SOCRadar®
Your Eyes Beyond

FRANCE

Threat Landscape Report

SOCRadar®
Your Eyes Beyond

Table of Contents

Executive Summary 3
Technical Details 6
Recent Dark Web Activities Targeting France 8
Ransomware Attacks Targeting France 10
Top Threat Actors Targeting France 14
Stealer Log Statistics: Top Domains in France 19
Phishing Threats Targeting France 21
DDoS Attack Statistics 24
Lessons Learned: Key Insights and Strategic Recommendations 25

Executive Summary

France, known for its iconic landmarks like the Eiffel Tower, the elegance of Paris, and its world-renowned croissants, is a nation that blends tradition with modernity. Beyond its cultural and artistic heritage, France plays a significant role in the global digital landscape. As a nation deeply integrated into the world's technological and financial systems, France's advanced infrastructure and strategic importance make it a key target for cyber threats.

As the 2024 Paris Olympic Games approach on July 26, security experts say MSSPs and MSPs should already prepare to help their customers mitigate the risks of destructive and debilitating cyberattacks.
Recent data reveals a notable increase in cyber-attacks aimed at French critical infrastructure and essential sectors. These attacks are increasingly sophisticated, as threat actors employ complex tactics, techniques, and procedures (TTPs) to breach defenses and exploit vulnerabilities.

France faces cyber threats from various sources, including organized crime syndicates and state-sponsored entities. The country's prominence in manufacturing, information and telecommunication, and retail trade industries makes it a lucrative target for cyber espionage, financial theft, and disruptive operations.

The dark web significantly contributes to the proliferation of these threats, providing a clandestine marketplace for malicious tools, stolen data, and illicit services. The anonymity and reach of the dark web pose substantial challenges for French cybersecurity professionals striving to anticipate and mitigate these threats.

This report provides a comprehensive analysis of the threat landscape in France, utilizing extensive data from open-source and proprietary intelligence. By continuously monitoring cyber activities and scrutinizing attack patterns, our team delivers an in-depth overview of the threats facing French entities. The insights presented herein are designed to empower stakeholders across both public and private sectors to strengthen their cybersecurity defenses, reduce risks, and enhance France's resilience against future cyber threats.

Top Takeaways

Dark Web Dynamics: A Surge in Threat Actor Activity

In 2023, a diverse group of 309 threat actors actively targeted French enterprises, collectively posting 489 times on the dark web, predominantly trading in database sales, underscoring the criticality of data security measures.

Vulnerable Sectors: Targeting Information and Telecommunication

The Information and Telecommunication industry, making up 15.54% of dark web activities, stood out as the primary industry targeted by threat actors worldwide, highlighting its strategic importance and vulnerability to digital threats.

Ransomware Resurgence: A Year of Unprecedented Attacks

France grappled with 324 unique ransomware incidents throughout the year, with 157 attacks pinpointing the country as the primary target, revealing a focused aggression by threat actors.

Top Ransomware Threats: LockBit 3.0, Cl0p, and Play

Prominent ransomware groups, including LockBit 3.0, Cl0p, and Play, specifically targeted France, signifying the high stakes and sophistication of the country's cyber threat landscape.

Top Takeaways

Data Breaches on the Rise: The Impact of Stealer Logs

The widespread use of Stealer Logs in 2023 led to significant breaches, compromising critical data for thousands of individuals across France.

Phishing in the Digital Economy: Rising Threats in Delivery Services

The year also saw 3,203 phishing attacks, with a marked emphasis on the emerging Delivery Services industry. These attacks spotlighted the growing cyber risks in these innovative financial technologies.

DDoS Deluge: A Record Year of Attacks

France experienced a landmark DDoS attack involving 25 vectors and achieving a maximum bandwidth of 1,005 Gbps amidst a total of 202,397 DDoS incidents, illustrating the intense and escalating cyber assault landscape.

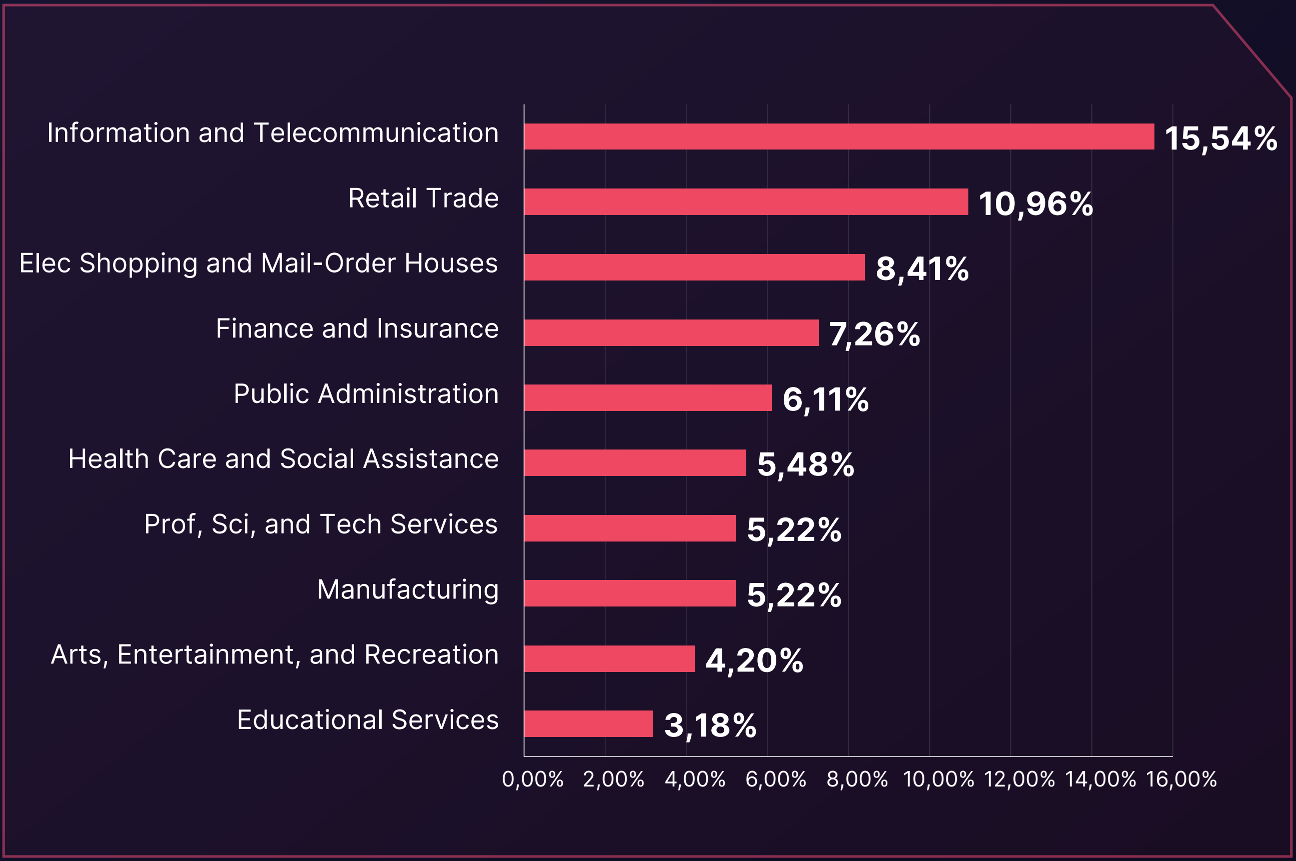
Technical Details

Dark Web Threats Targeting France

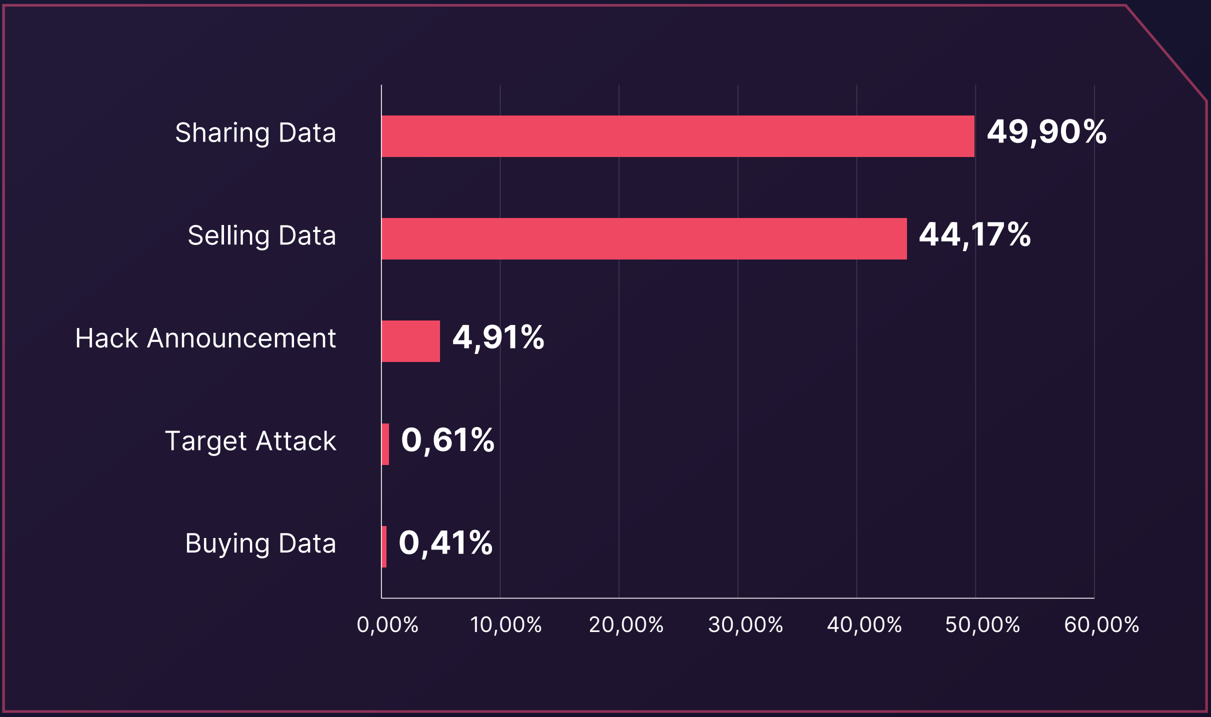
Over the past year, SOCRadar's Dark Web Analysts have meticulously monitored dark web activities, uncovering significant trends and establishing connections between French enterprises and covert threat actors. Throughout 2023, French entities faced a relentless wave of cyber threats, with various actors attempting to exploit successful intrusions by trading or leveraging their gains in dark web forums.

During this period, SOCRadar observed 489 dark web forum posts linked to 309 distinct threat actors. The Information and Telecommunication industry emerged as the most prominently affected sector, representing 15.54% of the identified cyber threats. Following closely, the Retail Trade and Electronic Shopping and Mail-Order Houses industries accounted for 10.96% and 8.41% of the threats, respectively.

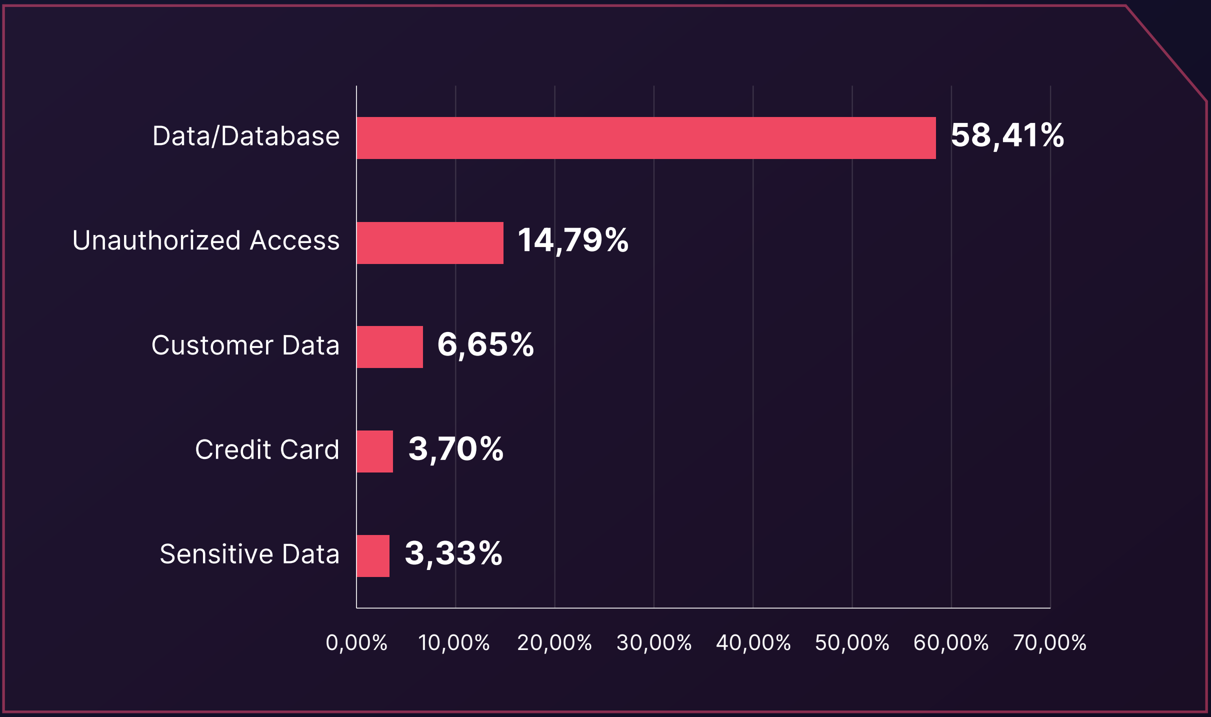
Industry Distribution of Dark Web Threats



Distribution of Dark Web Threats by Post Type



Distribution of Dark Web Threats by Threat Type



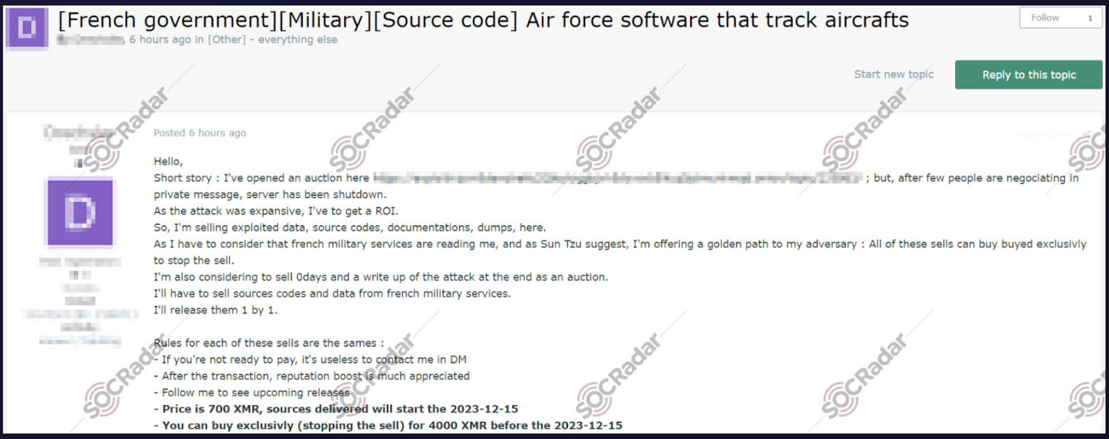
Protect your business from the dangers lurking in the hidden corners of the internet.

Book your demo

Recent Dark Web Activities Targeting France

Source Code of French Military is on Sale

08 Dec
2023


[French government][Military][Source code] Air force software that track aircrafts

[redacted], 6 hours ago in [Other] - everything else

Posted 6 hours ago

Hello,
Short story : I've opened an auction here [redacted] ; but, after few people are negociating in private message, server has been shutdown.
As the attack was expansive, I've to get a ROI.
So, I'm selling exploited data, source codes, documentations, dumps, here.
As I have to consider that french military services are reading me, and as Sun Tzu suggest, I'm offering a golden path to my adversary : All of these sells can buy buyed exclusivly to stop the sell.
I'm also considering to sell 0days and a write up of the attack at the end as an auction.
I'll have to sell sources codes and data from french military services.
I'll release them 1 by 1.

Rules for each of these sells are the sames :
- If you're not ready to pay, it's useless to contact me in DM
- After the transaction, reputation boost is much appreciated
- Follow me to see upcoming releases
- **Price is 700 XMR, sources delivered will start the 2023-12-15**
- **You can buy exclusivly (stopping the sell) for 4000 XMR before the 2023-12-15**

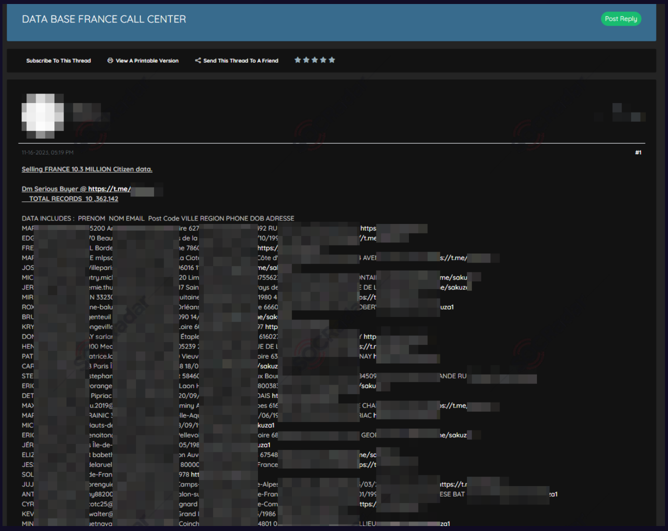
Screenshot of the forum post - French Military Source Code Sale

In a hacker forum monitored by SOCRadar, a new alleged source code sale is detected for French Military. The seller claims to have obtained the code through an exploit and is offering it for sale, along with other sensitive data and documentation.

Data of a French Call Center are on Sale

16 Nov
2023

A new alleged data sale involving a French call center has been detected in a hacker forum monitored by SOCRadar. The data, containing the personal information of over 10.3 million individuals, includes names, email addresses, phone numbers, dates of birth, addresses, and other sensitive details.


DATA BASE FRANCE CALL CENTER

11-16-2023, 05:19 PM #1

Selling FRANCE 10.3 MILLION Citizen data.

Dm Serious Buyer @ https://t.me/[redacted]
TOTAL RECORDS 10 ,362,142

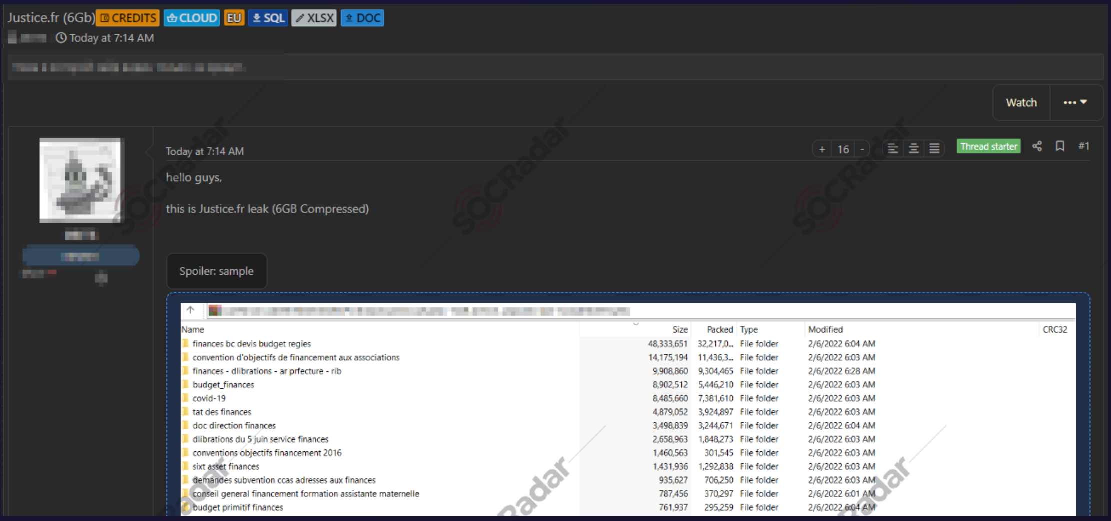
DATA INCLUDES : PRENOM NOM EMAIL Post Code VILLE REGION PHONE DOB ADRESSE

[redacted]

Screenshot of the forum post - French Call Center Database Sale

26 May
2023

French Ministry of Justice Database Compromised



Justice.fr (6Gb) CREDITS CLOUD EU SQL XLSX DOC

[redacted] Today at 7:14 AM

[redacted]

Today at 7:14 AM

hello guys,

this is Justice.fr leak (6GB Compressed)

[redacted]

Name	Size	Packed	Type	Modified	CRC32
finances bc devis budget regies	48,333,651	32,217,0...	File folder	2/6/2022 6:04 AM	
convention d'objectifs de financement aux associations	14,175,194	11,436,3...	File folder	2/6/2022 6:03 AM	
finances - dlibrations - ar prfecture - rib	9,908,860	9,304,465	File folder	2/6/2022 6:28 AM	
budget_finances	8,902,512	5,446,210	File folder	2/6/2022 6:03 AM	
covid-19	8,485,660	7,381,610	File folder	2/6/2022 6:03 AM	
tat des finances	4,879,052	3,924,897	File folder	2/6/2022 6:03 AM	
doc direction finances	3,498,839	3,244,671	File folder	2/6/2022 6:04 AM	
dlibrations du 5 juin service finances	2,658,963	1,848,273	File folder	2/6/2022 6:03 AM	
conventions objectifs financement 2016	1,460,563	301,545	File folder	2/6/2022 6:03 AM	
sixt asset finances	1,431,936	1,292,838	File folder	2/6/2022 6:03 AM	
demandes subvention ccas adresses aux finances	935,627	706,250	File folder	2/6/2022 6:03 AM	
conseil general financement formation assistante maternelle	787,456	370,297	File folder	2/6/2022 6:01 AM	
budget primitif finances	761,937	295,259	File folder	2/6/2022 6:04 AM	

Screenshot of the forum post - French Call Center Database Sale

In a hacker forum monitored by SOCRadar, a new alleged database leak is detected for French Ministry of Justice. The leaked database likely contains sensitive personal and legal information, posing a significant risk to individuals and the French government.

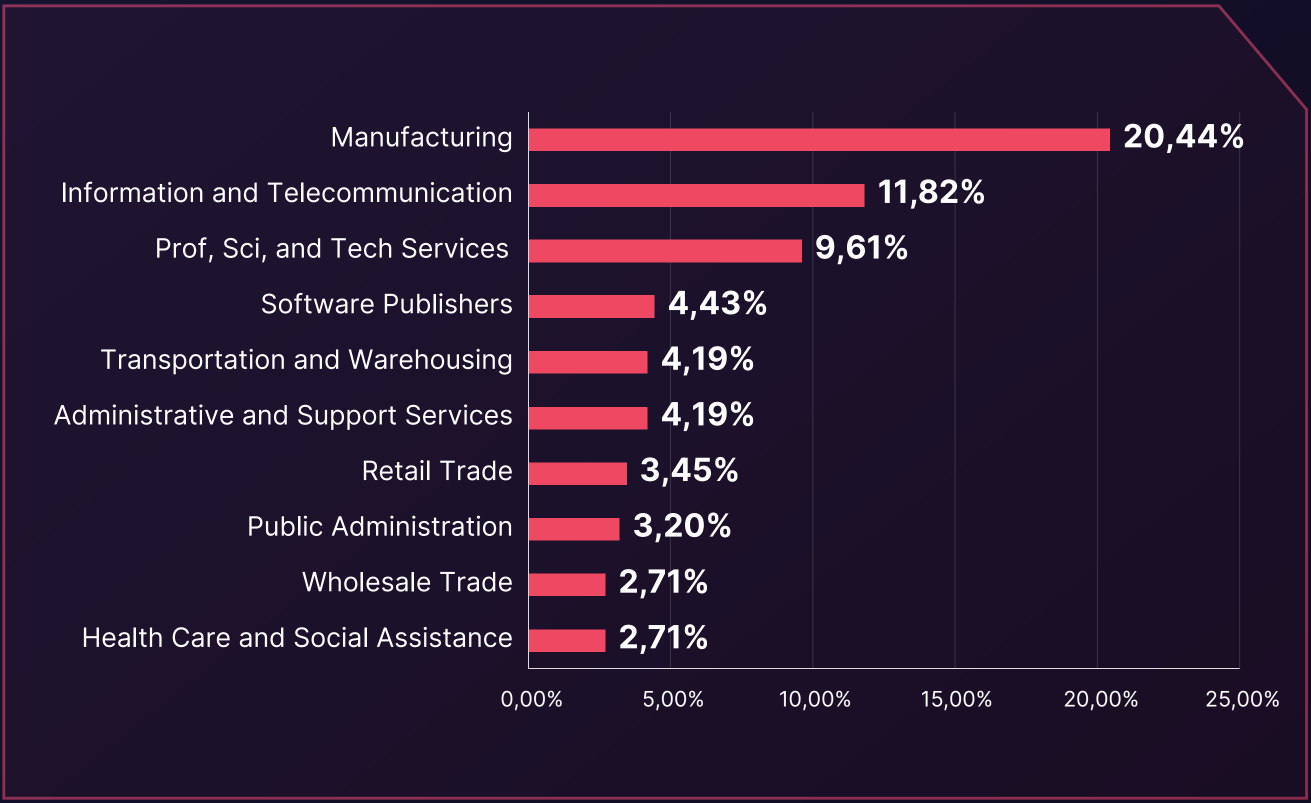
Ransomware Attacks Targeting France

Ransomware attacks represent significant threats to organizations, often resulting in dire consequences such as extensive data loss and the exposure of sensitive information. SOCRadar's surveillance has identified 324 instances of ransomware victim notifications attributable to various ransomware threat actors and/or groups.

Of the 324 ransomware attacks referenced, France emerged as the primary target in 157 cases. The nation also featured among the most affected countries in the remaining 167 global incidents.

Manufacturing emerges as the most prominently affected sector among the targeted industries, representing 20.44% of the identified ransomware attacks during this period. Following this, the Information and Telecommunication industry accounted for 11.82% of the attacks, while the Professional, Scientific, and Technical Services industry experienced 9.61% of the ransomware incidents.

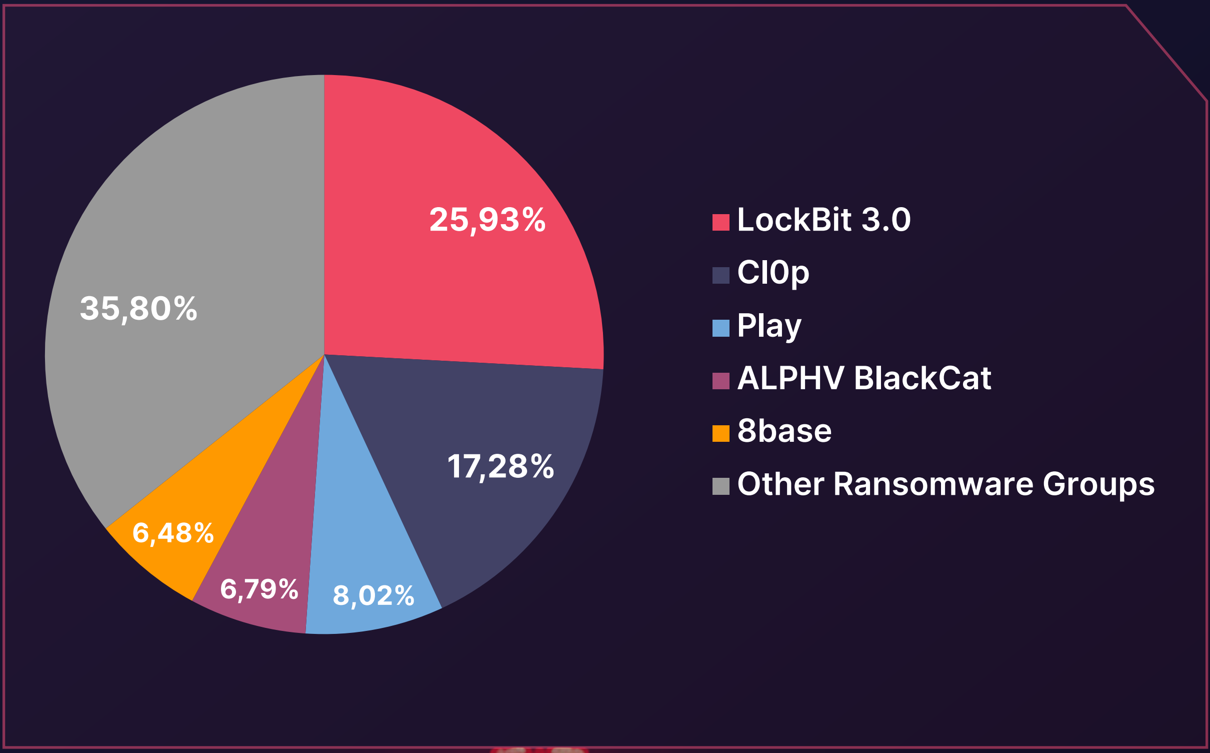
Distribution of Ransomware Attacks by Industry

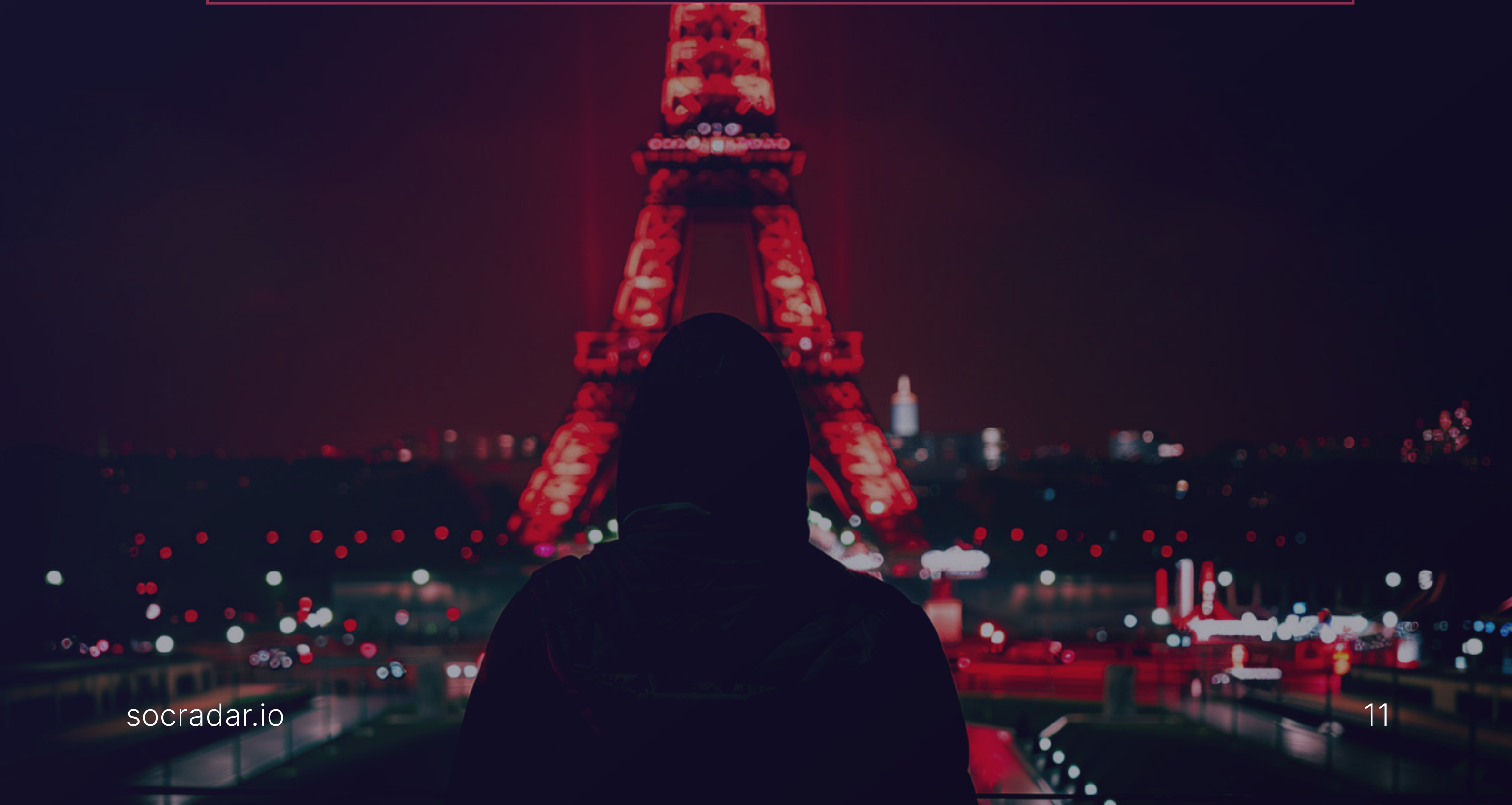


Top Ransomware Groups Targeting France

When examining the top ransomware groups targeting France, **LockBit 3.0** emerges as the most prolific threat, accounting for 25.93% of the attacks. Following closely, **Cl0p** represents 17.28% of the ransomware incidents, while **Play** and **ALPHV BlackCat** contribute 8.02% and 6.79% respectively. Additionally, **8base** accounted for 6.48% of the ransomware attacks. The remaining 35.80% is attributed to various other ransomware groups.

Top Ransomware Groups Targeting Targeting France

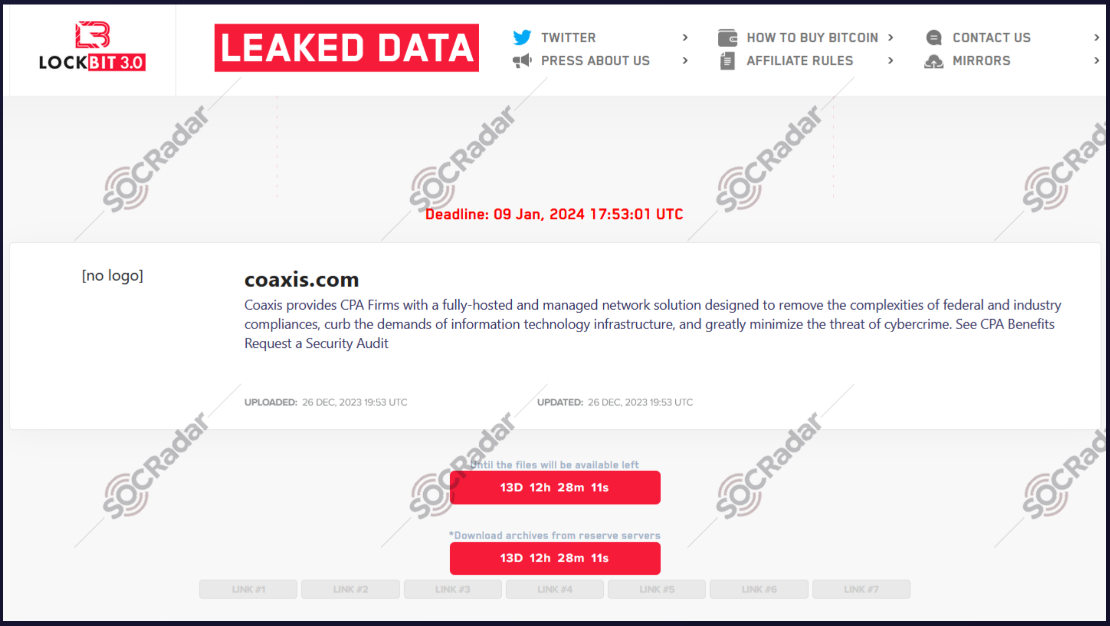




Recent Ransomware Attacks Targeting French Entities

The New Ransomware Victim of Lockbit 3.0: Coaxis

26 Dec
2023



Deadline: 09 Jan, 2024 17:53:01 UTC

[no logo]

coaxis.com

Coaxis provides CPA Firms with a fully-hosted and managed network solution designed to remove the complexities of federal and industry compliances, curb the demands of information technology infrastructure, and greatly minimize the threat of cybercrime. See CPA Benefits Request a Security Audit

UPLOADED: 26 DEC, 2023 19:53 UTC

UPDATED: 26 DEC, 2023 19:53 UTC

Until the files will be available left

13D 12h 28m 11s

*Download archives from reserve servers

13D 12h 28m 11s

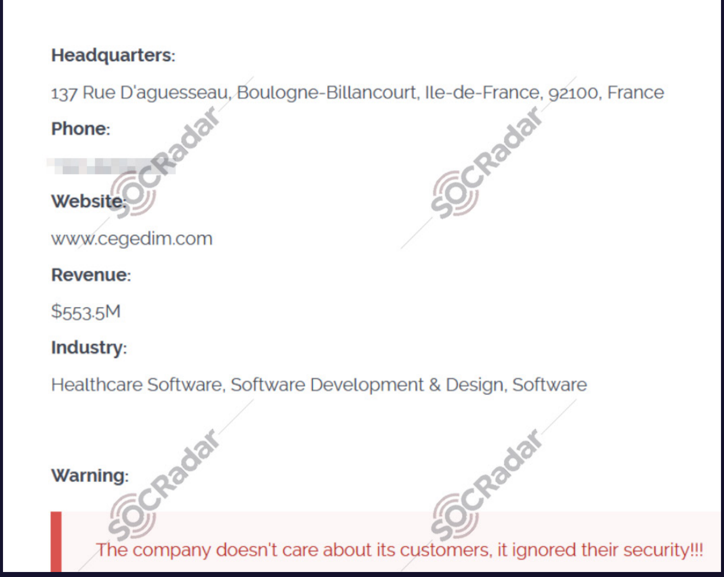
Screenshot from Lockbit 3.0 ransomware group's website

In the Lockbit 3.0 ransomware group website monitored by SOCRadar, a new ransomware victim was allegedly announced as Coaxis, a provider of network solutions for CPA firms. The ransomware group has set a deadline of January 9, 2024, for Coaxis to pay the ransom, indicating the urgency of the situation.

The New Ransomware Victim of Cl0p: Cegedim

17 Jun
2023

In the Cl0p ransomware group website monitored by SOCRadar, a new ransomware victim allegedly announced as Cegedim, a healthcare software company. The ransomware group has published a ransom demand and threatens to release stolen data if the ransom is not paid.



Headquarters:

137 Rue D'aguesseau, Boulogne-Billancourt, Ile-de-France, 92100, France

Phone:

[redacted]

Website:

www.cegedim.com

Revenue:

$553.5M

Industry:

Healthcare Software, Software Development & Design, Software

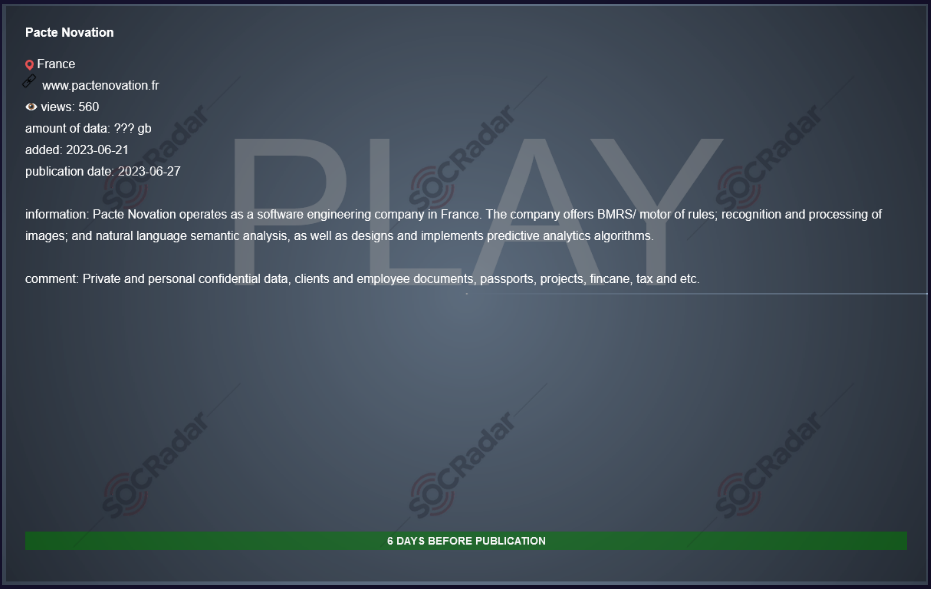
Warning:

The company doesn't care about its customers, it ignored their security!!!

Screenshot from Cl0p ransomware group's website

The New Ransomware Victim of Play: Pacte Novation

21 Jun
2023



Pacte Novation

France
www.pactenovation.fr
views: 560
amount of data: ??? gb
added: 2023-06-21
publication date: 2023-06-27

information: Pacte Novation operates as a software engineering company in France. The company offers BMRS/ motor of rules; recognition and processing of images; and natural language semantic analysis, as well as designs and implements predictive analytics algorithms.

comment: Private and personal confidential data, clients and employee documents, passports, projects, fincane, tax and etc.

Screenshot from Play ransomware group's website

In the Play ransomware group website monitored by SOCRadar, a new ransomware victim was allegedly announced as Pacte Novation, a software engineering company in France. The attackers claim to have stolen sensitive data, including personal information, client documents, and financial records.

Top Threat Actors Targeting France

Lockbit 3.0 Ransomware Group

Country of Origin: Russia

The most successful RaaS group operating since 2019. The group is continuously evolving and is highly active in deploying models such as double-extortion and initial access broker affiliates.

-Ransomware Group-

Motivation:	Financial Gain
Target Countries:	United States, United Kingdom, Canada, Europe, Thailand, Taiwan
Target Sectors:	Manufacturing, Professional Services, IT, Healthcare, Finance, Education, Legal Services
Attack Type:	Phishing, RDP and VPN access Exploitation, Ransomware, Data Exfiltration, Double-extortion

-TTPs-

Exploit Public-Facing Application:	T1190
Remote Desktop Protocol:	T1021.001
Data Encrypted for Impact:	T1486

LockBit 3.0, a successor to LockBit and LockBit 2.0, operates as a Ransomware-as-a-Service (RaaS) group. Since January 2020, LockBit has shifted to an affiliate-based model, employing various tactics to target businesses and critical infrastructure organizations. They are known for employing strategies like double extortion and initial access broker affiliates, as well as recruiting insiders and hosting hacker recruitment contests. With over 1,500 victim announcements on the SOCRadar platform, LockBit emerged as the most active ransomware group in 2022 following Conti's shutdown. As of the first quarter of 2023, they remain the most prolific group, boasting over 300 announced victims.

For more detailed information about the Lockbit 3.0 Ransomware Group, you can visit our blog post.

Cl0p Ransomware Group

Country of Origin: Russia

A Ransomware group that has been active since 2019 and currently brings up its name by exploiting zero-day vulnerabilities that existed in GoAnyWhere MFT and MOVEit MFT software.

-Ransomware Group-

Motivation:	Financial Gain
Target Countries:	The US, Canada, The UK, Australia, Colombia, Sweden, Germany, India, Mexico, Turkey
Target Sectors:	IT, Healthcare, Finance, Professional Services, Retail, Media, Telecommunication
Attack Type:	Spearphishing, Zero-Day Exploitation, Compromised RDP, Ransomware, Data exfiltration, Double-extortion

-TTPs-

Exploit Public-Facing Application:	T1190
Exploitation for Privilege Escalation:	T1068
Exfiltration Over C2 Channel:	T1041

Cl0p is a cybercriminal entity recognized for its sophisticated extortion tactics and widespread dissemination of malware across the globe. The word “clop” comes from the Russian word “klop,” which means “bed bug,” a Cimex-like insect that feeds on human blood at night (mosquito). A distinguishing feature of Cl0p is the string “Don’t Worry C|0P” found in the ransom notes.

With a track record of extorting over $500 million in ransom payments, the group focuses on major organizations on a global scale. Gaining infamy in 2019, Cl0p ransomware group has executed notable attacks, employing extensive phishing initiatives and advanced malware to breach networks and coerce ransom payments, leveraging the threat of data exposure if demands remain unmet.

For more detailed information about the Cl0p Ransomware Group, you can visit our blog post.

Play Ransomware Group

Play Ransomware

Country of Origin: Unknown

Play Ransomware (PlayCrypt) is a ransomware group first observed in June 2022. The group commonly targets organizations based in Latin America but mainly focuses on Brazil.

-Ransomware Group-

Motivation:	Financial Gain
Target Countries:	Latin America, India, Hungary, Spain, Netherlands, United States
Target Sectors:	Manufacturing, Education, Real Estate, Technology, Transportation, Healthcare
Attack Type:	Compromised Valid Accounts, LOLBins, Ransomware, Data Exfiltration

-TTPs-

Process Injection:	T1055
Input Capture:	T1068
Proxy:	T1090

Play Ransomware is a ransomware group notorious for their advanced tactics and the use of intermittent encryption, a method that allows them to partially encrypt files and evade detection. Initially observed in 2022, they target exposed RDP servers and exploit vulnerabilities in FortiOS to gain network access. Their operations include double extortion, where they threaten to leak stolen data if ransoms are not paid. The group has targeted various sectors, including IT companies, banks, and governmental organizations.

For more detailed information about the Play Ransomware Group, you can visit our blog post.

ALPHV Blackcat Ransomware Group

BlackCat Ransomware

Country of Origin: Russia

BlackCat, or ALPHV, is a ransomware group known for being the pioneer to use Rust and the group first announced its RaaS affiliate program in a dark web forum in December 2021.

-Ransomware Group-

Motivation:	Financial Gain
Target Countries:	United States, United Kingdom, Canada, Germany, Australia, France, Italy, Spain
Target Sectors:	Professional Services, Manufacturing, Healthcare, Finance, Information Technology
Attack Type:	Spearphishing, Stolen Credentials, RaaS, Ransomware, Triple-Extortion

-TTPs-

User Execution: Malicious File:	T1204.002
Defacement:	T1491
Data Encrypted for Impact:	T1486

BlackCat, or ALPHV, is a ransomware group known for being the first to use Rust -a cross-platform language programming language that allows for easy malware customization for different operating systems, such as Windows and Linux- successfully. The group has been able to evade detection and successfully encrypt their victims' files by using Rust, which allows them to target multiple operating systems and bypass security controls that are not designed to analyze malware written in Rust.

For more detailed information about the ALPHV BlackCat Ransomware Group, you can visit our blog post.

8base Ransomware Group

8Base

Country of Origin: Unknown

8Base is a ransomware group active since April 2022, targeting small and medium-sized businesses (SMBs) across various sectors, including business services, finance, manufacturing, and IT.

-Ransomware Group-

Motivation:	Financial Gain
Target Countries:	United States, Brazil, UK, Australia, Germany, Canada, Spain, Italy, Belgium
Target Sectors:	Professional Services, Manufacturing, Construction, Finance, Healthcare, Transportation
Attack Type:	RaaS, Ransomware, Double Extortion

-TTPs-

Phishing: Spearphishing Attachment:	T1566.001
OS Credential Dumping:	T1003
Exfiltration Over C2 Channel:	T1041

8base is a ransomware group that has been active since April 2022. Despite its relatively recent emergence, the group has rapidly gained notoriety due to its aggressive tactics and the significant number of victims it has claimed. The group primarily targets small and medium-sized businesses (SMBs) across various sectors, including business services, finance, manufacturing, and information technology.

The group's identity, methods, and motivations largely remain a mystery. However, based on its leak site and public accounts, along with the group's communications, researchers think the group's verbal style is quite similar to that of RansomHouse, a group that typically purchases already compromised data or works with data leak sites to extort victims. This has led to speculation that 8Base may be an offshoot of RansomHouse.

For more detailed information about the 8base Ransomware Group, you can visit our blog post.

Stealer Log Statistics
Top Domains in France

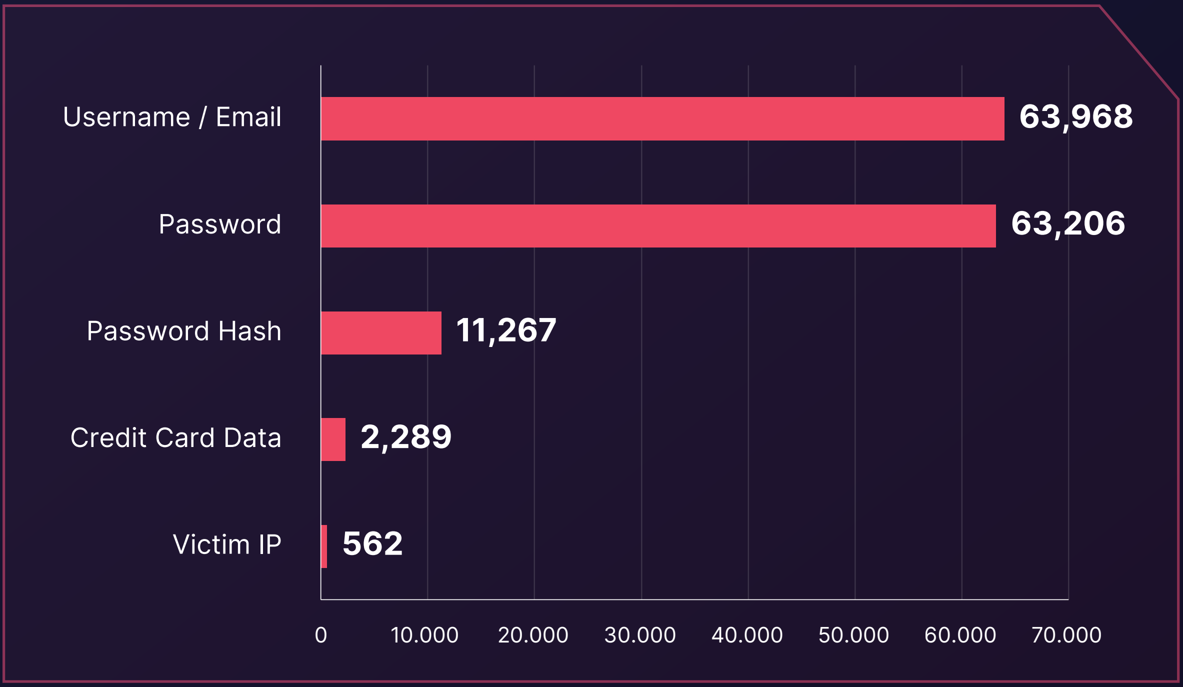
Throughout 2023, thousands of users' user IDs/email addresses, passwords, credit card data, password hashes, and victim IP address information were compromised via Stealer Logs from the computers of users with accounts or access to some of the highest traffic domains in France.

The table below lists the domains associated with France with the highest traffic.

orange.fr
amazon.fr
lefigaro.fr
leboncoin.fr
lemonde.fr
ouest-france.fr
bfmtv.fr
actu.fr
leparisien.fr
lequipe.fr

The graph below showcases the distribution of the compromised user data obtained through Stealer Logs across the highest-traffic domains associated with France.

Stealer Logs - Compromised Data



The data reveals significant dissemination of compromised information, including **63,968** passwords, **63,206** usernames/emails, **11,267** password hashes, **2,289** credit card data entries, and **562** compromised victim IPs, each representing significant instances of compromise.

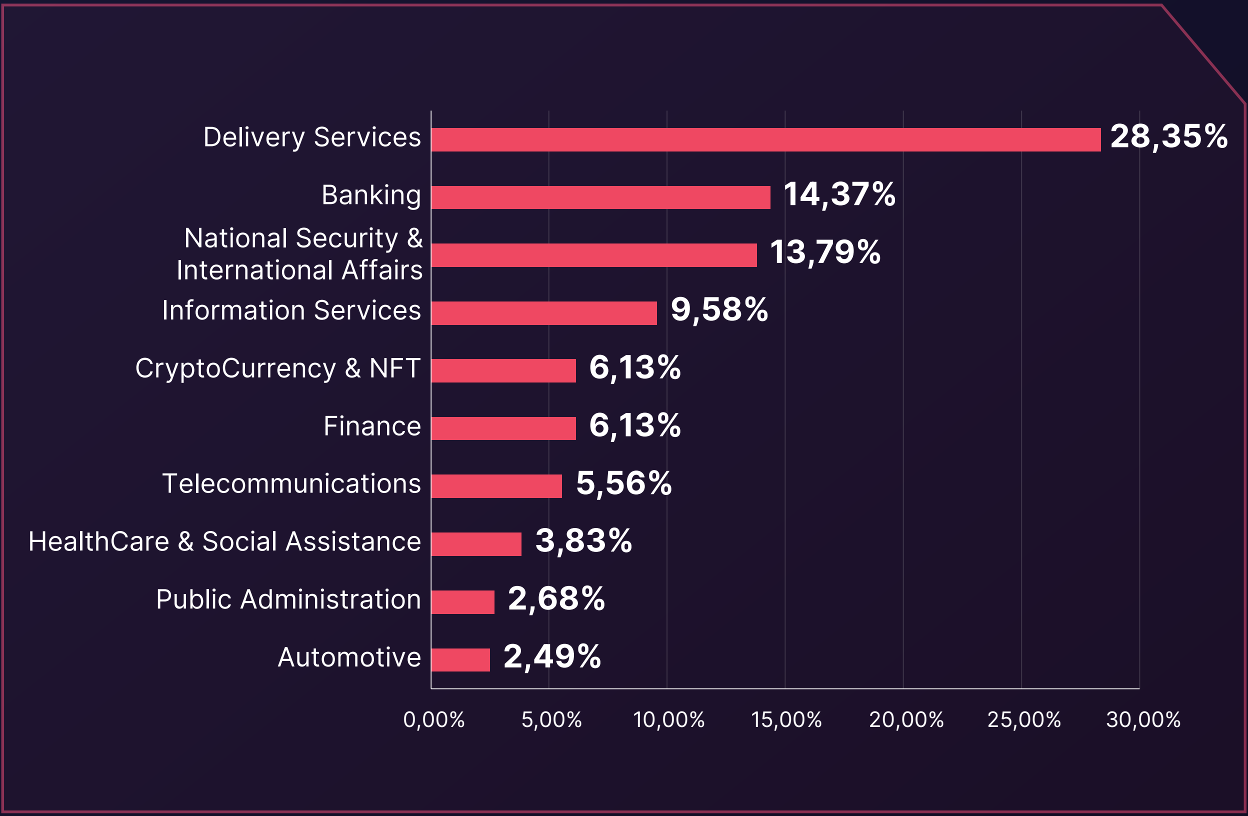
These discoveries emphasize the gravity of data compromises impacting users in France's digital sphere, emphasizing the urgent necessity for robust cybersecurity protocols to alleviate such risks efficiently.

Phishing Threats Targeting France

Phishing is an effective method to initially breach an organization's infrastructure by deceiving individuals into divulging sensitive credentials on fraudulent websites.

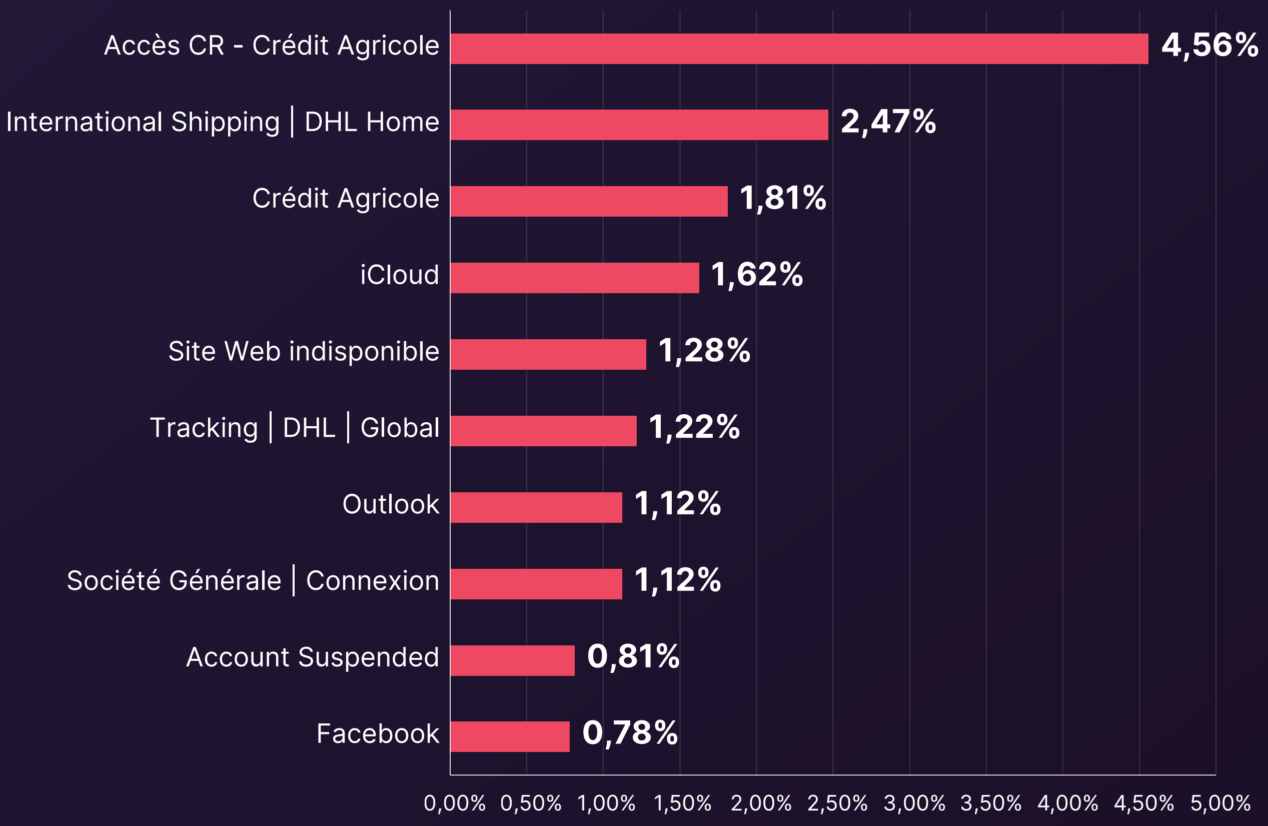
Typically, phishing attacks are coupled with social engineering tactics to acquire such credentials. Over the past year, French enterprises have encountered **3,203 distinct instances of phishing attacks**, primarily targeting the **Delivery Services** industry.

Phishing Attacks - Distribution by Industry



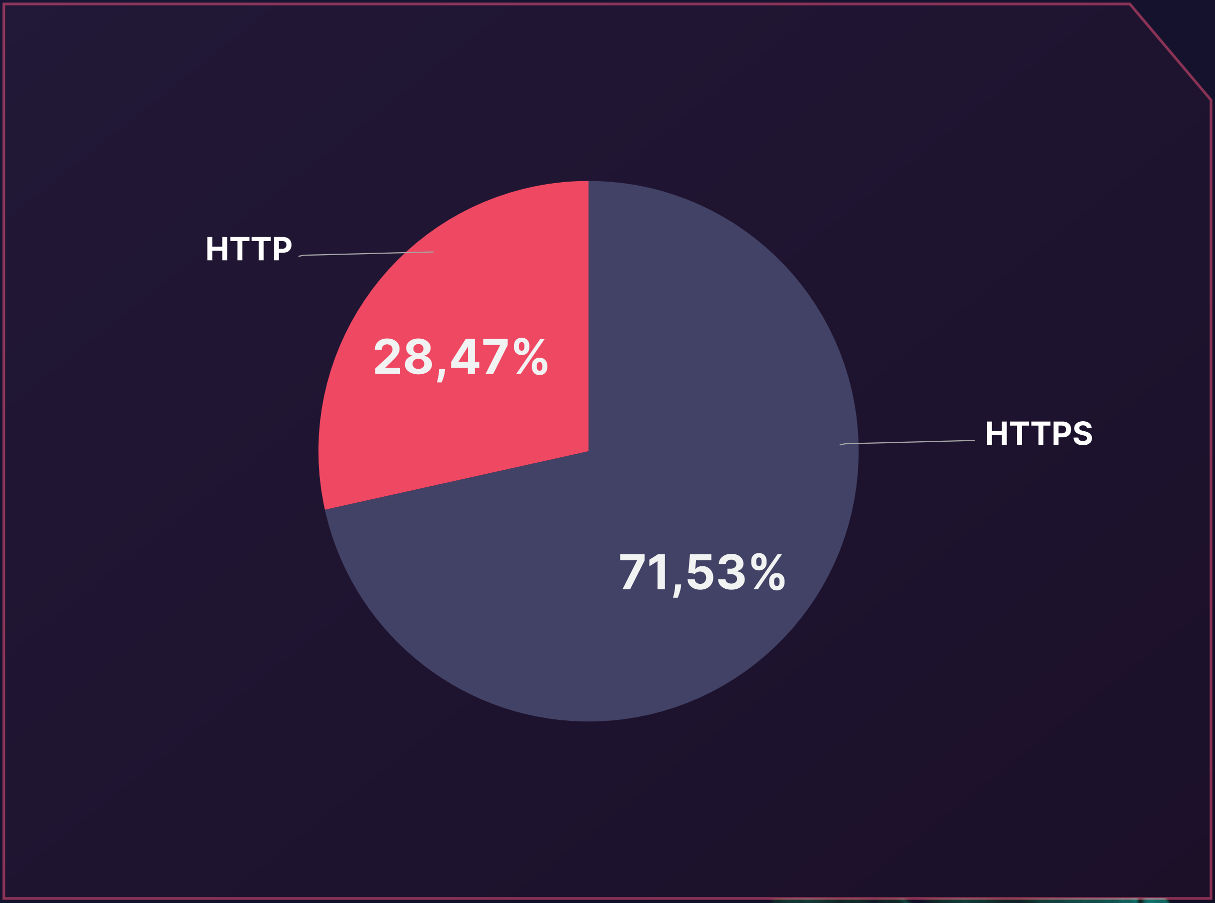
The graph below illustrates the distribution of Page Titles used by threat actors for phishing attacks. Notably, the data reveals a predominant usage of the **Accès CR - Crédit Agricole** page title.

Phishing Attacks - Distribution by Phishing Page Title



When closely examining the SSL/TLS protocols of domains prepared for phishing attacks by threat actors, we observe an increasing trend in the usage of HTTPS compared to the past.

Phishing Attacks- Distribution by SSL/TLS Protocol



DDoS Attack Statistics

France experienced a dynamic DDoS threat landscape marked by considerable cyber activity in 2023.

- The most extensive multivector DDoS attack recorded encompassed **25 vectors**, featuring prevalent techniques such as **TCP ACK** and **DNS Amplification** attacks.
- The maximum bandwidth observed during a DDoS attack reached **1,005 Gbps** (peak aggregate bandwidth in one minute), indicating the severe capacity of these cyber threats.
- The highest recorded throughput during these incidents was **452 Mpps** (peak aggregate throughput in one minute), underscoring the intense rate at which data packets were sent.
- On average, each DDoS attack lasted for **28 minutes**, indicating a strategy focused on short but effective service disruptions.
- A total of **202,397** DDoS attacks were recorded throughout the year, illustrating a high frequency of cyber-attacks aimed at targets in France.

Attack Vector	Number of Attacks in 2023
TCP ACK	43,987
DNS Amp	42,006
TCP RST	20,957
ICMP	19,022
TCP SYN/ACK Amp	18,611

The ongoing evolution of DDoS tactics underscores the importance of implementing stringent monitoring and resilient defense mechanisms to safeguard essential infrastructures and ensure uninterrupted service delivery. Enhance your DDoS defense with SOCRadar's DoS Resilience module, a sophisticated tool designed to assess and fortify your infrastructure's resilience to DoS attacks.

Lessons Learned: Key Insights and Strategic Recommendations

Upon examining the cybersecurity threats facing organizations in France, several critical lessons and recommendations have emerged. These insights, enhanced by SOCRadar's capabilities, provide a strategic roadmap to bolster cyber resilience and safeguard operational integrity. Here are the key takeaways from our analysis:

Vigilance in an Evolving Cyber Threat Landscape

The dynamic nature of the cyber threat landscape, marked by an increase in dark web activities and ransomware incidents related to France, demands constant vigilance. Organizations must keep pace with these changes by adapting their security strategies. By adopting a proactive approach like SOCRadar’s Extended Threat Intelligence solution, organizations can gain real-time insights into emerging threats, positioning them to counteract cyber adversaries proactively.

Implementation of Multi-layered Security Measures

Given the broad spectrum of industries targeted by cyber threats, it is essential to implement multi-layered security defenses. SOCRadar supports these efforts with its proactive Threat Intelligence and monitoring services, ensuring comprehensive protection.

Consistent Guard Against Ransomware

The persistent threat posed by ransomware underscores the need for strong defensive and responsive strategies. SOCRadar’s Attack Surface Management capabilities are crucial for businesses to identify potential ransomware threats and to formulate effective countermeasures.

Continuous Employee Education and Training

The ongoing risk of phishing attacks makes continuous education and training for employees imperative. Enhancing their ability to recognize phishing tactics and detection methods is vital. SOCRadar's Digital Risk Protection suite provides comprehensive VIP Protection and Brand Protection services, effectively addressing the challenges posed by identity-based attacks.

Robust Defenses Against Stealer Malware

With France frequently targeted by Stealer malware, strengthening defenses against this malicious software is crucial. SOCRadar's Identity & Access Intelligence module is vital in detecting and mitigating data breach threats, enhancing an organization's security framework.

Strategies Against DDoS Attacks

As DDoS attacks become more complex and voluminous, organizations must prioritize the implementation of robust DDoS mitigation strategies. This involves deploying advanced DDoS protection technologies that can absorb high-volume traffic and mitigate multi-vector attack strategies effectively.

Enhance your DDoS defense with SOCRadar's DoS Resilience module, a sophisticated tool designed to assess and fortify your infrastructure's resilience to DoS attacks. Leveraging state-of-the-art AI and cloud technologies, this module provides a crucial layer of protection for global organizations.

Conclusion

Adopting a proactive and comprehensive cybersecurity approach is crucial for France's organizations. By partnering with advanced solutions like SOCRadar, they can enhance their defenses and effectively navigate the evolving cyber threat landscape.

Building a culture of risk awareness and implementing proactive mitigation strategies fortifies defenses against dynamic threats. Utilizing Cyber Threat Intelligence empowers teams to respond to immediate threats and confidently prepare for future challenges.

Collaboration among cybersecurity professionals, supported by robust CTI frameworks, is essential for safeguarding digital assets and maintaining organizational resilience against cyber threats.

Who is SOCRadar®?

Your Eyes Beyond

SOCRadar provides Extended Threat Intelligence (XTI) that combines: **"Cyber Threat Intelligence, Brand Protection, External Attack Surface Management, and Dark Web Radar Services."** SOCRadar provides the actionable and timely intelligence context you need to manage the risks in the transformation era.

Trusted by **21.000+ companies** in **150+ countries**

Dark Web Monitoring: SOCRadar's fusion of its unique Dark Web recon technology with the human analyst eye further provides in-depth insights into financially-targeted APT groups and the threat landscape.

Protecting Customers' PII: Scan millions of data points on the surface, deep and Dark Web to accurately identify the leakage of your customers' Personally Identifiable Information (PII) in compliance with regulations.

Credit Card Monitoring: Enhance your fraud detection mechanisms with automation speed by identifying stolen credit card data on popular global black markets, carding forums, social channels, and chatters.

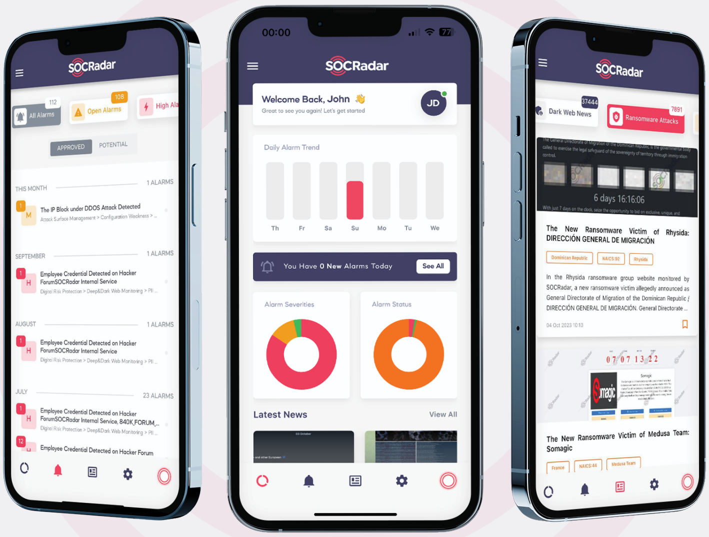
360-Degree Visibility: Achieve digital resilience by maintaining internet-facing digital asset inventory. Significantly accelerate this process by automated discovery, mapping, and continuous asset monitoring.

GET ACCESS FOR FREE

MEET THE NEW MOBILE APP

Access threat intelligence, act on-the-go, and be instantly notified of new threats.View alerts, breaking Dark Web news, and new ransomware attacks

Download on the App Store



SOCRadar

112 All Alarms | 108 Open Alarms | High Ala

APPROVED | POTENTIAL

THIS MONTH — 1 ALARMS

1 M The IP Block under DDOS Attack Detected
Attack Surface Management > Configuration Weakness > ...

SEPTEMBER — 1 ALARMS

1 H Employee Credential Detected on Hacker ForumSOCRadar Internal Service
Digital Risk Protection > Deep&Dark Web Monitoring > PII ...

AUGUST — 1 ALARMS

1 H Employee Credential Detected on Hacker ForumSOCRadar Internal Service
Digital Risk Protection > Deep&Dark Web Monitoring > PII ...

JULY — 23 ALARMS

1 H Employee Credential Detected on Hacker ForumSOCRadar Internal Service, 840K FORUM_...
Digital Risk Protection > Deep&Dark Web Monitoring > PII ...

12 Employee Credential Detected on Hacker Forum

00:00

SOCRadar

Welcome Back, John 👋
Great to see you again! Let's get started

JD

Daily Alarm Trend

Th Fr Sa Su Mo Tu We

You Have 0 New Alarms Today — See All

Alarm Severities | Alarm Status

Latest News — View All

SOCRadar

37444 Dark Web News | 7891 Ransomware Attacks

6 days 16:16:06

The New Ransomware Victim of Rhysida: DIRECCIÓN GENERAL DE MIGRACIÓN

Dominican Republic | NAICS:92 | Rhysida

In the Rhysida ransomware group website monitored by SOCRadar, a new ransomware victim allegedly announced as General Directorate of Migration of the Dominican Republic / DIRECCIÓN GENERAL DE MIGRACIÓN. General Directorate ...

04 Oct 2023 10:13

The New Ransomware Victim of Medusa Team: Somagic

France | NAICS:44 | Medusa Team

GET IT ON Google Play

Gartner Peer Insights™ Customer First

4.8/5 ★★★★★