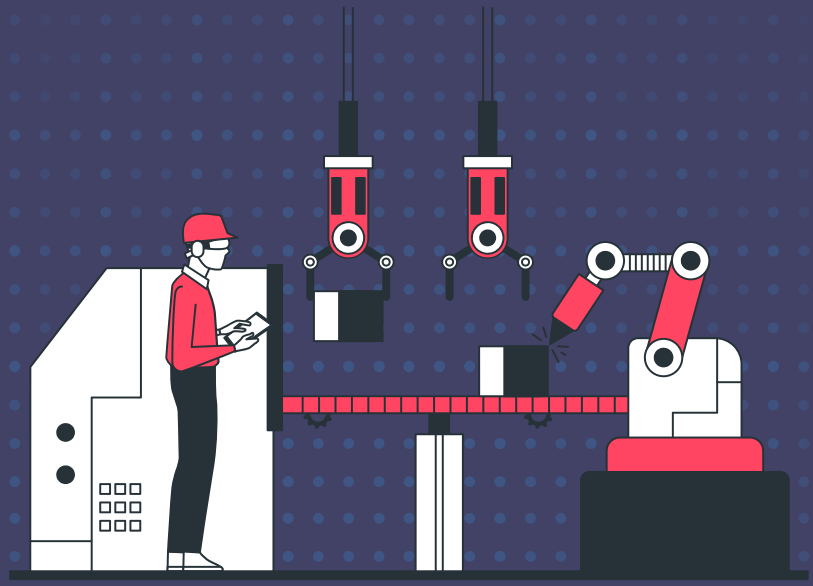
SOCRadar LABS



Industry Threat Landscape Report

HealthCare & Social Assistance

Time Period: 2024/10/30 - 2025/10/30 | Report Date: 2024-10-30

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

609 Dark Web Threats

in last one year.

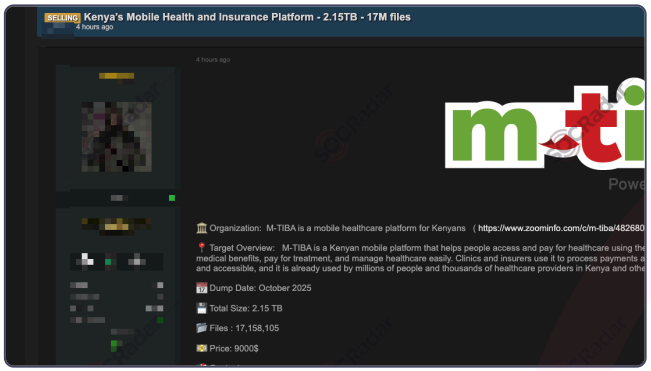
Most category are Selling and Sharing

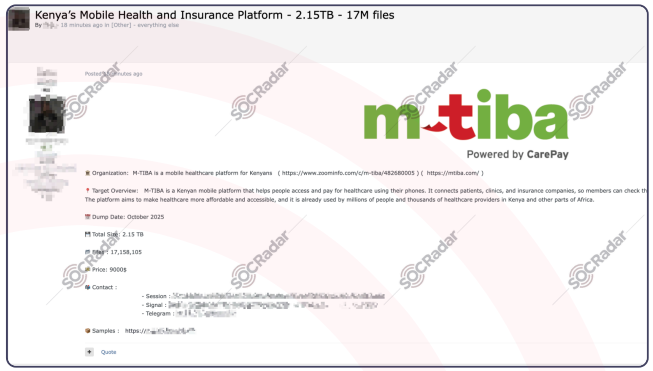
SOCRadar CTIA team has monitored the dark web to find trends and essential links. Throughout the this year, HealthCare & Social Assistance enterprises were bombarded with cyber attacks. Various threat actors have tried to sell and sometimes share the fruits of these successful cyberattacks on dark web hacker forums.

400 Dark web Threat Actors

- Kazu
- vulnerandolo
- injectioninferno2
- betway
- Loser

Classification [Confidential] Only For Designated Individuals
©SOCRadar Cyber Intelligence Inc. All rights reserved.





2025-10-25

Alleged Database of M-TIBA is on Sale

In a hacker forum monitored by SOCRadar, a new alleged database sale is detected for M-TIBA. https://image.socradar.com/screenshots/2025/10/25/53ad5bed-21d2-4a87-9b5c-50ac3e69163e.pngOrganization: M-TIBA is a mobile healthcare platform for Keny...

2025-10-25

The Alleged Database of M-TIBA is on Sale

In a hacker forum monitored by SOCRadar, a new alleged database sale is detected for M-TIBA. https://image.socradar.com/screenshots/2025/10/25/f090cbf3-d1cd-42e4-a18b-cefd11d6f3fb.png Organization: M-TIBA is a mobile healthcare platform for Kenyan...

Classification [Confidential] Only For Designated Individuals
©SOCRadar Cyber Intelligence Inc. All rights reserved.

2025-10-22

Alleged Citizen Database of Bo...

In a hacker forum monitored by SOCRadar, a new alleged citizen database sale is detected for Bolivia. https://image.socradar.com/screenshots/2025/10/22/de2ddf5c-5c33-4b71-b572-675b2ab1a76f.pngBolivia FRESH Citizen Database (Central Citizen Registry -...

2025-10-22

The Alleged Data of Argentinia...

In a hacker forum monitored by SOCRadar, a new alleged data sale is detected for Argentinian companies. https://image.socradar.com/screenshots/2025/10/22/64a78a98-d85e-4447-a495-839184e54b15.pngMEGA DATABASE ARGENTINA DATABASE ARGENTINA 650 GB BANK...

2025-10-20

The Alleged Database of Bova A...

In a hacker forum monitored by SOCRadar, a new alleged database leak is detected for Bova Aus. https://image.socradar.com/screenshots/2025/10/20/11494305-81ad-4bca-bd80-bcf66dd1dbde.pngIn 2025, we breached bovavet.com.au in Australia and exported ~18...

Classification [Confidential] Only For Designated Individuals
©SOCRadar Cyber Intelligence Inc. All rights reserved.

Ransomware Threats

2 ransomware attacks

in HealthCare & Social Assistance.

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.

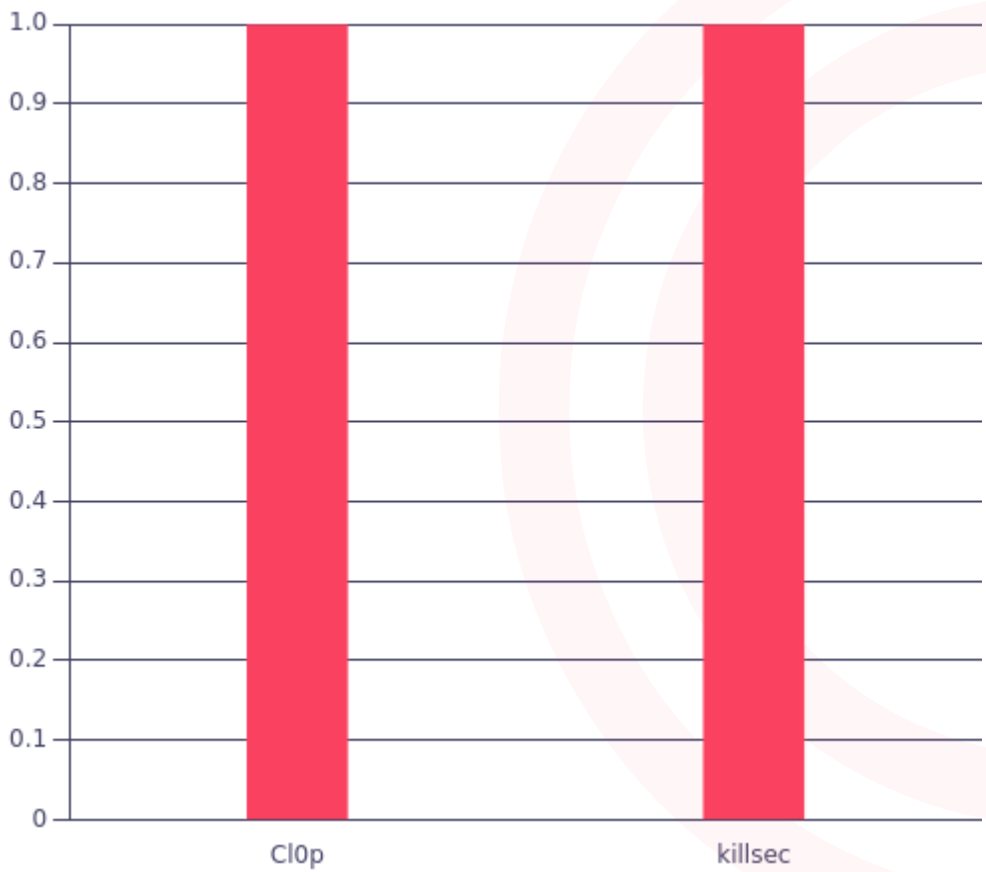
2 Ransomware Gangs

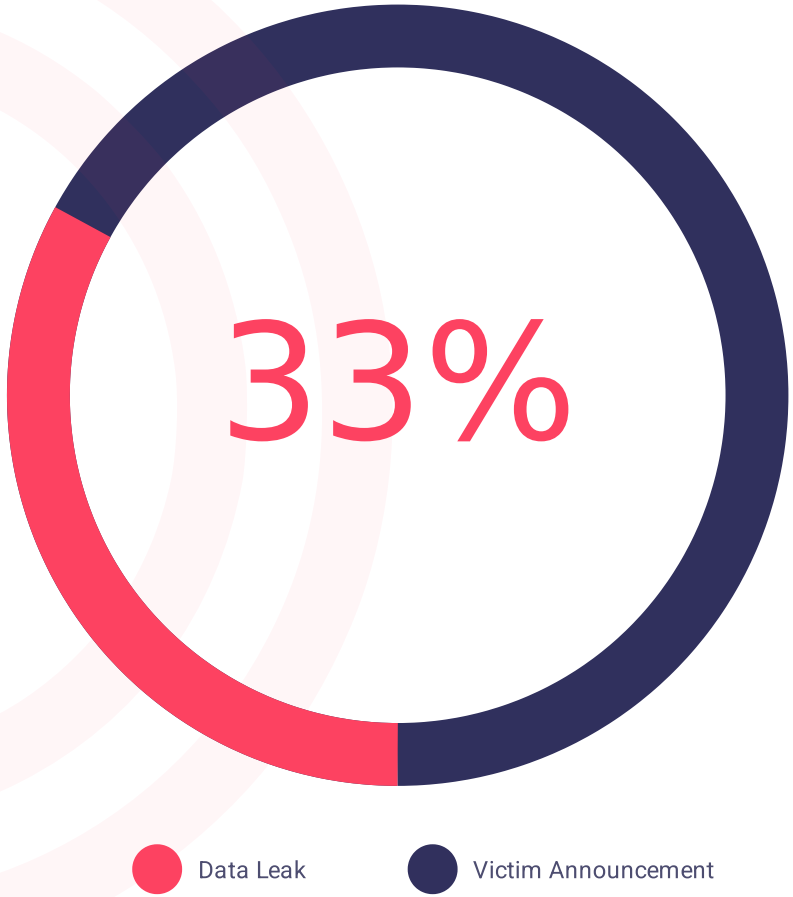
killsec

Cl0p

Classification [Confidential] Only For Designated Individuals
©SOCRadar Cyber Intelligence Inc. All rights reserved.

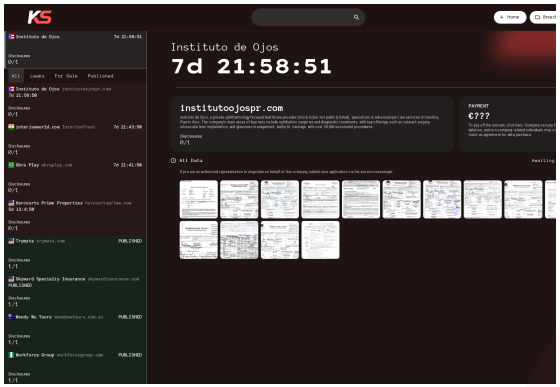
Ransomware Threats





Classification [Confidential] Only For Designated Individuals
©SOCRadar Cyber Intelligence Inc. All rights reserved.

Ransomware Threats



The New Ransomware Victim of killsec: Instituto de Ojos

2025-03-20

In the killsec ransomware group website monitored by SOCRadar, a new ransomware victim allegedly announced as Instituto de Ojos https://image.socradar.com/screenshots/2025/03/20/4ff73f3a-2889-4af2-b5bb-58d47d8bd6a5.pngN/A

Cleo Data Breach Victims Given 48 Hours by Cl0p Gang

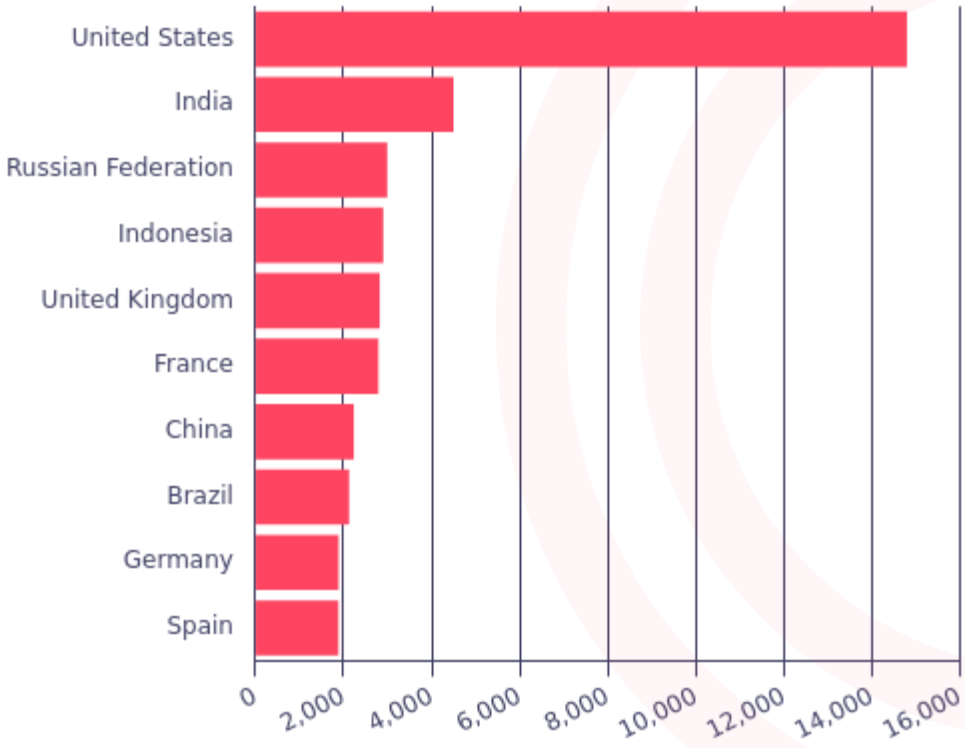
2024-12-24

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/...

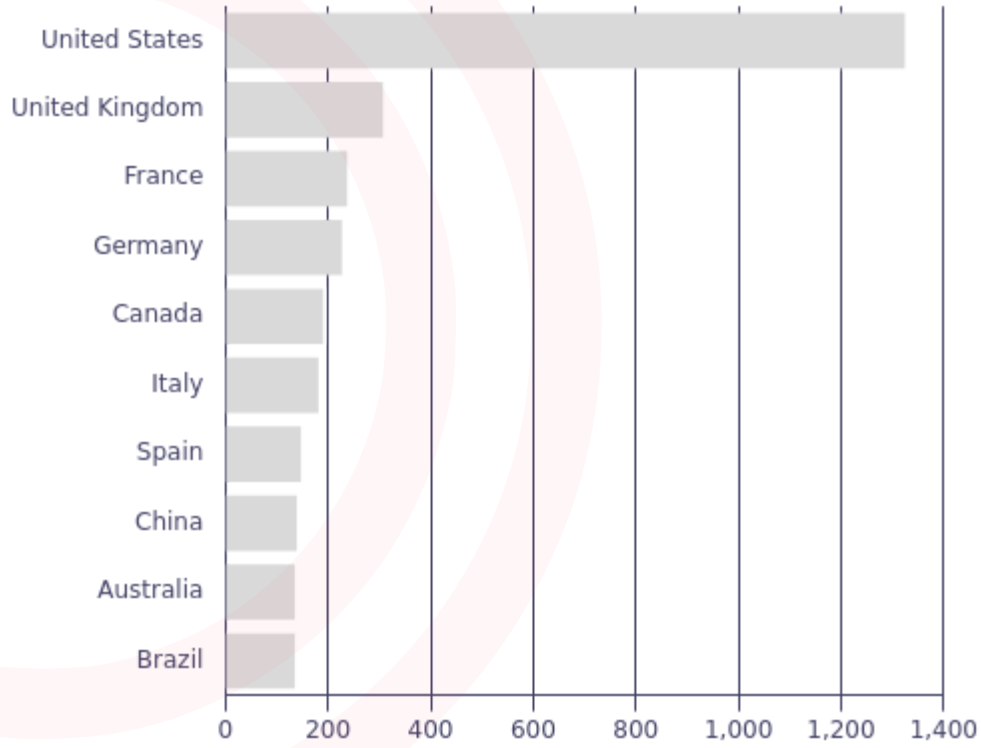
Classification [Confidential] Only For Designated Individuals
©SOCRadar Cyber Intelligence Inc. All rights reserved.

Top Target Countries

239 Different industries targeted in HealthCare & Social Assistance



Dark Web Industry Threats



Ransomware Industry Threats

Classification [Confidential] Only For Designated Individuals
©SOCRadar Cyber Intelligence Inc. All rights reserved.

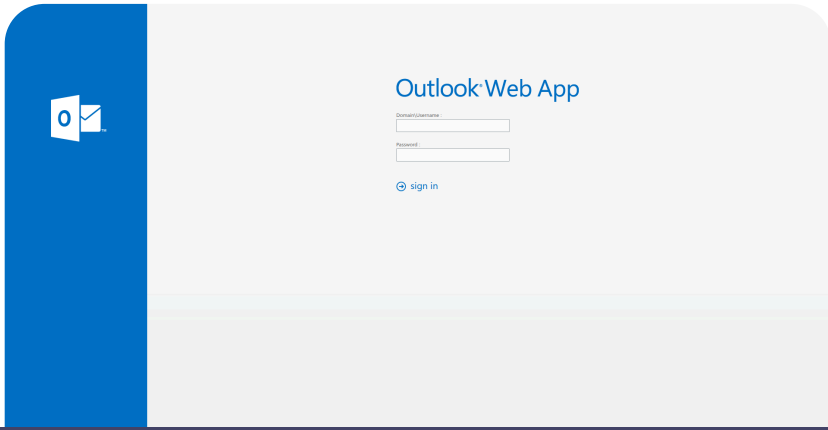
Phishing Threats

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
aiko[.]com[.]mx	HealthCare & ...	2025-10-26
nutrihealth4u[.]com	HealthCare & ...	2025-10-23
g-citi[.]org	Telecommunication...	2025-10-22
000webhostapp[.]com	HealthCare & ...	2025-10-22
weebly[.]com	HealthCare & ...	2025-10-21
ngmedicalbeauty[.]com	HealthCare & ...	2025-10-21
medicaltourismvithas[.]co...	HealthCare & ...	2025-10-21
covid19portal[.]s3[.]us-w...	Information Servi...	2025-10-21

+992 Phishing Threats

4985 phishing domains detected in HealthCare & Social Assistance



Classification [Confidential] Only For Designated Individuals
©SOCRadar Cyber Intelligence Inc. All rights reserved.

85 apt groups found in HealthCare & Social Assistance

Group Name	Aliases	Country
RomCom	Storm-0978 UAT-5647	Russian Federation , Spain ...
Storm-2372	-	-
RAZOR TIGER	Razor Tiger , BabyElephant , HN2 G0121 ...	Sri Lanka , Afghanistan ...
CHRYSENE	NewsBeef , Parastoo , Newscaster G0003 ...	Canada , Qatar ...
Ice Fog	Dagger Panda , TEMP.Trident , Moshen Dragon RedFoxtrot ...	Taiwan , Canada ...
Evilnum	TA4563 , Evilnum , G0120 Jointworm	Albania , Canada ...
Turla Group	Shell Crew , JerseyMikes , Turbine Panda Venomous Bear ...	Syria , Canada ...
APT42	APT 42 GreenBravo	Malaysia , Norway ...

+77 Threat Actors

Classification [Confidential] Only For Designated Individuals
©SOCRadar Cyber Intelligence Inc. All rights reserved.

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