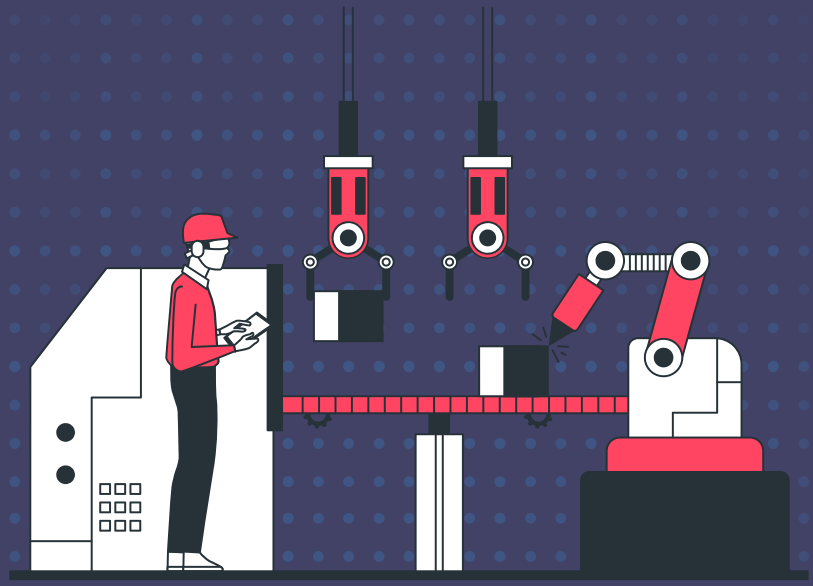
SOCRadar LABS



Industry Threat Landscape Report

Banking

Time Period: 2024/11/15 - 2025/11/15 | Report Date: 2024-11-15

SOCRadar® Your Eyes Beyond

651 N Broad St, Suite 205
Middletown, DE 19709

+1 (571) 249-4598

info@socradar.io

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™

5/5

Agenda

SOCRadar®

01 Dark Web Threats

02 Ransomware Threats

03 Top Target Industry

04 Phishing Threats

05 APT Groups

819 Dark Web Threats

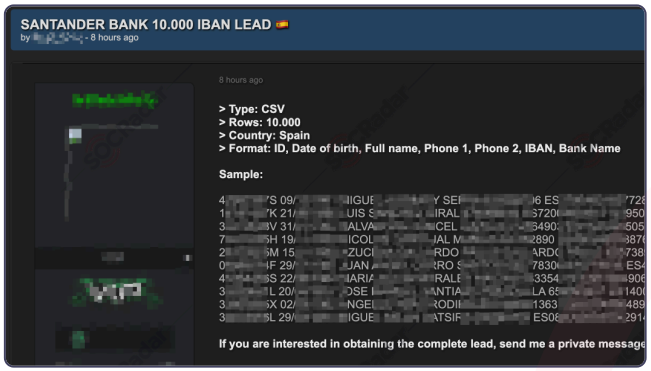
in last one year.

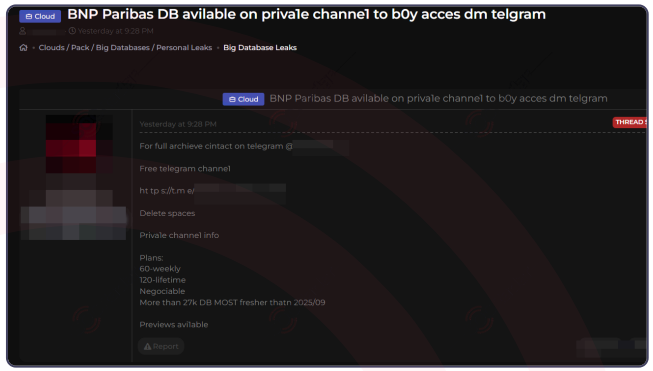
Most category are Selling and Sharing

SOCRadar CTIA team has monitored the dark web to find trends and essential links. Throughout the this year, Banking 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.

594 Dark web Threat Actors

- BreachParty
- Yees0987
- khatun5
- BreachPart
- cashmoneycard





2025-11-08

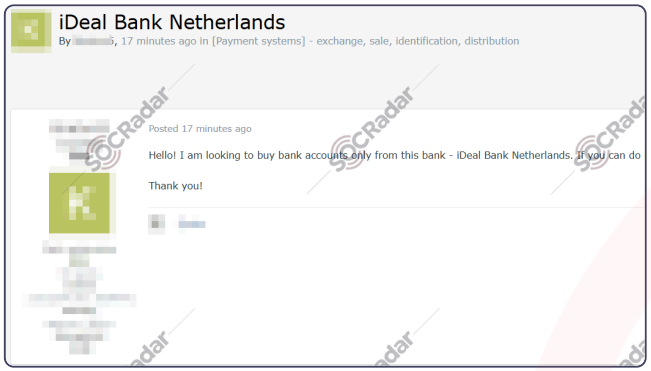
The Alleged Customer Database of Banco Santander is on Sale

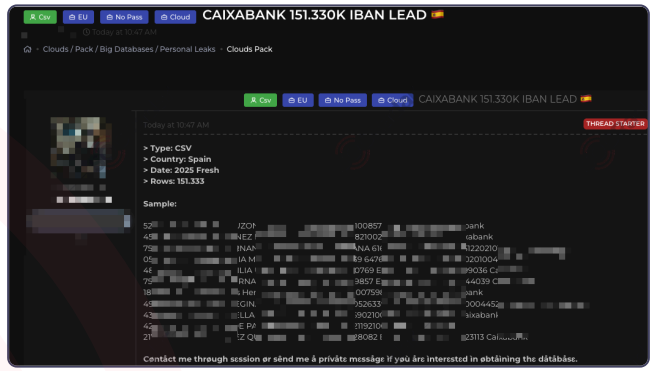
In a hacker forum monitored by SOCRadar, a new alleged database sale is detected for Banco Santander. https://image.socradar.com/screenshots/2025/11/08/eab0edc0-af59-4823-b706-a18b6642088e.png> Type: CSV > Rows: 10.000 > Country: Spain > ...

2025-11-07

The Alleged Database of BNP Paribas is on Sale

In a hacker forum monitored by SOCRadar, a new alleged database sale is detected for BNP Paribas. https://image.socradar.com/screenshots/2025/11/07/53c9e925-673a-4385-8d42-328fcfbca802.pngFor full archieve cintact on telegram @***** Free telegram cha...





2025-11-07

Data Purchasing Announcement i...

In a hacker forum monitored by SOCRadar, a new data purchasing announcement is detected for the French Sports Federation. https://image.socradar.com/screenshots/2025/11/07/edfae4b0-e638-4744-b543-9857d2976d4b.pngHello! I am looking to buy bank accoun...

2025-11-07

Alleged IBAN Lead of Abanca Ba...

In a hacker forum monitored by SOCRadar, a new alleged IBAN lead sale is detected for Abanca Bank. https://image.socradar.com/screenshots/2025/11/07/bcccbe65-8c27-4d85-a94f-4b20e59b8f7b.png> Type: CSV > Date: 2025 Fresh > Country: Spain...

2025-11-07

Alleged IBAN Leada of Caixaban...

In a hacker forum monitored by SOCRadar, a new alleged IBAN lead leak is detected for Caixabank. https://image.socradar.com/screenshots/2025/11/07/f74eb2a9-f277-4ae9-9884-99c06d0279f0.png> Type: CSV > Country: Spain > Date: 2025 Fresh &...

Ransomware Threats

1 ransomware attacks

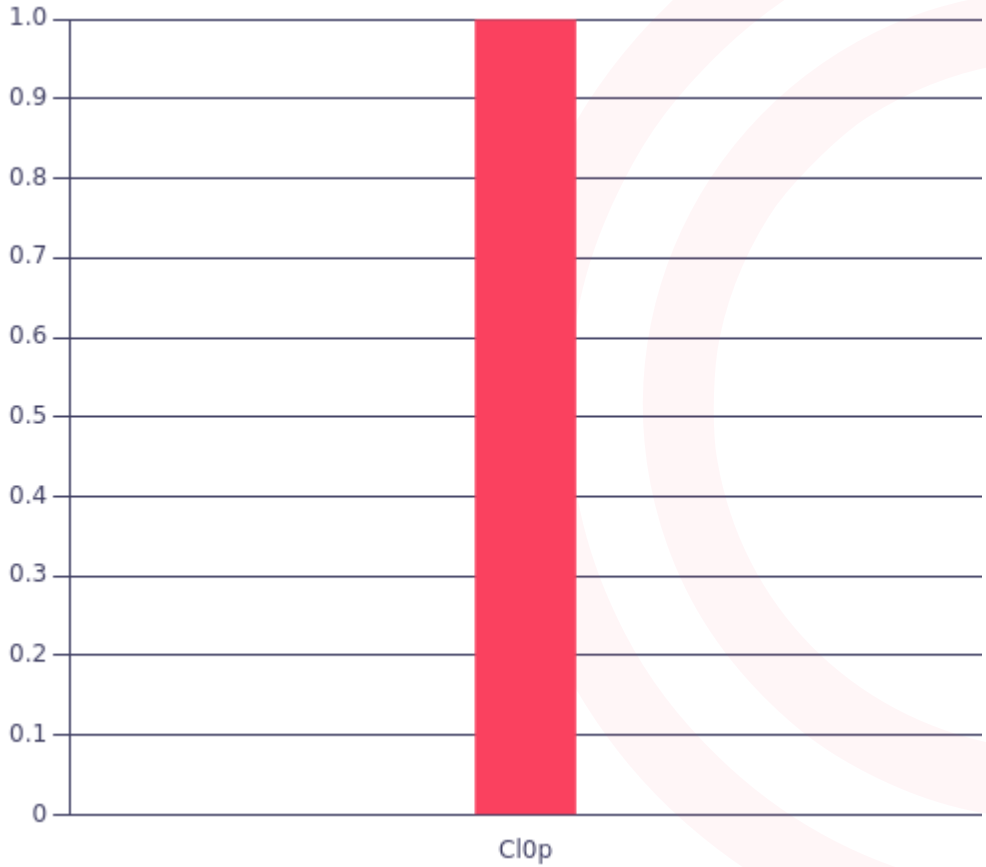
in Banking.

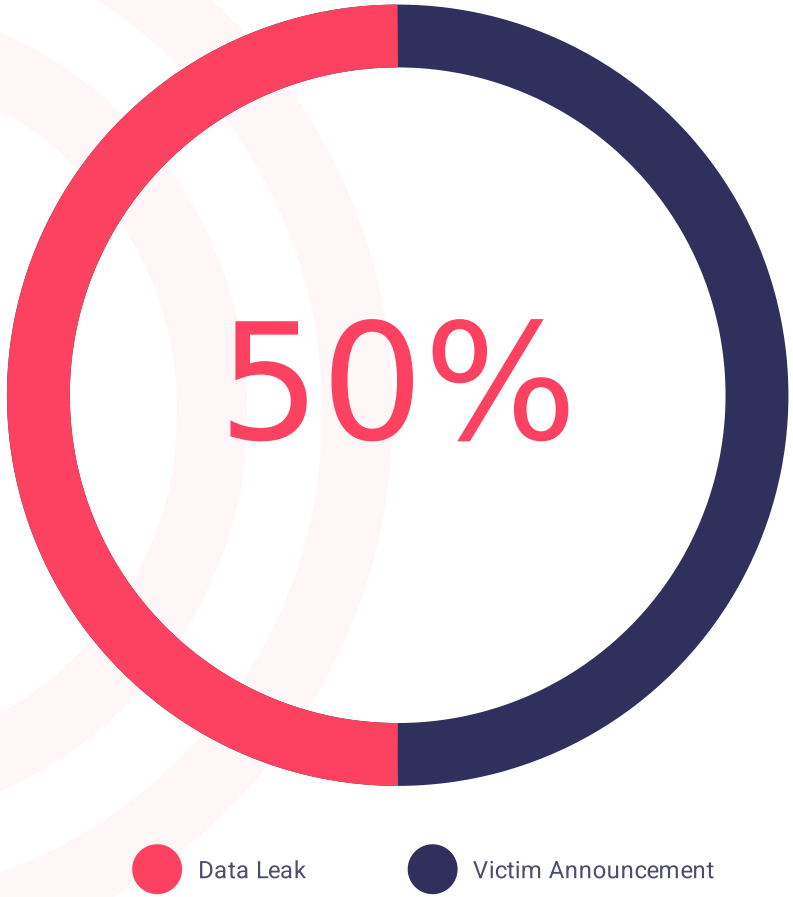
Ransomware attacks are among the most critical cyber attacks an organization can experience. The results can be destructive for an organization and lead to massive data loss and leaks of the victim company's sensitive data.

1 Ransomware Gangs

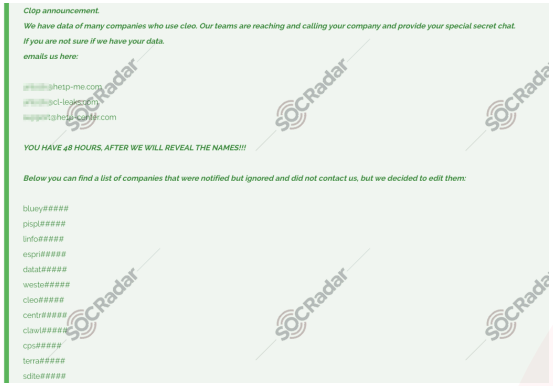
Cl0p

Ransomware Threats





Ransomware Threats



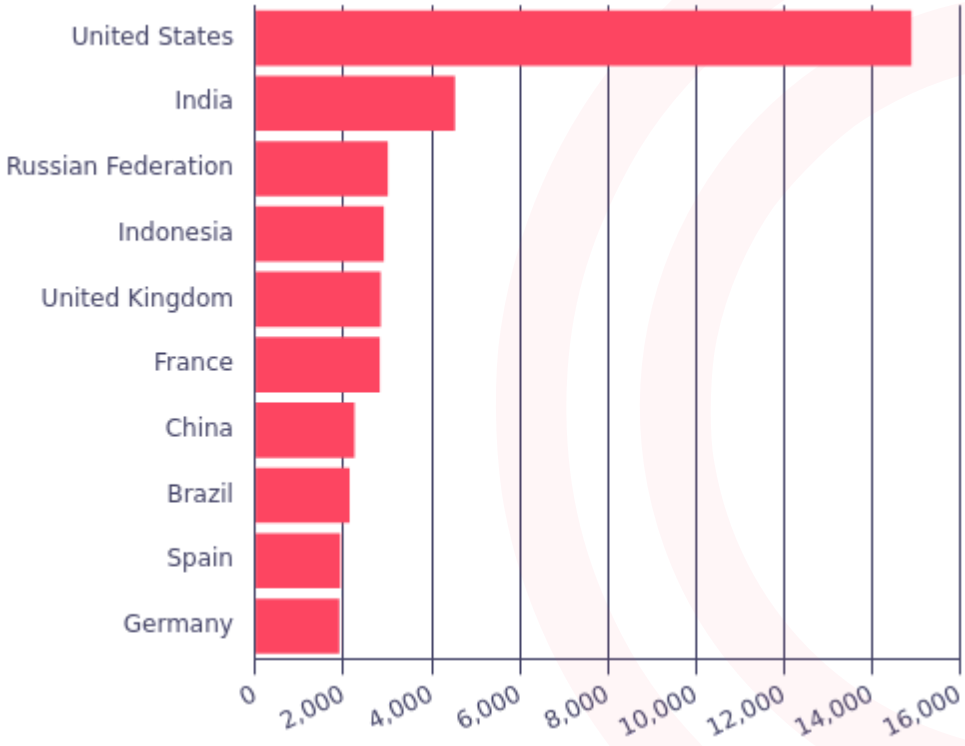
Cleo Data Breach Victims Given 48 Hours by Cl0p Gang

2024-12-24

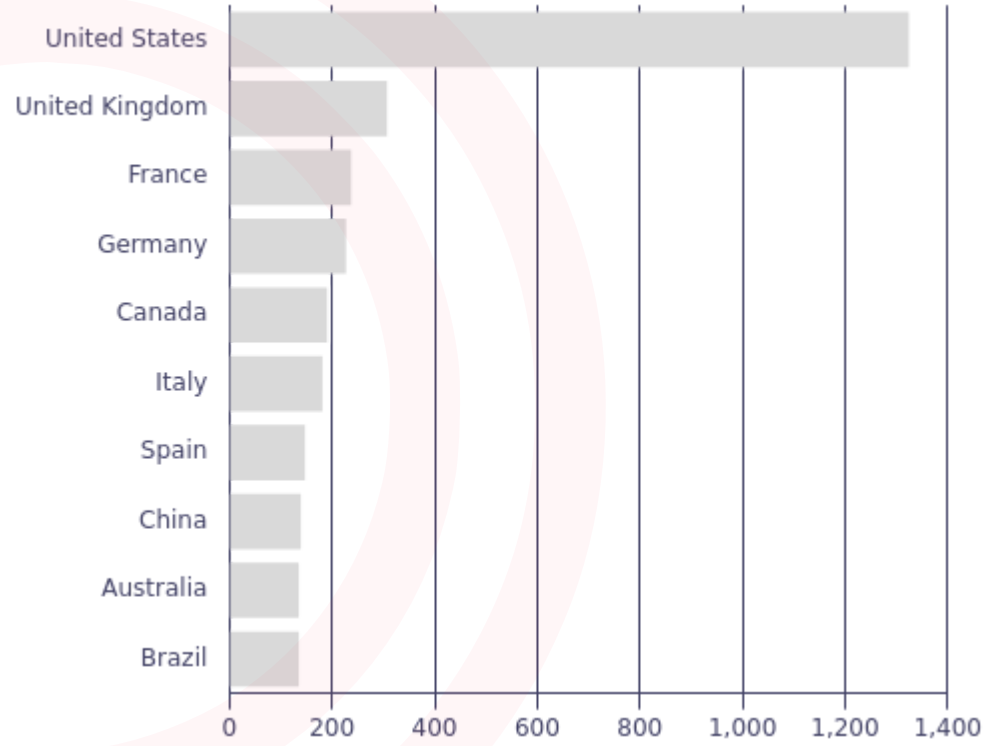
The Clop ransomware group has begun extorting victims of its Cleo data theft attacks. According to an announcement on the group's blog, 66 companies have been given 48 hours to respond to their demands. https://image.socradar.com/screenshots/2024/12/...

Top Target Countries

239 Different industries targeted in Banking



Dark Web Industry Threats



Ransomware Industry Threats

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
mizuhobank[.]fun	Banking	2025-11-08
mizuhobank[.]fun	Banking	2025-11-08
recuperation-des-fonds[.]...	Banking	2025-11-07
weebly[.]com	Banking	2025-11-07
isantander[.]info	Banking	2025-11-09
isantander[.]store	Banking	2025-11-09
isantander[.]net	Banking	2025-11-09
ea6ylx[.]hair	National Security...	2025-11-08

+992 Phishing Threats

22231 phishing domains detected in **Banking**

24 apt groups found in Banking

Group Name	Aliases	Country
GXC Team	-	Brazil , United Kingdom ...
LYCEUM	ATK 120 , siamesekitten , Yellow Dev 9 UNC1530 ...	Tunisia , Philippines ...
TA2719	Vendetta TA2719	Russia , Spain ...
RipperSec	-	-
TeamTNT	-	-
Unit 29155	GRU Unit 29155	Poland , Estonia ...
Cron	Cron	Poland , Hong Kong ...
Go1ano Developer	-	Brazil

+16 Threat Actors

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

SOCRadar®
Your Eyes Beyond

Trusted by world's leading organizations

Gartner
Peer Insights™

5/5