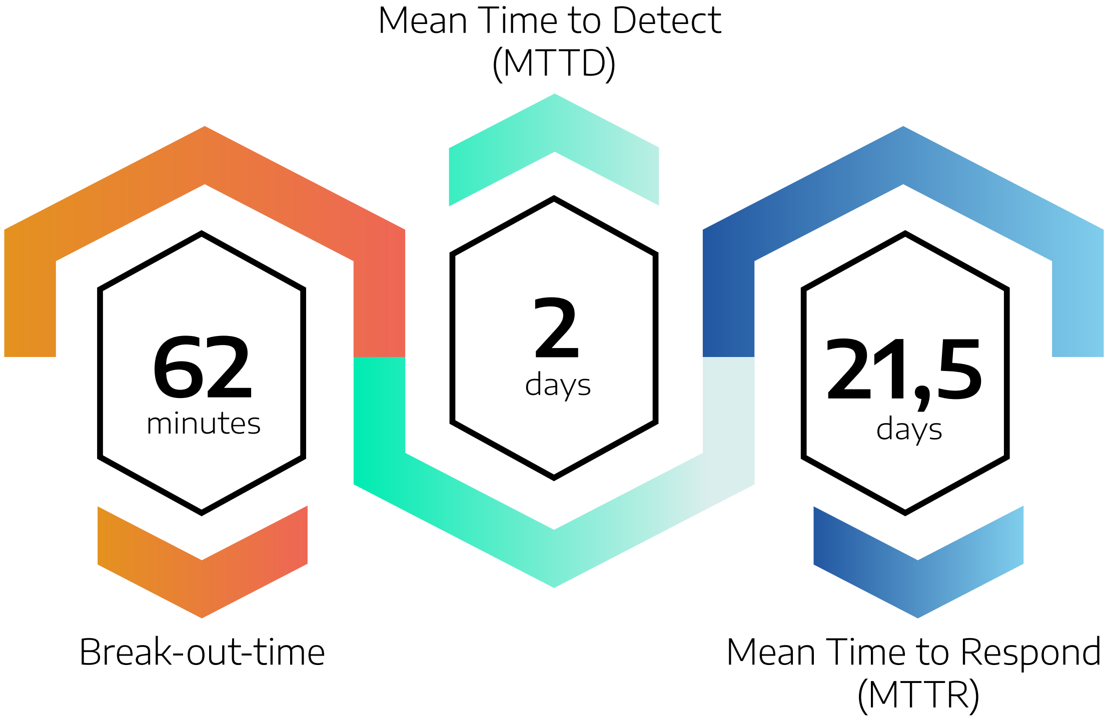
Those numbers remind us that attackers always have advance time on the defense.

CWATCH OBSERVATIONS

5 642
ransomware victims in 2024 in the World

2 170
ransomware victims in Europe

282
French ransomware victims



Mean Time to Detect (MTTD)

62 minutes

2 days

21,5 days

Break-out-time

Mean Time to Respond (MTTR)

01.

RANSOMWARE: THE INVASION CONTINUES

What lies behind the rankings

Data can be incomplete as it was mainly compiled from Western sources.

This report is based on the publicly disclosed victims on the walls of shame of cybercriminals. Caution, they don't display all their victims ***as we have seen in our incident response team with only one out of two attacks are claimed.***

RANSOMWARE VICTIMOLOGY

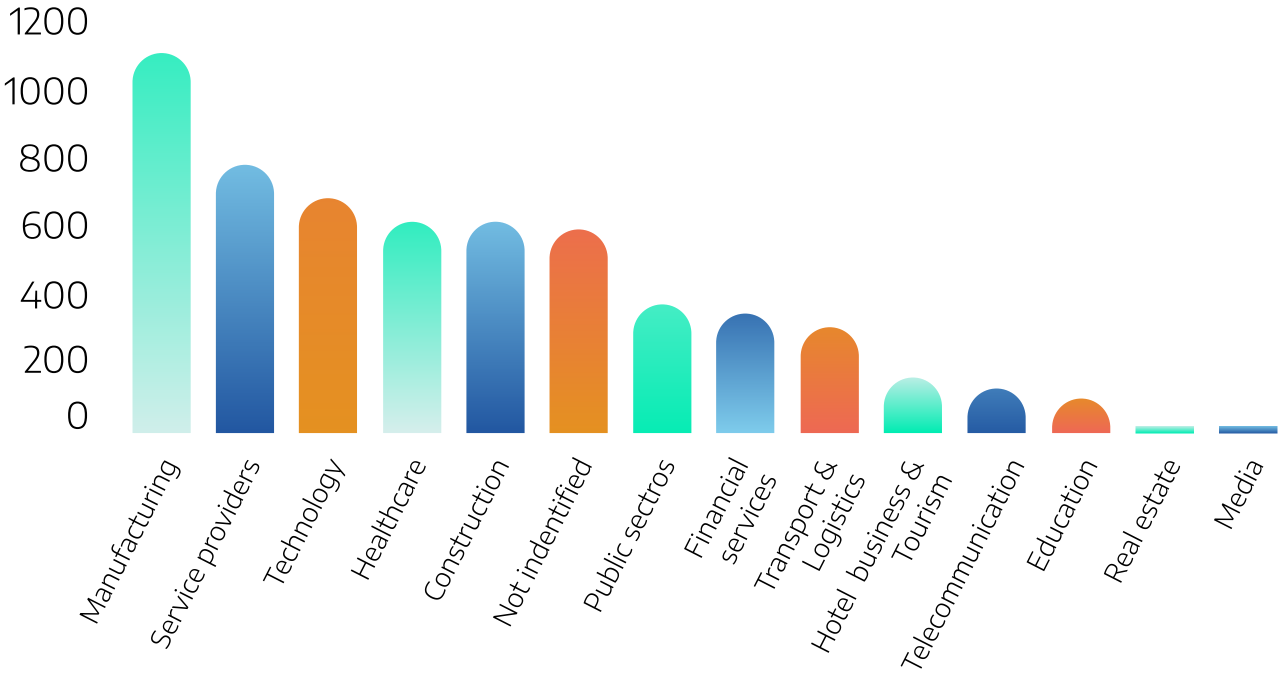
The terms **industry** covers the majority of critical infrastructure such as energy, aerospace, agricultural production, water distribution, etc. It's a sector, like **healthcare**, that attracts attackers because of its **media coverage**. Emerging groups see it to gain **brand recognition** and assert their presence in the competitive ecosystem of RaaS.

TOP 3

01. Manufacturing

02. Service providers

03. Technology



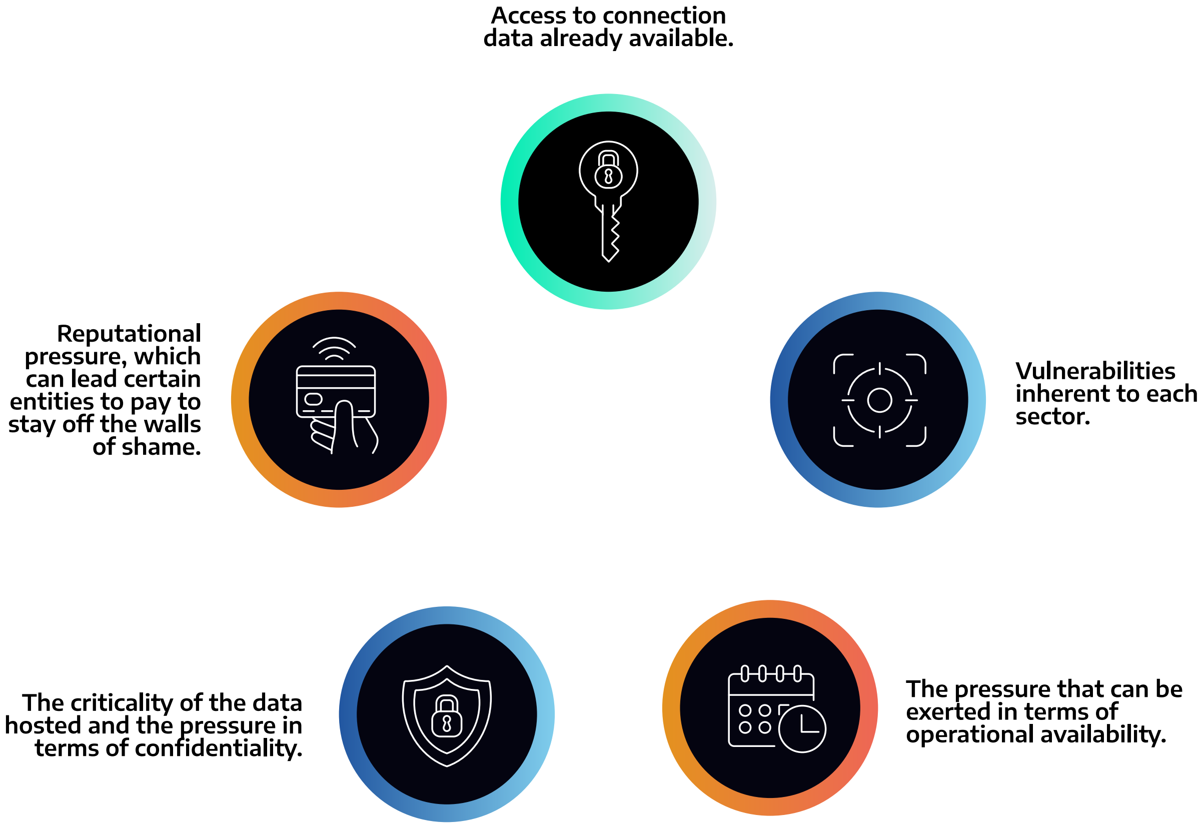
01.

RANSOMWARE: THE INVASION CONTINUES

Almond observes that in this edition, industry and services remain in first and second place respectively.
See the Almond Threat Landscape 2023/2024

SELECTION OF POTENTIAL VICTIMS BY RANSOMWARE GROUPS

The 10 most affected sectors by ransomware have remained the same for several years. Variations can be observed **in terms of ranking**. To maximize their success in terms of financial gain, ransomware operators regularly target entities that **can afford to pay**.
They can base their selection on those conditions:



Access to connection data already available.

Reputational pressure, which can lead certain entities to pay to stay off the walls of shame.

Vulnerabilities inherent to each sector.

The criticality of the data hosted and the pressure in terms of confidentiality.

The pressure that can be exerted in terms of operational availability.

01.

RANSOMWARE: THE INVASION CONTINUES

Here is the new generation

The ransomware threat landscape has been reshaped with the rise of several groups and the permanence insured par **LockBit** which remains unresolved.

It is common within the ransomware ecosystem that groups are formed to claim as many victims as possible in a given period before disbanding and continuing their activities under a new identity.

COMPARISON OF GROUP DISTRIBUTION 2023/2024

TOP 2024

Lockbit	518
RansomHub	505
Play	337
Akira	282
Hunters	215
Medusa	206
BlackBasta	174
Qilin	171
Bianlian	161
Incransom	155

TOP 2023

Lockbit	1 030
AlphV	416
Cl0p	384
Play	301
8Base	269
Bianlian	178
BlackBasta	176
Malas	173
Akira	160
Medusa	145

According to our data, **LockBit** remains in the leading position despite destabilization operations conducted by the coordinated authorities of several countries since February 2024 and the arrest in December of the group's members **including the alleged developer Rostislav Panev**.
It is closely followed by **RansomHub** who started from the code of the **Knight** ransomware, which constituted a key element of its rise. When it comes to **Play**, this group has allegedly benefited from the collaboration - or at least the interest - of the North Korean group Jumpy Pisces to conduct some operations.

In 2023, the **LockBit** group was followed by **AlphV** and **Cl0p** whom both experienced a sharp slowdown of their activities this year. The **revindications of AlphV have dropped by 87% and those of Cl0p by 96%.** Furthermore, **the** 8Base **group experienced a 47% drop in their activities.**
The business of Play increased by 12%.

01.

RANSOMWARE: THE INVASION CONTINUES

Multifaceted impacts

After having launched an attack against the Bologna football club, **RansomHub broadcast data about financial, personal and medical information of players as well as sponsorship contracts.** Strategic plans regarding transfers, data on supporters, employees and club affiliates were also found.

TIMELINE OF THE RESUMPTION OF ACTIVITIES AT COPPELL

Fear on the city

In October 2024, **RansomHub** targeted the city of Coppell, in Texas, as well as the Minneapolis Park and Recreation Board. The attack disrupted the WIFI, municipal court activities, the library services and the inspection and license platforms.

Priority given to profit

This year, the group **Dark Angels** demanded the highest ransom ever reported, more than **75 million dollars, to Cencora** an American pharmaceutical company. The average price of a ransom was more than 2 million the dollars in 2023.

The visibility which benefits ransomware groups because of their seizing impact for the victims should not dissimulate a **more complex financial ecosystem** which is of far greater benefit to other malicious actors.

October 23

Cyberattack detected and impacting a major part of the city's services

November 1st

Restoring telephone services

November 14

Reinstatement of utility billing forms

November 15

Local libraries back in service

November 20

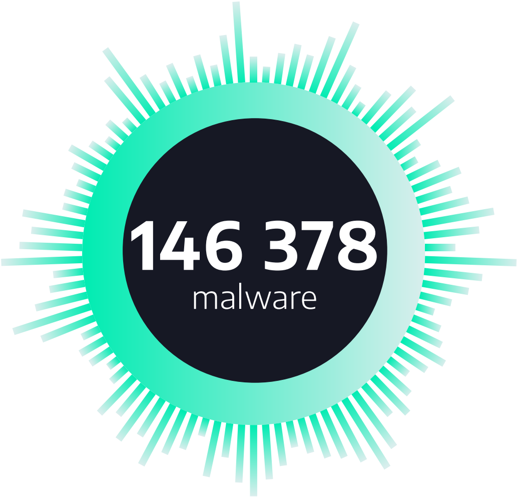
Cancellation of municipal events

02.

THE LUCRATIVE BUSINESS OF INFOSTEALERS

An infostealer is a malicious program which aims to collect sensitive data such as authentication, registered banking information, etc. Just like the Ransomware-as-a-Service, these programs are developed by groups then sold as Malware-as-a-Service to all comers. The financial gain from the sale of the collected data enabled, as the ransomware business, to professionalize the ecosystem.

INFOSTEALER, SO FASHIONABLE



In 2024, nearly 146 378 malware have been identified by Anyrun, the [majority](#) with infostealers' features. This year confirms the growth of their activities in the malware landscape. Inexpensive tools, easily accessible and within the reach of "novices", infostealers are becoming increasingly popular as the market for stolen data grows ever more lucrative. Too often without the victim even being aware that exfiltration has taken place.

snowflake

Help, dataleak...

Snowflake found itself in turmoil. A **large-scale campaign** aimed at collecting the hosted data for profit resale. It's not Snowflake company that's been compromised. It has been highlighted as part of the [incident response](#) that customers' accesses to the platform have been collected and sold by **multiple infostealers** such as **LUMMA, Redline, Vidar et MetaStealer** for at least four years. In addition to this, the absence of multifactor authentication on these environments was noticed. **The purchase by a threat actor of one of these valid accounts has enabled the compromising of at least one hundred clients, including Santander Bank and Live Nation.**

02.

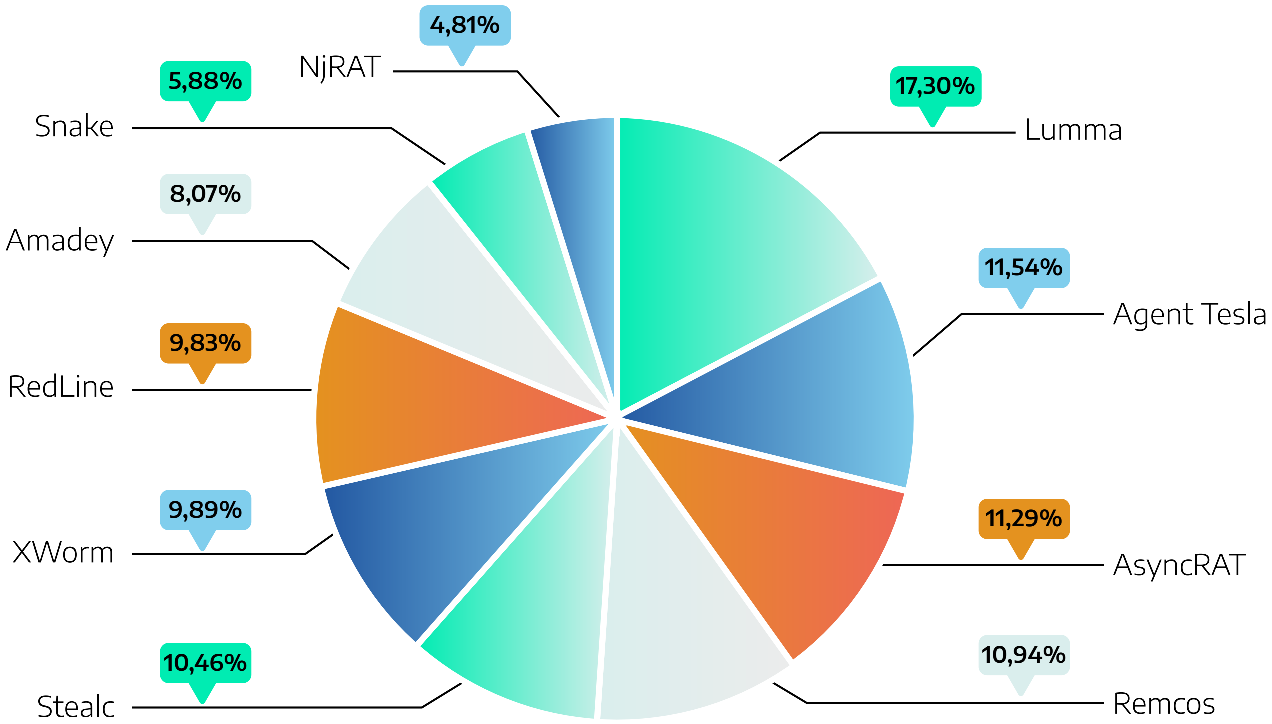
THE LUCRATIVE BUSINESS OF INFOSTEALERS

In 2024, three families of malware stand out.

Lumma Stealer appears to be one of the most prolific *malware-as-a-service* this year. From the second half of the year onwards, the popularity of this infostealer has felt as it moves ahead of the very popular Remcos, AsynRat and AgentTesla.

These commercialized infostealers feed the Initial Access Broker market, vital for ransomware groups. In this competitive environment, investment in improving their offensive capabilities has led to constant shuffling in the rankings. The disruption of cybercriminal networks by the authorities in 2024 also contributes to this chess game.

TOP OF THE MALWARE FAMILIES



TOP 1

LummaStealer

MaaS with advanced features sold on a subscription basis (up to $1 000/month). Beyond its data exfiltration capabilities, it offers multiple defensive evasion options, making detection complex.

TOP 2

AgentTesla

A widely used RAT with infostealer and keylogger capabilities. This malware as a service (MaaS) is often used by initial access brokers in targeted phishing campaigns.

TOP 3

AsyncRAT

A very popular RAT in the cybercriminal community, thanks to its open-source access. Available on GitHub, it features keylogger, initial access exfiltration and payload repository functions.

IMPACT

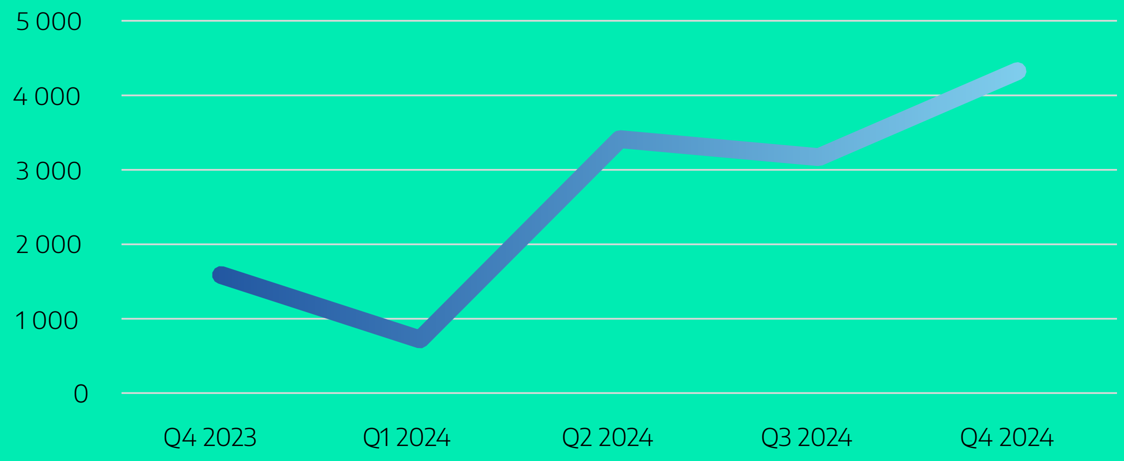
THE LUCRATIVE BUSINESS OF INFOSTEALERS

In recent years, defensive actions by governments have multiplied. Cooperation between public entities (national police forces, Europol, FBI, etc.) and private entities (recognized security companies), these operations tend to weaken criminal networks. They demonstrate the offensive capabilities of the international community in the face of the resurgence of cyber-attacks in all their forms.

A race against time

Operation Magnus

After Operation Cronos, which had a major impact on **LockBit**'s activities, came **Operation Magnus**. The aim of the international cooperative action of October 28, 2024, was to dismantle the **Redline and META** infostealer networks. The success of this operation may explain the disappearance of MetaStealer from the rankings as of Q4 2024. Redline, one of the most popular MaaSs, accounted for almost **30%** of total detections in 2023. As a direct or indirect consequence of the operation, it lost its leading position and **dropped to 7th place, despite an upturn in activity** towards the end of the year.
The aim of these operations is to **disrupt these supply networks** and, even temporarily, **reduce the overall** cybercriminal activity providing initial access.

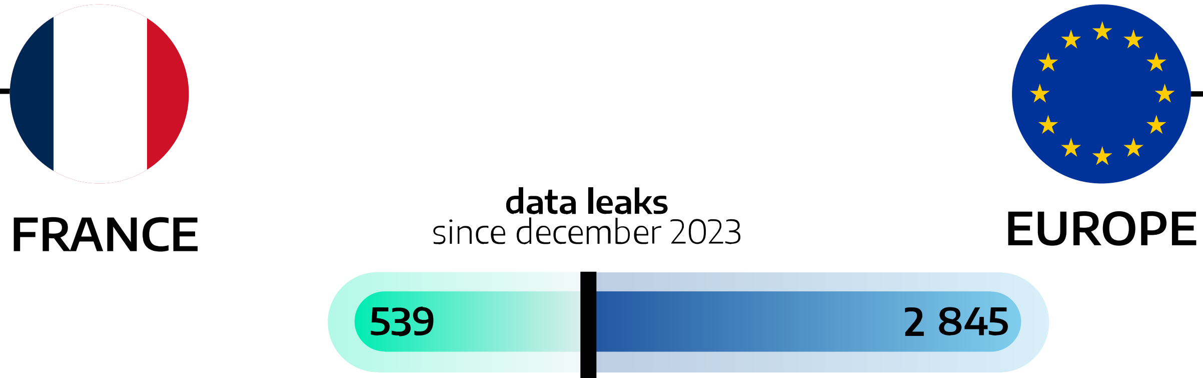


03.

DATA BREACHES: A PRODUCTIVE YEAR FOR CYBERCRIMINALS

This number is partially biased due to the lack of coverage regarding entities located in certain regions which do not have elaborate regulations. Thus, they are less likely to report data breaches.

DATA LEAKS IN FRANCE AND IN EUROPE


FRANCE

data leaks
since december 2023

EUROPE

French companies have been particularly affected this year by data breaches. There are thousands, even millions of customers whose data has been leaked online.

The inflation of the number of data stolen can have several explanations:

- France has been particularly highlighted on the international scene this year.
- Attackers who would be specialized in reselling French access or databases.
- Service providers have been compromised as part of a supply chain attack.

Security investments in Europe remain insufficient as we observe strong inequalities within Europe due to unequal maturity levels from one country to another.

Nordic countries appear to be more aware, especially because of their proximity to Russia, which can explain the reduced number of incidents reported if we make a comparison with Western Europe. However, the recent adhesion of Sweden and Finland to NATO puts the resilience of their organizations and infrastructure to the test.

At the same time, a better familiarization with regulations combined with compliance requirements encourages organizations to further report data breaches. This number could increase even more with the implementation of DORA, starting in January 2025, which requires financial institutions to guarantee the security of data transmission.

IMPACT

DATA BREACHES: A PRODUCTIVE YEAR FOR CYBERCRIMINALS

Targeted organizations have an increased vulnerability to phishing and social engineering attacks. Incidents of this nature damage the brand image of the company as well as their customers' trust , which can indirectly lead to financial loss.

The protection of data, a challenge in the fight against cybercriminals

Record data leak: France Travail and Cap Emploi targeted by cybercriminals

Among the numerous attacks undergone by France, the databases of **France Travail and Cap Emploi containing the personal information of 43 million individuals** (social security number, identity, address) have been compromised. This massive violation of data is sure to arouse the interest of threat actors on cybercriminal forums given the scale of the phishing campaigns that can be carried out.

The European Parliament, guardian of the GDPR, in turn exposed!

Despite its work on the protection of data, the European Parliament is not exempt from being targeted. In May 2024, a data breach that affected the human resources of the Parliament has been made public. It concerned the data of **8 000 applicants for fixed-term contracts** (identity cards and passports, criminal record extracts, residence documents, and even sensitive information such as marriage certificates revealing a person's sexual orientation).

04.

CWATCH

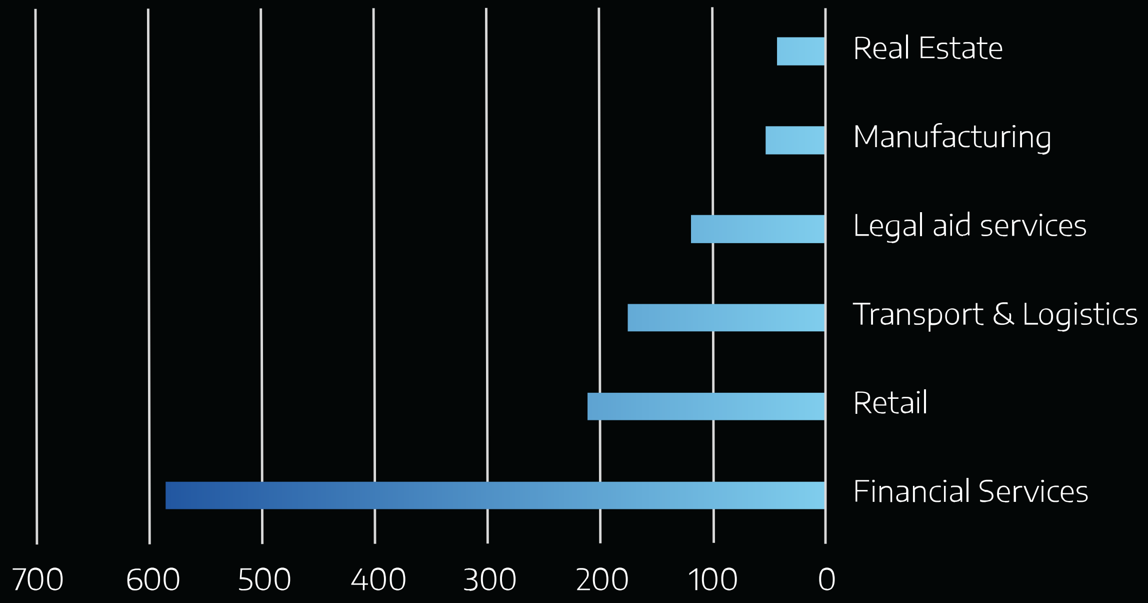
CWATCH OBSERVATORY

Through its services, Almond helps its customers anticipate threats and protect their information systems. Day-to-day, the CWATCH SOC monitors and detects security incidents of any kind.

TOP 5 VICTIMOLOGY OF CWATCH IN 2024

In 2024, the **Financial Services** sector has been the most targeted by attempts and/or proven compromissions, followed by **Retail as well as Transport & Logistics.**

If phishing campaigns are a daily batch, entities in **Insurance** and **Private Equity** are the first victims. These two sectors are also particularly sensitive to internal threats, especially in the context of data exfiltration.



The monitoring of stolen databases ensures the rapid identification of possible entry points via valid accounts. Observable on every perimeter, the Finance and Commerce sectors are particularly subject to the **compromising of their collaborators' accounts** which are then put up for sale.

04.

CWATCH OBSERVATORY

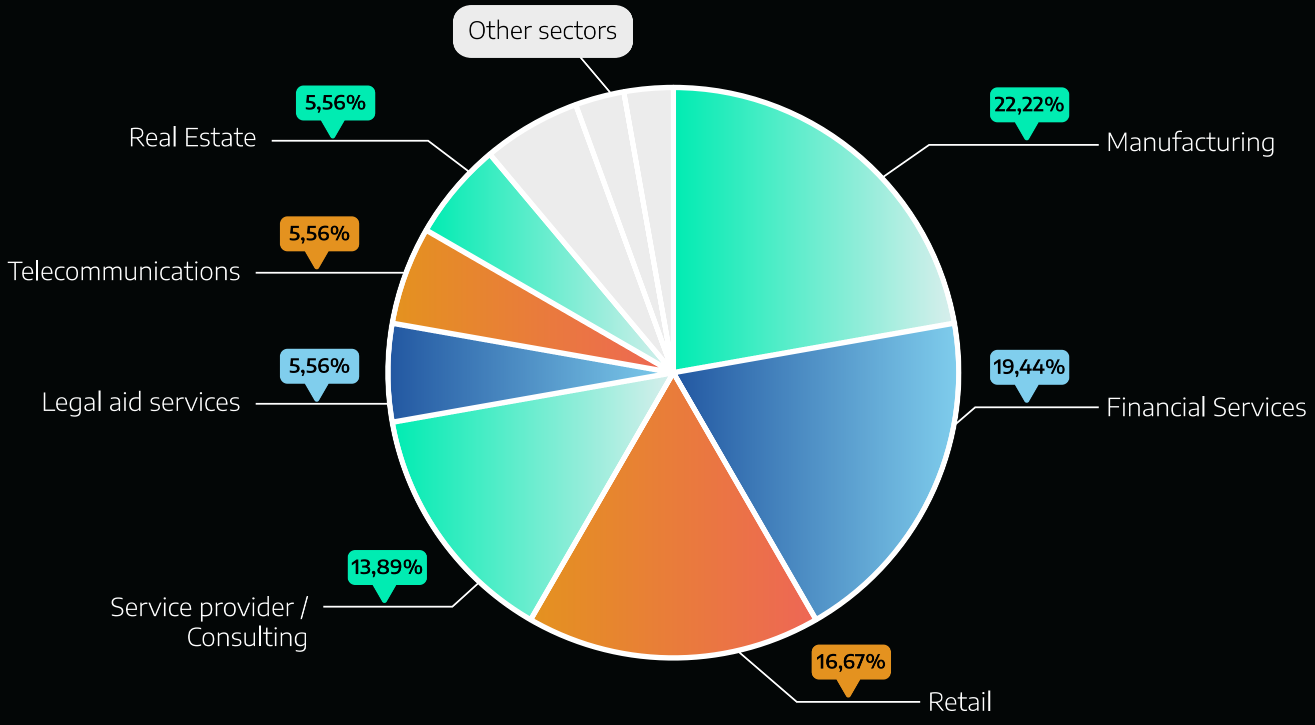
The Almond CWATCH CERT has participated besides nearly 80 French CERTs to the first edition of the InterCERT France Incidentology report.

Almond has contributed up to 10% of the total of incidents reported in 2023 as part of the incident response. Healthcare, Consulting and the Transportation sector topped the ranking

VICTIMOLOGY OF INCIDENT RESPONSES OF THE CERT

Looking at the CERT Almond data, the **Industry, Financial Services and Retail sectors have made up a major part of the incident responses throughout the year.**

Healthcare, consulting and transportation came out on top.



IMPACT

CWATCH OBSERVATORY

Discover the Olympic Games **infography**

Cybersecurity Insights

Paris 2024 Olympic Games: a breeding ground for cyber threats

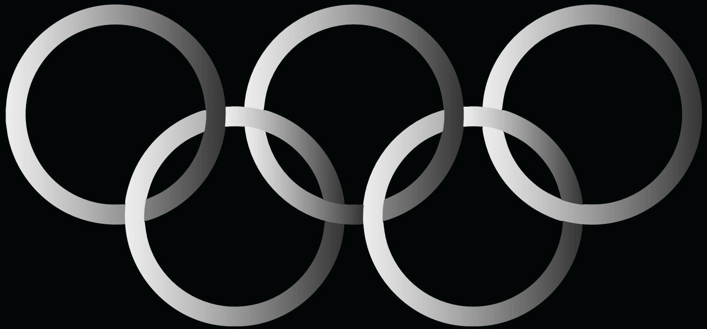
CWATCH

A Parisian summer in the limelight... of medals!

For four years, France and the security teams prepared for a steep rise of cybercriminal activity during the 2024 Olympic Games in Paris. It would seem that, ultimately, cybercriminals also enjoyed the summer as there was no major incident in this period.

Keeping the spotlight on France for 4 weeks with a **tried-and-tested safety system, France CERTs and SOCs on the alert and companies sensitized** could have had the effect of deterring compromising attempts.

Once again Armageddon won't have happened!



04.

CWATCH

CWATCH OBSERVATORY

TTPs: An array of offensives

MITRE | ATT&CK®

TOP 10 OF THE 2024 MITRE ATT&CK TECHNIQUES

01
[T1566]
Phishing
Initial Access

02
[T1562]
Impair Defenses
Defense Evasion

03
[T1078]
Valid Accounts
Defense Evasion, Initial Access, Persistence, Privilege Escalation

04
[T1059]
Command and Scripting Interpreter
Execution

05
[T1204]
User Execution
Execution

06
[T1053]
Scheduled Task/Job
Execution, Persistence, Privilege Escalation

07
[T1548]
Abuse Elevation Control Mechanism
Defense Evasion, Privilege Escalation

08
[T1546]
Event Triggered Execution
Persistence, Privilege Escalation

09
[T1584]
Compromise Infrastructure
Resource Development

10
[T1651]
Cloud Administration Command
Execution

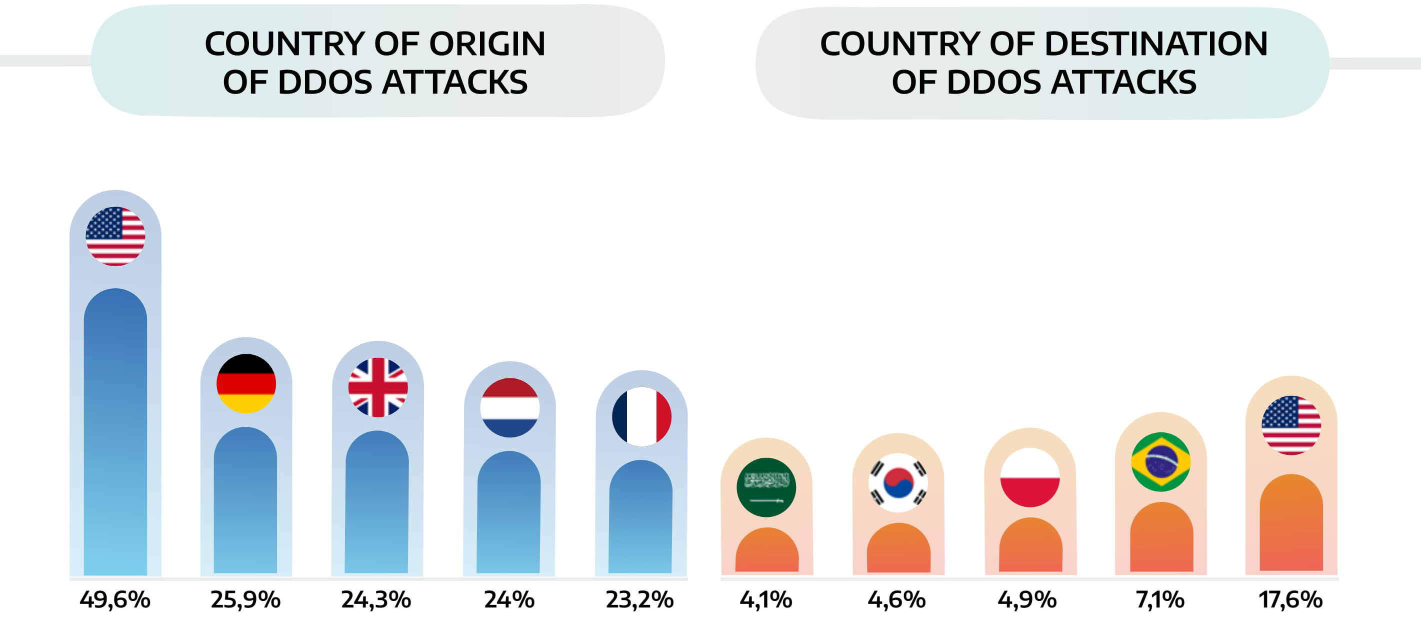
05.

DDOS: EUROPE IN THE COLLIMATOR

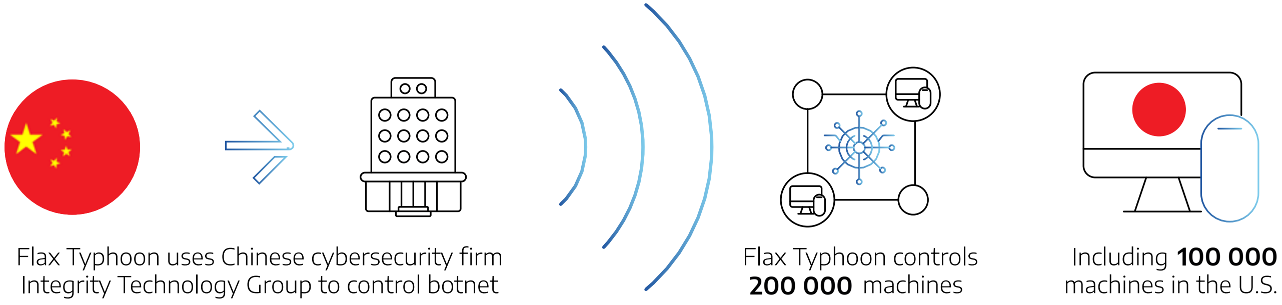
Already observed in 2023, the share of DDoS operations continued to grow in 2024.

The intensification of the war in Ukraine, the shifting of power balance in the Near and Middle East in connection to the fall of the Syrian leader, the setback inflected to Moscow, the increasing tensions in Pakistan, are all revindications for hacktivist groups.

Despite the intensity of these events, most DDoS attacks came from the **United States** followed by **Great Britain** as well as a **few Western European countries including France**.



This type of attack, whether they are perpetrated by an individual or a group, use a compromised network located outside of the network's borders.



Flax Typhoon uses Chinese cybersecurity firm Integrity Technology Group to control botnet
Flax Typhoon controls **200 000** machines
Including **100 000** machines in the U.S.

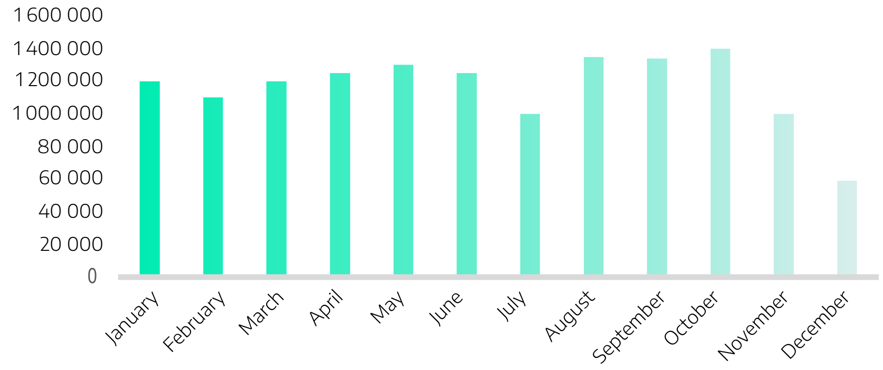
Example of Flax Typhoon, a Chinese botnet

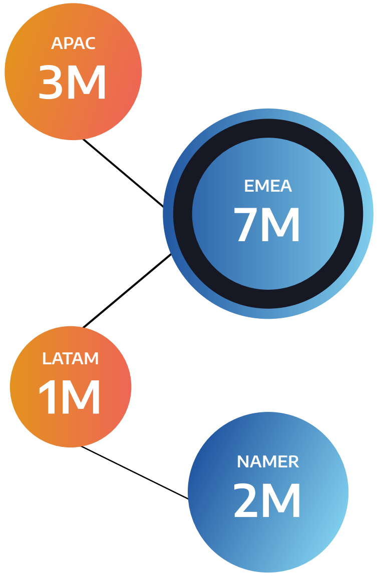
05.

DDOS: EUROPE IN THE COLLIMATOR

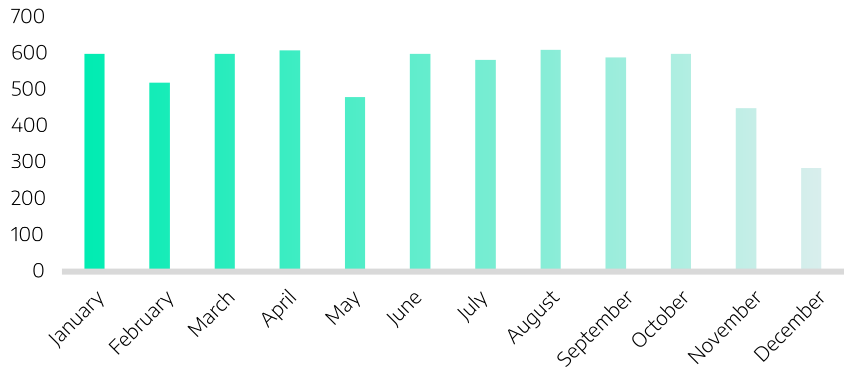
On a global scale, the frequency and the volume of attacks remained elevated and relatively stable. A slight increase in frequency can be observed from July to October.

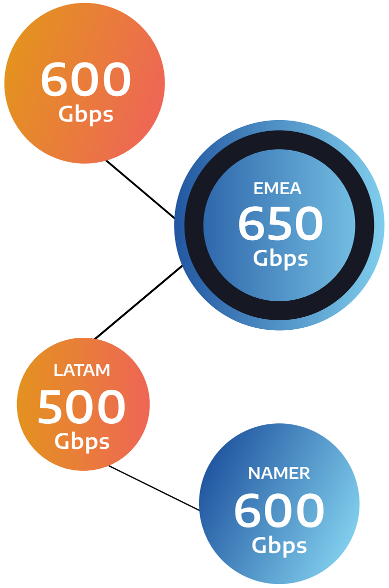
FREQUENCY OF ATTACKS IN MILLIONS IN THE WORLD





VOLUME OF ATTACKS IN GBPS IN THE WORLD



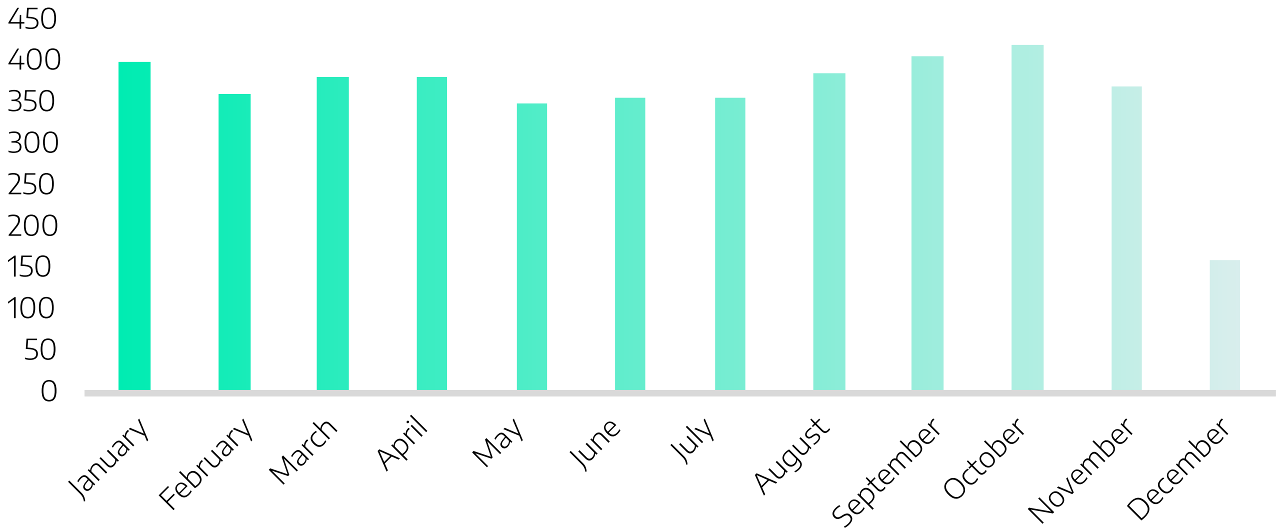


05.

DDOS: EUROPE IN THE COLLIMATOR

DDOS-style attacks are of low intensity but disrupt the course of an organization's activities. According to a joint study led by Splunk and Oxford Economics, the degradation of services and breakdowns cost Global 2000 companies $400 billion a year.

SPEED OF ATTACKS TARGETING EUROPE IN MPPS



VOLUME OF REPORTED ATTACKS TARGETING EUROPE

400 000
DDoS attacks
per month

A consequence of European powers regarding global geopolitical events, European states suffered a high level of attacks throughout the year. Attacks carried out as part of the conflict between Russia and Ukraine may influence the values indicated

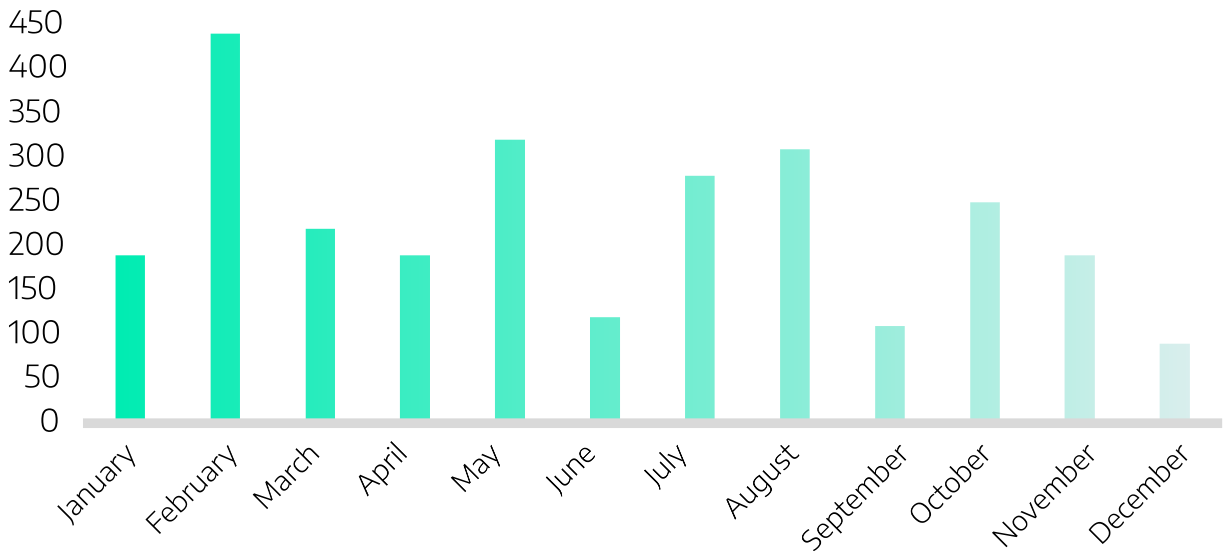
05.

DDOS: EUROPE IN THE COLLIMATOR

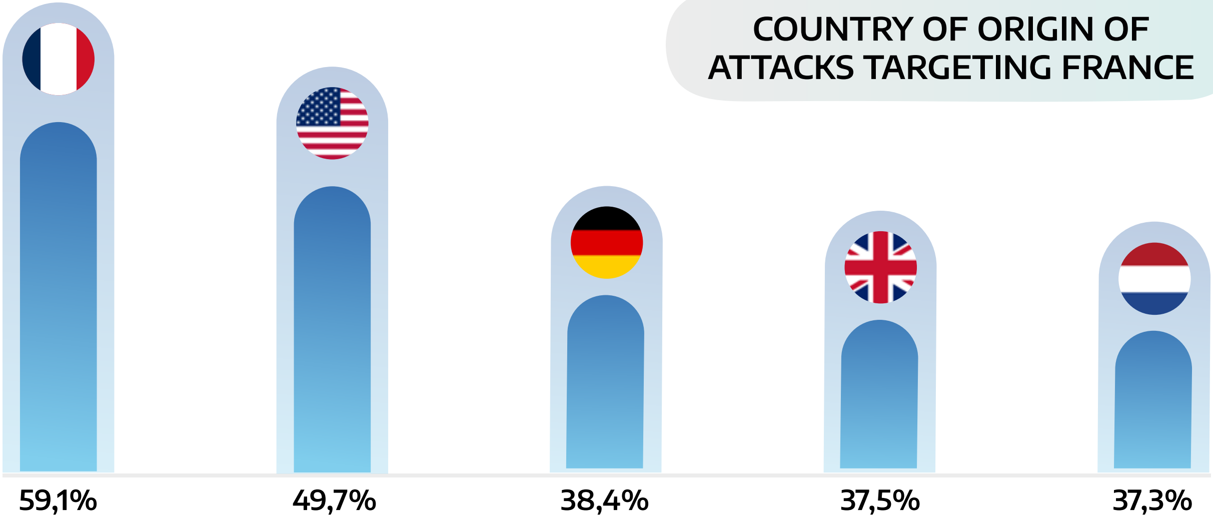
Attacks on France mainly come from **West European** countries as well as the **United States**. France leading the way, it is possible that French attackers focus on compromising machines located on their own territory due to linguistic and cultural proximity.

The fastest attacks were led in July 2024, a date matching the beginning of the 2024 Olympic Games in Paris. The sensitivity of targeted entities can explain the speed of execution of attacks.

VOLUME OF ATTACKS IN GBPS TARGETING FRANCE



COUNTRY OF ORIGIN OF ATTACKS TARGETING FRANCE



Volume and countries of origin of attacks targeting France

IMPACT

DDOS: EUROPE IN THE COLLIMATOR

Because of its position regarding the situation in Ukraine and Israel, France has been a target of choice in 2024 to launch DDoS campaigns. The hacktivist coalition « **Holy league** » appeared in July. Made up of nearly 70 members, it unites **against Europe, Ukraine, Israel and NATO**. Taking advantage of the political uncertainty surrounding the government of Macron, several groups such as **NoName057(16), Mr. Hamza, Anonymous Guys** attacked private and public entities in France in late 2024.

The group **NoName057(16**) which has played a central role in this upsurge of DDoS attacks against France beyond the coalition, just like **RipperSec**.

Geopolitic reprisals

February 2024
Statement by Emmanuel Macron on the deployment of European armed forces in Ukraine.

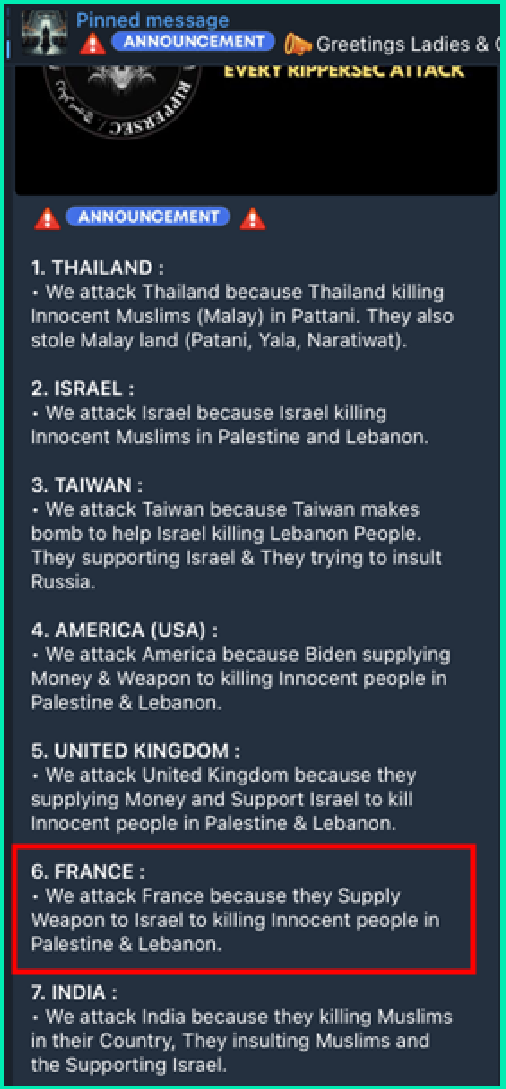
March 2024

- Outbreak of an attack in Moscow that the Kremlin believes may have been organized by the French state.
- In March 2024, government services also reported attacks on an unprecedented scale, claimed by Anonymous Sudan among others, the impact of which was reportedly contained. The critical nature of the targeted entities may explain a slight increase in speed in March.

August 2024
The Olympic Games were held in Paris, and Pavel Duro was arrested for his limited efforts to curb the proliferation of cybercriminal activities on the platform.

As the year draws to a close, France is once again the target of what appears to be a coalition of "Holy League" hacktivists. Groups such as NoName057(16), Mr. Hamza and Anonymous Guys have taken advantage of the political uncertainty to attack French private and public entities.

December 2024
A number of hacktivist groups have taken advantage of Michel Barnier's resignation to target some fifty French websites, mainly government sites.



Pinned message
⚠ ANNOUNCEMENT 📣 Greetings Ladies & (

⚠ ANNOUNCEMENT ⚠

1. THAILAND :
• We attack Thailand because Thailand killing Innocent Muslims (Malay) in Pattani. They also stole Malay land (Patani, Yala, Naratiwat).

2. ISRAEL :
• We attack Israel because Israel killing Innocent Muslims in Palestine and Lebanon.

3. TAIWAN :
• We attack Taiwan because Taiwan makes bomb to help Israel killing Lebanon People. They supporting Israel & They trying to insult Russia.

4. AMERICA (USA) :
• We attack America because Biden supplying Money & Weapon to killing Innocent people in Palestine & Lebanon.

5. UNITED KINGDOM :
• We attack United Kingdom because they supplying Money and Support Israel to kill Innocent people in Palestine & Lebanon.

6. FRANCE :
• We attack France because they Supply Weapon to Israel to killing Innocent people in Palestine & Lebanon.

7. INDIA :
• We attack India because they killing Muslims in their Country, They insulting Muslims and the Supporting Israel.

IMPACT

DDOS: EUROPE IN THE COLLIMATOR

The fastest attacks were conducted in July 2024, which corresponds to the start of the Olympic Games. The sensitivity of targeted entities can explain the speed of execution of attacks.

Hyper-volumetric attacks

The adoption of AI to assist cybercriminals in the conduct of their botnet attacks makes it easier to circumvent defensive measures and imitate legitimate traffic.

They use huge volumes of traffic to overload a target's network

They generate huge volumes of bandwidth (up to 100 Gbps, or even terabits per second)

They use gigantic networks of consisting of machines comprising tens or hundreds of thousands of devices.

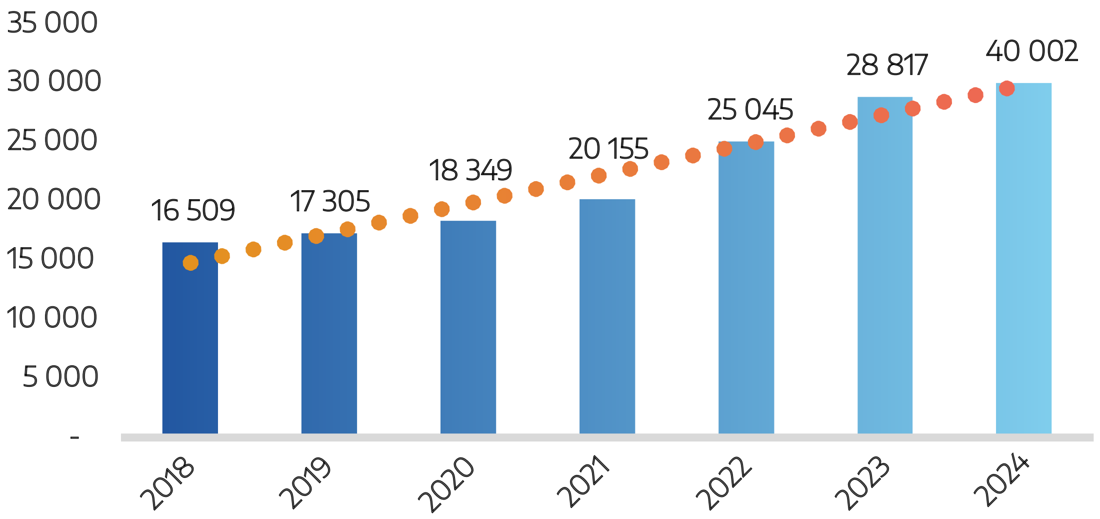
This makes it almost impossible for the targets to defend themselves against these attacks. Hyper-volumetric attacks are a subset of a larger model of DDoS attacks which are becoming increasingly complex and powerful. To conceal more targeted attacks, they often mix volumetric attacks with attacks on the application layer.

06.

LET'S TALK VULNERABILITIES

The year 2024 was once again marked by an increase in vulnerabilities. The visible impact appears to be the inability of entities to consider this volume in their patch management program (if any), as it represents a significant cost. In the face of this frantic race, is there an explanation for this phenomenon, which shows no sign of slowing down?

VULNERABILITIES IN 2024



A FEW KEYS TO UNDERSTAND THE SITUATION

Entities being more and more dependent on digital solutions, new products are entering the market every year with their own set of vulnerabilities. In relation to the number of existing solutions, can we say that the number of vulnerabilities is on the same curve?

More and more companies are specialized in the discovery and publication of vulnerabilities as their business model, which could explain to some extent the annual growth in volume.

Today's data are based on the NVD's annual CVE figures. Vulnerabilities without CVE or the SaaS products' vulnerabilities are not considered and could also affect the total volume.

Some of the published vulnerabilities include bugs and configuration errors which, in the sense of security, are not so.

06.

LET'S TALK VULNERABILITIES

Another EPSS scoring system has been introduced in addition to the CVSS score to help organizations better prioritize vulnerability management, not based on criticality but on actual exploitation. *However, certain vulnerabilities, which have been identified as being exploited by APT or ransomware groups, have low CVSS and/or EPSS scores. If scores can be used to sort through the volume of data, it is essential that the subject of vulnerability management is approached in a cross-functional manner between the Cyber Threat Intelligence, the CISO as well as patch management teams to make informed, contextualized decisions.*

RETROSPECTIVE ON VULNERABILITIES IN 2024

Over the year 2024, 2,291 critical vulnerabilities have been listed, up +44% compared with 2023. If we look at the CVE exploited, without severity criteria, the KEV catalog counts 186. This represents 0,5% of the total of reported vulnerabilities. In our 2023-2024 Threat Landscape, we have already observed the start of 2024 marked by the targeting of tools widely used by companies worldwide. The trend has been confirmed with the trio Ivanti, Fortinet and PaloAlto. Equipment from these publishers has been among the most targeted in terms of critical vulnerabilities exploitation.

Fortinet

February 2024
CVE-2024-21762, an out-of-bound write flaw in Fortinet FortiOS; score CVSS 9.8 and score EPSS 2.11%

October 2024
CVE-2024-47575, a missing authentication in FortiManager; score CVSS 9.8 and score EPSS 88.63%

PaloAlto

April 2024
CVE-2024-3400, a command injection flaw in Palo Alto Networks PAN-OS score CVSS 10; score EPSS 96.37%

November 2024
CVE-2024-9474, a privilege escalation vulnerability in Palo Alto Networks PAN-OS software; score CVSS 7.2; score EPSS 97.52%

Citrix

January 2024
CVE-2023-6549, an improper Restriction of Operations within the Bounds of a Memory Buffer in NetScaler ADC and NetScaler Gatewayscore; score CVSS 7.5 and score EPSS 1.23%

Ivanti

January 2024
CVE-2024-21887, a command injection flaw in Ivanti Connect and Policy Secure; score CVSS 9.1 and score EPSS 97.11%

CVE-2023-46805, a remote authentication bypass flaw in Ivanti Connect and Policy Secure; score CVSS 8.2 and score EPSS 96.41%,

CVE-2024-21893, an elevation of privilege flaw in Ivanti Connect and Policy Secure score CVSS 8.2 and score EPSS 95.90%

Cisco

July 2024
CVE-2024-20399, a command line interface command injection flaw in Cisco NX-OS Software; CVSS 6.7; score EPSS 0.25%

Microsoft

March 2024
CVE-2024-26169, Windows Error Reporting Service Elevation of Privilege Vulnerability; score CVSS 7.8; score EPSS 0.67%

REFERENCES

https://www.lebigdata.fr/ce-celebre-club-de-foot-frappe-par-un-ransomware-les-donnees-des-supporters-en-fuite

https://www.lemagit.fr/actualites/366599633/Ransomware-75-millions-de-dollars-la-rancon-record-obtenue-par-Dark-Angels

https://therecord.media/ransomhub-cybercrime-coppell-texas-minneapolis-parks-agency

https://www.oxfordeconomics.com/resource/the-hidden-costs-of-downtime-the-400b-problem-facing-the-global-2000/

https://www.euronews.com/next/2024/08/22/european-parliament-under-scrutiny-after-data-breach-complaints

https://www.francetvinfo.fr/replay-radio/le-choix-franceinfo/piratage-de-france-travail-la-direction-avait-ete-alertee-sur-une-faille-de-securite_6536786.html

https://cyble.com/blog/hacktivist-alliances-target-france/

https://www.helpnetsecurity.com/2024/02/22/stolen-credentials-exploit/

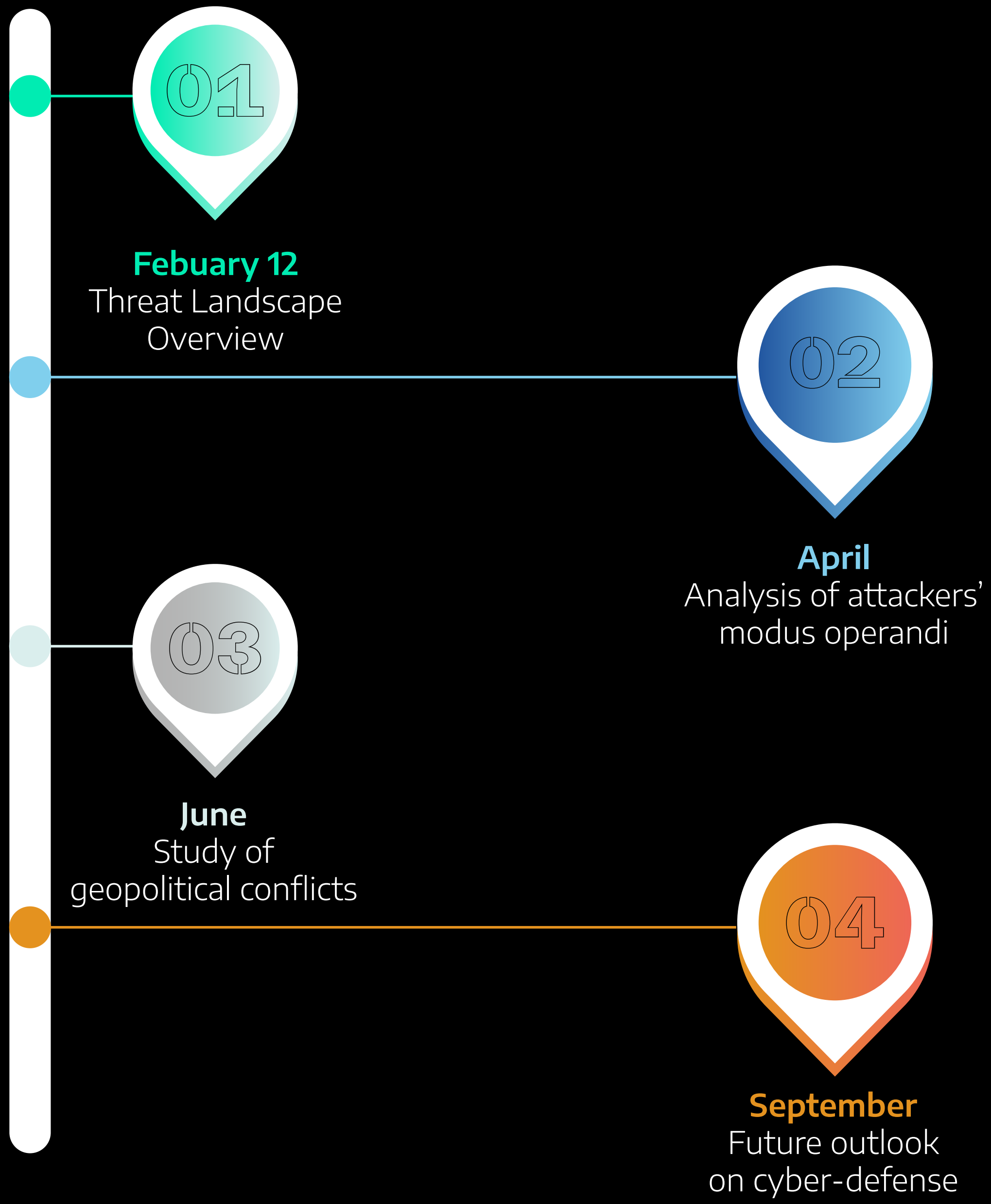
https://www.cisa.gov/known-exploited-vulnerabilities-catalog

https://any.run/cybersecurity-blog/

https://nvd.nist.gov/

https://tribune-assurance.optionfinance.fr/depeches/d/2024-10-17-qbe-une-hausse-de-74-des-attaques-par-ransomware-en-2023.html

CALENDAR 2025



Febuary 12
Threat Landscape
Overview

April
Analysis of attackers'
modus operandi

June
Study of
geopolitical conflicts

September
Future outlook
on cyber-defense

almond

→ contact@almond.eu

→ +33 1 46 48 26 00