

## Industry Threat Landscape Report

### Telecommunications

Time Period: 2024/11/17 - 2025/11/17 | Report Date: 2024-11-17



📍 651 N Broad St, Suite 205  
Middletown, DE 19709

📞 +1 (571) 249-4598

✉️ info@socradar.io

[www.socradar.io](http://www.socradar.io)

SOCRadar delivers intelligent digital risk protection platform against sophisticated cyber attacks for organizations of any size. Its portfolio of digital assets and perimeter monitoring platforms hardened with targeted threat intelligence – all automated and supported by a global team of qualified intelligence analysts – provides unparalleled visibility, management, and protection of digital risks. Prioritized, up-to-date, and relevant cyber threat insights empower customers to take action starting from the reconnaissance stage of the cyberattack life cycle.

Gartner  
Peer Insights™



# Agenda

01 Dark Web Threats

---

02 Ransomware Threats

---

03 Top Target Industry

---

04 Phishing Threats

---

05 APT Groups



## 823 Dark Web Threats in last one year.

Most category are Selling and Sharing

SOCRadar CTIA team has monitored the dark web to find trends and essential links.

Throughout the this year,

**Telecommunications** enterprises were bombarded with cyber attacks. Various threat actors have tried to sell and sometimes share the fruits of these successful cyberattacks on dark web hacker forums.

## 537 Dark web Threat Actors

xcxxw

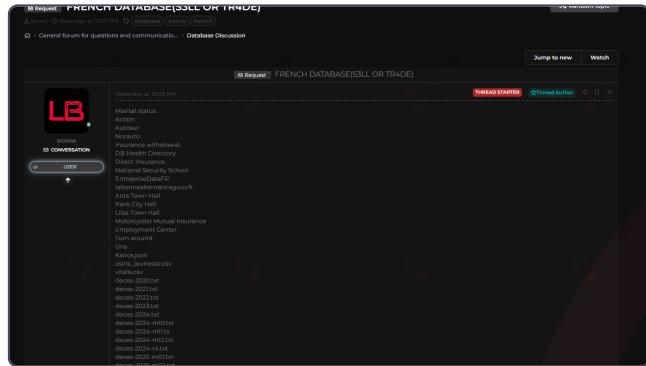
ByteToBreach

user747

ShinyHunters

Good\_bases

# Dark Web Threats



2025-11-14

## The Alleged Data of Various French Companies are on Sale

In a hacker forum monitored by SOCRadar, a new alleged data sale is detected for various French companies. <https://image.socradar.com/screenshots/2025/11/14/ea73791b-7b54-4ffe-9f46-44c917f22d34.png>  
Marital status : Action Autosur Noraauto Insurance wit...

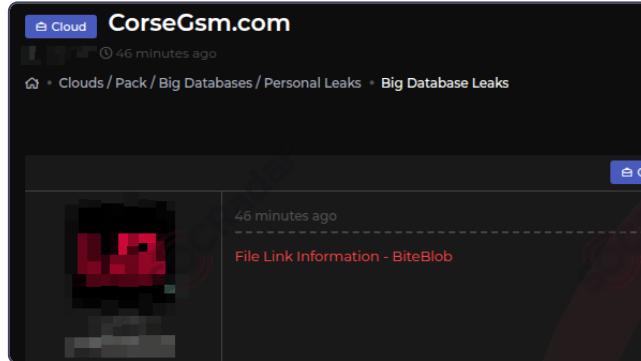


2025-11-14

## The Alleged Data of Eurofiber are on Sale

In a hacker forum monitored by SOCRadar, a new alleged data sale is detected for Eur ofiber. <https://image.socradar.com/screenshots/2025/11/14/17c9d257-a03b-4e6a-b8c6-701454e503eb.png> This is the whole dat abase of EuroFiber GLPI IT System,one of t he bi...

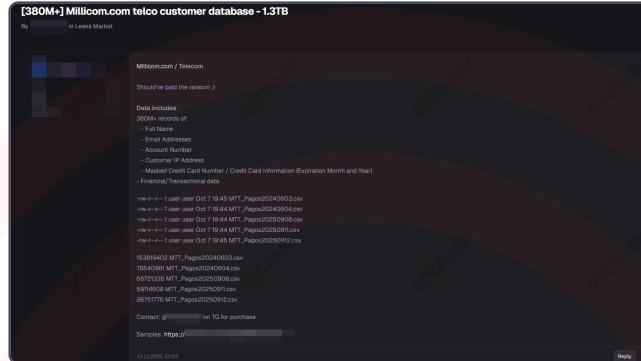
# Dark Web Threats



2025-11-14

## The Alleged Data of Corse GSM ...

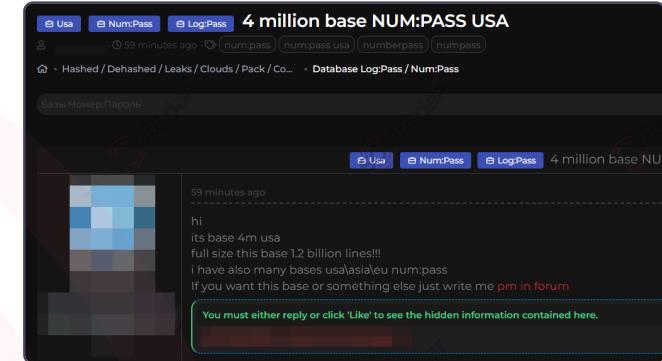
In a hacker forum monitored by SO CRadar, a new alleged data leak is detected for Corse GSM. <https://image.socradar.com/screenshots/2025/11/14/3f224ea8-645a-4d67-b8e8-8977a1078242.png> File Link Information - BiteBlob



2025-11-13

## The Alleged Database of Millic...

In a hacker forum monitored by SO CRadar, a new alleged database sale is detected for Millicom. <https://image.socradar.com/screenshots/2025/11/13/fad95754-a1a3-4665-9475-ba96b558fbfa.png> Millicom.com / Telecom Should've paid the ransom ;) Data includes...



2025-11-13

# The Alleged Phone Number Data ...

In a hacker forum monitored by SO CRadar, a new alleged phone number data leak is detected for the United States. <https://image.socradar.com/screenshots/2025/11/13/d8447716-eedc-4658-9f73-e3cba8ccbd01.png> its base 4m usa full size this base 1.2...

## 129 ransomware attacks

in Telecommunications.

Ransomware attacks are among the most critical cyber attacks an organization can experience. The results can be destructive for an organization and lead to massive data loss and leaks of the victim company's sensitive data.

## 85 Ransomware Gangs

qilin

---

coinbasecartel

---

play

---

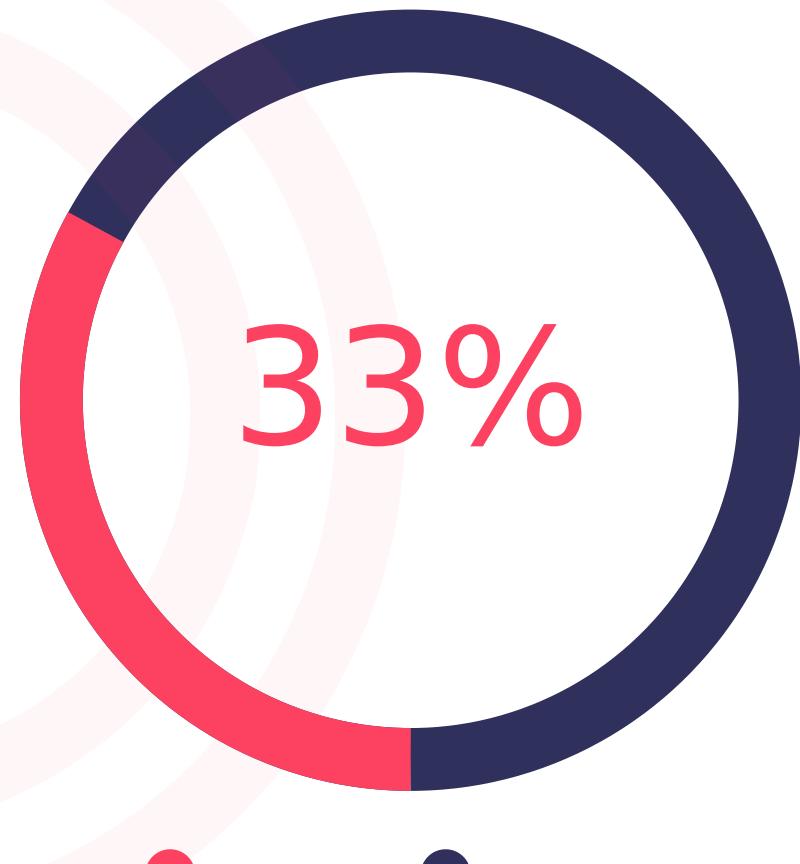
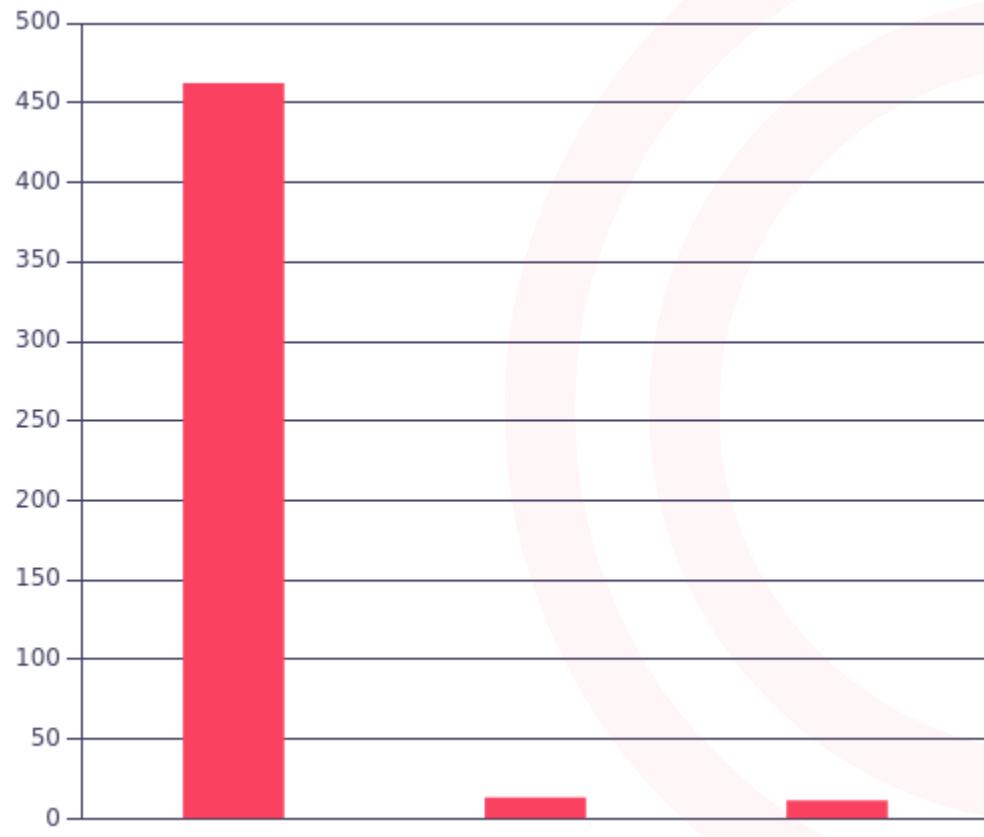
fog

---

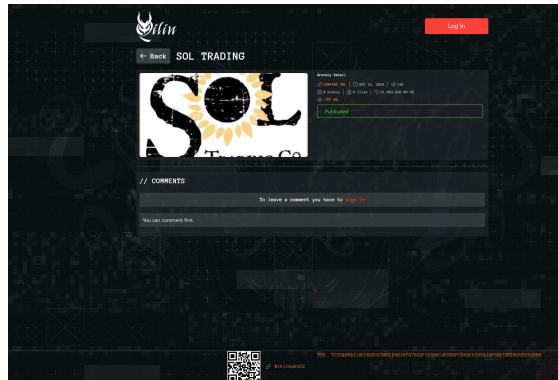
akira

---

# Ransomware Threats



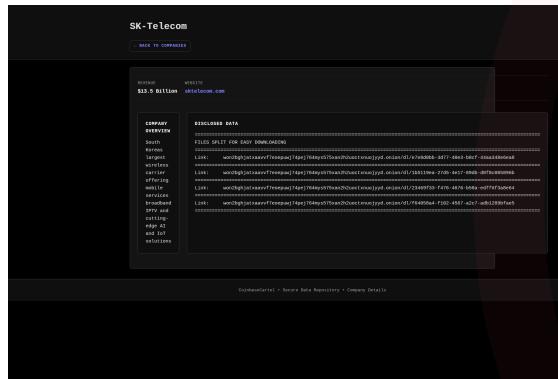
# Ransomware Threats



## The New Ransomware Victim of qilin: Sol Trading

2025-11-14

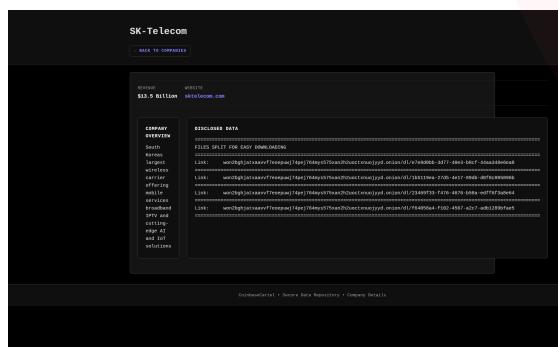
In the qilin ransomware group website monitored by SOCRadar, a new ransomware victim allegedly announced as Sol Trading [N/A](https://image.socradar.com/screenshots/2025/11/14/705e9ddd-20c8-4961-ac18-db8733f952c2.png)



## The New Ransomware Victim of coinbasecartel: SK-Telecom

2025-11-03

In the coinbasecartel ransomware group website monitored by SOCRadar, a new ransomware victim allegedly announced as SK-Telecom [South Korea's largest wireless ca...](https://image.socradar.com/screenshots/2025/11/02/64aa0583-4885-44f8-a7f5-1d8cb1323062.png)



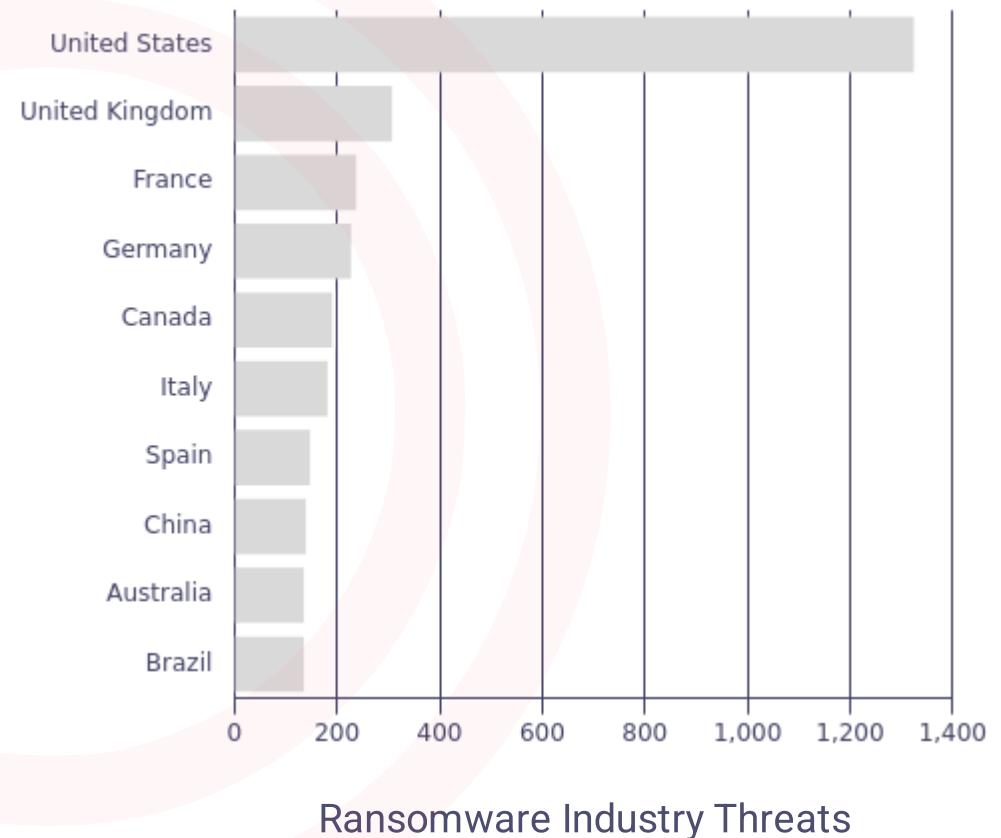
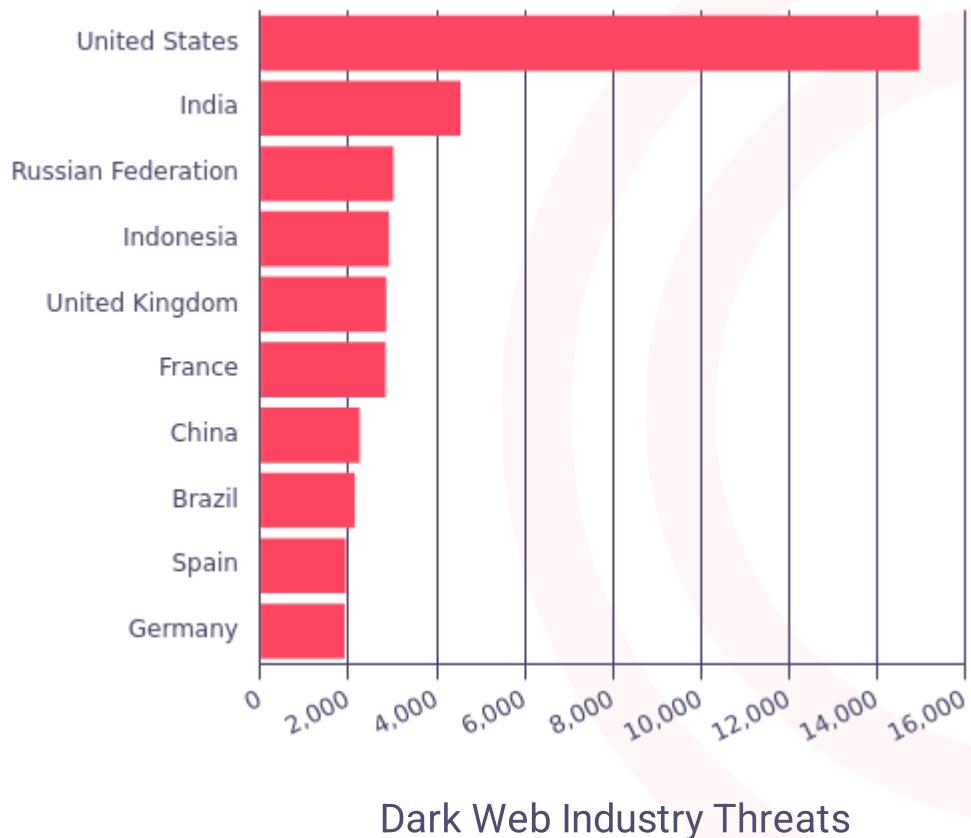
## The New Ransomware Victim of coinbasecartel: SK-Telecom

2025-11-03

In the coinbasecartel ransomware group website monitored by SOCRadar, a new ransomware victim allegedly announced as SK-Telecom [South Korea's largest wireless ca...](https://image.socradar.com/screenshots/2025/11/02/d524469d-bf66-4af2-b932-eb58c93355b6.png)

# Top Target Countries

239 Different industries targeted in Telecommunications



# Phishing Threats



Brand impersonation takes place when a threat actor creates a social account pretending to be your brand. SOCRadar can spot fraudulent and fake domain. Also can spot fake social accounts by monitoring well-known social media platforms so that you can quickly take action to stop possible phishing scams.

Phishing Domain	Sector	Register Date
linqapp[.]com	Telecommunication...	2025-11-15
weeblysite[.]com	Telecommunication...	2025-11-15
weebly[.]com	Telecommunication...	2025-11-15
linqapp[.]com	Telecommunication...	2025-11-14
ukit[.]me	Telecommunication...	2025-11-15

+992 Phishing Threats

11202 phishing  
domains detected in  
**Telecommunications**

# APT Groups



**69** apt groups found in **Telecommunications**

Group Name	Aliases	Country
Mirage	G0135 , G0004 , BackdoorDiplomacy Nickel ...	Egypt  Argentina ...

# Cyber Threat Intelligence for SOC Analysts

As an 'Extension to SOC Teams', CTI4SOC aims to provide you with actionable and contextualized TI with minimized false positives.

A unique assistant to SOC teams with 12 functional modules.



Sign Up for Free CTI4SOC

[Get Free CTI4SOC](#)



Trusted by world's leading organizations

Gartner  
Peer Insights™

