

Industry Threat Landscape Report

Banking

Time Period: 2024/11/26 - 2025/11/26 | Report Date: 2024-11-26



📍 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™



Agenda

01 Dark Web Threats

02 Ransomware Threats

03 Top Target Industry

04 Phishing Threats

05 APT Groups



800 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.

577 Dark web Threat Actors

corptoday

Borlov

XDev

miyako

PocketBins

Dark Web Threats



A screenshot of a dark web forum post from 'corptoday'. The post title is '700 USA CC / Sniff 70%+'. It was posted 9 minutes ago and edited. The post content includes: '★★ Who's not interested? ★★', 'Fresh USA since last week. Bulgaria https://...', 'Format: 4*****12/2028 | CVV: *** | FirstName LastName | Email: Pon*****@gmail.com | Phone: 630****041 | US phones are not available everywhere.', and a list of prices: 'Start: \$ 3k', 'Shag: \$ 500', 'Blic: \$5k', 'PPS 12c.'. The user has 48 posts and joined on 01/18/19. The post was edited 6 minutes ago by 'corptoday'.

A screenshot of a dark web forum post from 'Borlov'. The post title is 'General condition 41k us ss bin on request in ls valid 30-35%'. It was posted 40 minutes ago and edited. The post content includes: 'start 5k', 'ankle 500', 'flash 8k', and 'guarantor of you'. The user has 5 posts and joined on 09/19/25. The post was edited 38 minutes ago by 'Borlov'.

2025-11-21

Alleged 700 Credit Cards Belonging to the United States are on Sale

In a hacker forum monitored by SOCRadar, a new alleged credit cards sale is detected for the United States. <https://image.socradar.com/screenshots/2025/11/21/2598a001-6e4c-4f81-9b71-9ba6c6462d00.png> Fresh USA since last week. Bulgaria **** Format 4***...

2025-11-21

Alleged 41K Credit Cards Belonging to the United States are on Sale

In a hacker forum monitored by SOCRadar, a new alleged credit cards sale is detected for the United States. <https://image.socradar.com/screenshots/2025/11/21/695c7180-ac89-4ca8-b367-c66d69b64446.png> General condition 41k us ss bin on request in ls val...

Dark Web Threats



1400 US CC | VR 80%
By XDev , 1 hour ago in Auctions

XDev
byte
•
XDEV

Posted 1 hour ago
CCNUM|EXP_M|EXP_Y|CVV|FULL_NAME|ADDRESS|CITY|STATE|ZIP|COUNTRY|PHONE|EMAIL|IP

Fish dump, October. Didn't extract any bins, DB in its original form.
I won't sell to hucksters or let you test it. VR 84% according to 4Check, verified today. Expense guarantee.

Paid registration
② 15 posts Joined
08/26/25 (ID: 210634)
Activity coding / coder Car warranty 0
+ Quote

SELLING Venezuelan Bank
15 - 4 hours ago

4 hours ago
[+] OS: FortiOS
[+] Device: Firewall
[+] Permissions: Admin + CLI
[-] Revenue: Unknown
Contact Me via Session: [REDACTED]

2025-11-20

The Alleged Credit Card Data o...

In a hacker forum monitored by SO CRadar, a new alleged credit card data sale is detected for the United States. <https://image.socradar.com/screenshots/2025/11/20/640cc8dd-b32c-4398-a26f-85d0e7d6c12b.png> CCNUM|EXP_M|EXP_Y|CVV|FULL_NAME|ADDRESS|CIT...

2025-11-20

Alleged Unauthorized Admin Acc...

In a hacker forum monitored by SO CRadar, an unauthorized admin access sale is detected allegedly belongs to National Bank of Greece. <https://image.socradar.com/screenshots/2025/11/20/7b366a98-e103-4f0d-92ff-d619c611b05a.png> [+]
OS: FortiOS [+]
De...

2025-11-20

Alleged Unauthorized Admin Acc...

In a hacker forum monitored by SO CRadar, an unauthorized admin access sale is detected allegedly belongs to a bank that operates in Venezuela. <https://image.socradar.com/screenshots/2025/11/20/a622fae7-6cb8-4dbb-96fa-5490726e2379.png> [+]
OS: FortiOS [...]

1 ransomware attacks

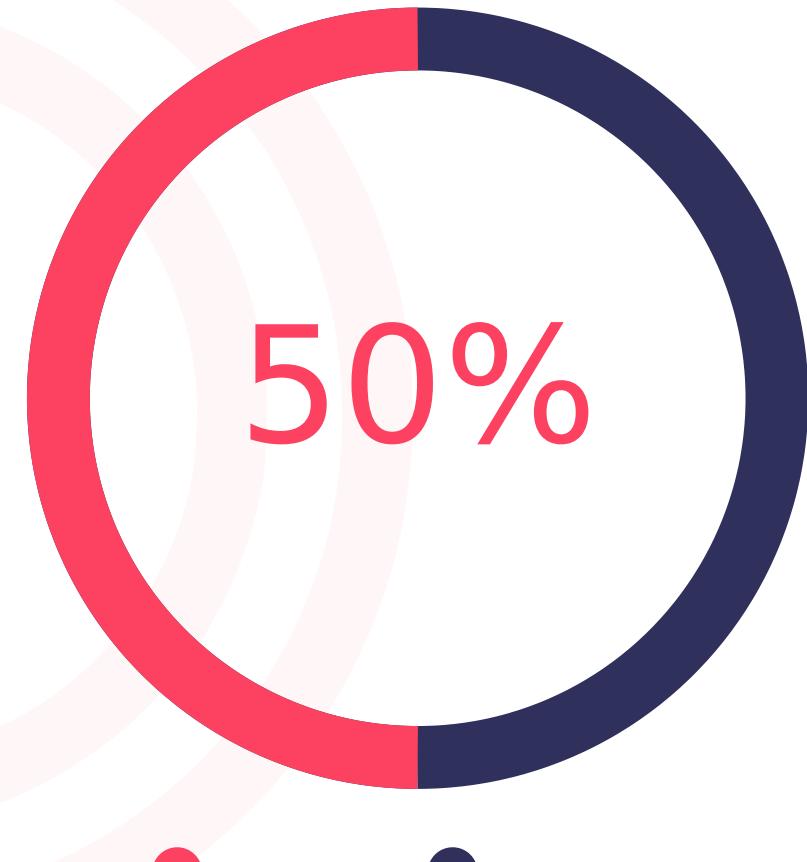
in Banking.

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



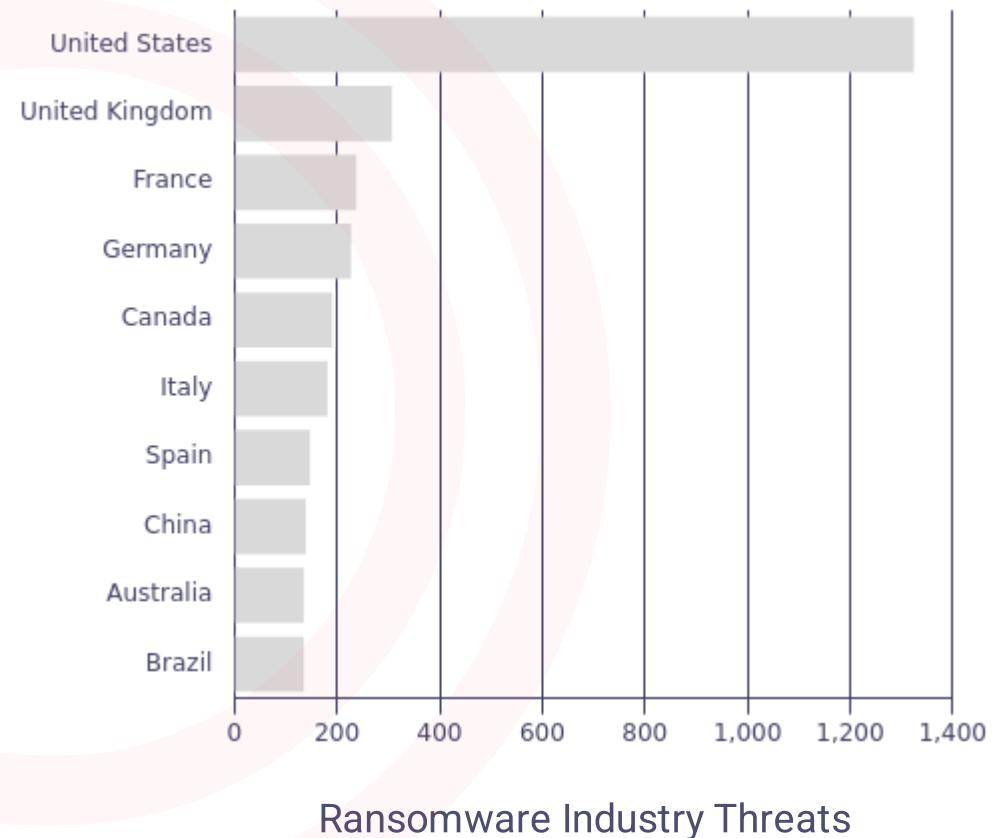
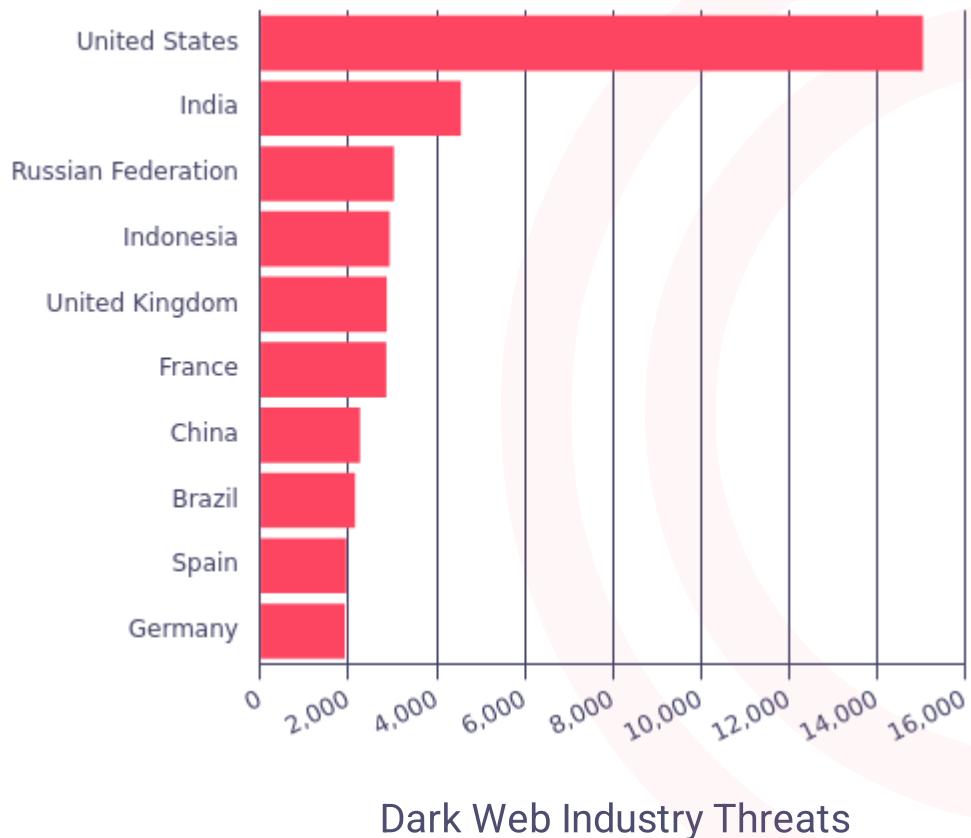
Cleo Data Breach Victims Given 48 Hours by Cl0p Gang

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/...](https://image.socradar.com/screenshots/2024/12/)

Top Target Countries

239 Different industries targeted in Banking



Phishing Threats

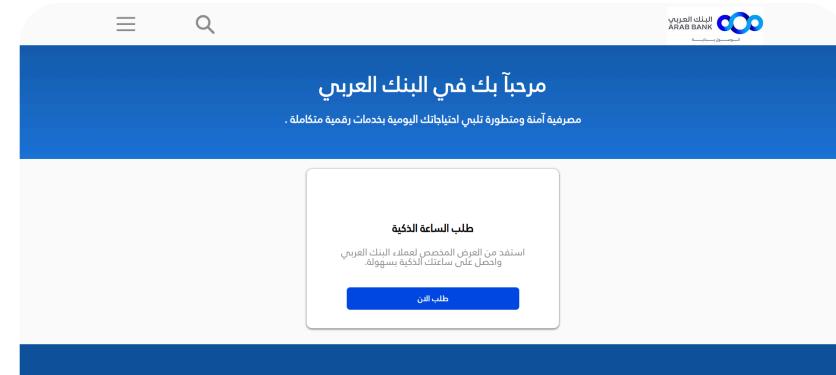


Brand impersonation takes place when a threat actor creates a social account pretending to be your brand. SOCRadar can spot fraudulent and fake domain. Also can spot fake social accounts by monitoring well-known social media platforms so that you can quickly take action to stop possible phishing scams.

Phishing Domain	Sector	Register Date
interbankcompe[.]com	Banking	2025-11-23
x5nglm[.]bond	Banking	2025-11-22
interbankcompe[.]com	Banking	2025-11-23
arbebanke[.]wixstudio[.]c...	Banking	2025-11-22
lyffirmenxx[.]fr	Banking	2025-11-20
lyffirmenxx[.]fr	Banking	2025-11-20
transit-clients-fr[.]com	Banking	2025-11-21
qsvx[.]fr	Banking	2025-11-21

+992 Phishing Threats

22132 phishing domains detected in Banking



23 apt groups found in Banking

Group Name	Aliases	Country
LYCEUM	Storm-0133 , Siamesekitten , Spirlin COBALT LYCEUM ...	 Pakistan  United Arab Emirates ...
Blue Mockingbird	-	 Australia  Ukraine ...
Void Balaur	Void Balaur RocketHack	 France  United States ...
Moonstone Sleet	-	 Argentina  Chile ...
Greedy Sponge	-	 Mexico
Killnet	-	 United States  France ...
Earth Berberoka	GamblingPuppet Earth Berberoka	 Southeast Asia  United States ...
NoName057	NoName05716 , 05716nnm , NoName057 Nnm05716	 United States  France ...

+15 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](#)



Trusted by world's leading organizations

Gartner
Peer Insights™

