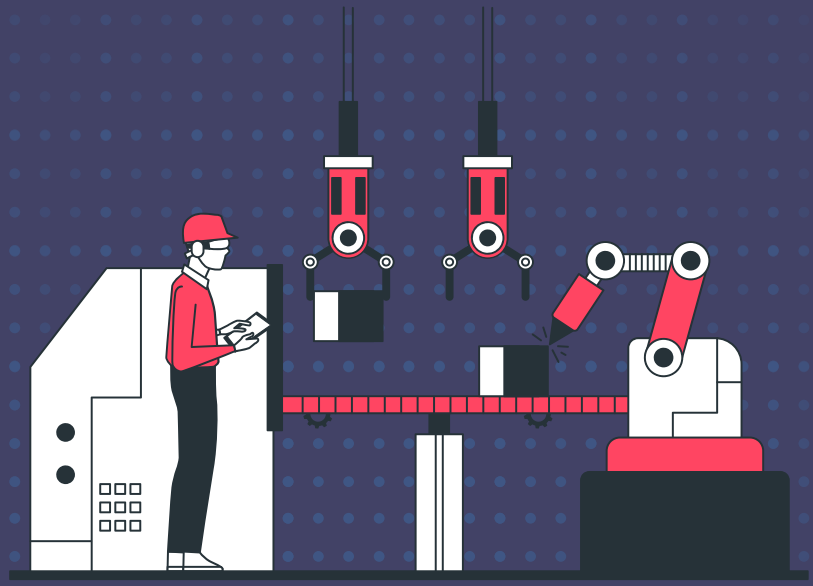
SOCRadar LABS



Industry Threat Landscape Report

Energy & Utilities

Time Period: 2024/11/18 - 2025/11/18 | Report Date: 2024-11-18

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

193 Dark Web Threats

in last one year.

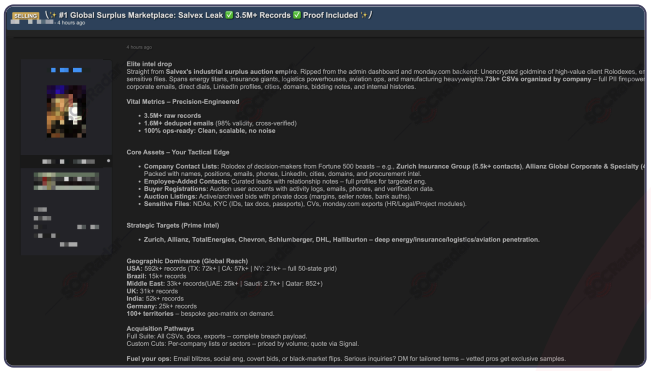
Most category are Selling and Sharing

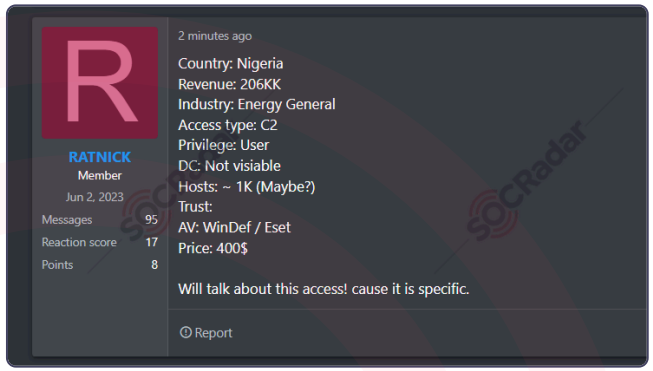
SOCRadar CTIA team has monitored the dark web to find trends and essential links. Throughout the this year, Energy & Utilities enterprises were bombarded with cyber attacks. Various threat actors have tried to sell and sometimes share the fruits of these successful cyberattacks on dark web hacker forums.

138 Dark web Threat Actors

- CharlesWilson
- RATNICK
- bitcoin
- Cayenne22
- Big-Bro

Dark Web Threats





2025-11-13

Alleged Database of Salvex is on Sale

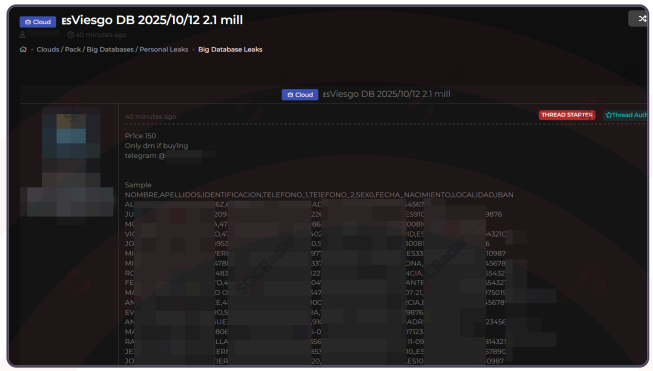
In a hacker forum monitored by SOCRadar, a new alleged database sale is detected for Salvex. https://image.socradar.com/screenshots/2025/11/13/e41ed503-bedf-4289-88d5-088c32a79fff.pngElite intel drop Straight from Salvex's industrial surplus auc...

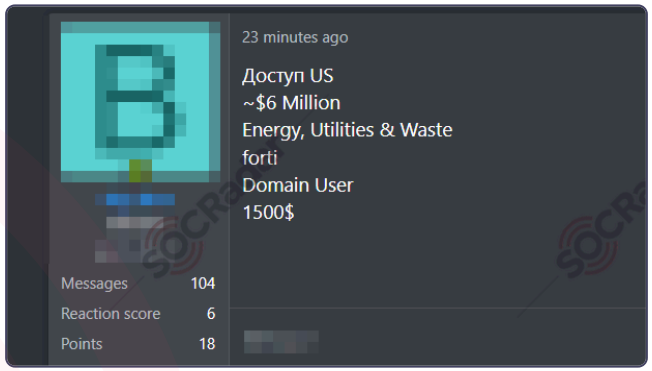
2025-11-12

The Alleged Unauthorized Access Sale is Detected for a Nigerian Energy Company

In a hacker forum monitored by SOCRadar, an unauthorized admin access sale is detected allegedly belongs to an energy company that operates in Nigeria. https://image.socradar.com/screenshots/2025/11/12/90fc7d70-c1c4-4f22-abe4-73c8d4c3d4f2.pngCou...

Dark Web Threats





2025-11-12

The Alleged Data of Power Tran...

In a hacker forum monitored by SOCRadar, a new alleged data sale is detected for Power Transmission Company No. 4. https://image.socradar.com/screenshots/2025/11/12/ef836948-da5d-4641-ba7f-1148c8a46258.png!!!IF ANY INTEREST IN ANYTHING I HAVE DO...

2025-11-08

The Alleged Database of Viesgo...

In a hacker forum monitored by SOCRadar, a new alleged database sale is detected for Viesgo. https://image.socradar.com/screenshots/2025/11/07/d38f8af5-5c95-4666-8e0b-0f50a1b5a912.pngPr1ce 150 Only dm if buy1ng telegram @ ***** Sample NOMBRE,APELLIDO...

2025-11-07

The Alleged Unauthorized Forti...

In a hacker forum monitored by SOCRadar, an unauthorized Forti access sale is detected allegedly belongs to a utilities company that operates in the United States. https://image.socradar.com/screenshots/2025/11/07/32366397-6539-4316-8f1b-748c9c85ccdf...

63 ransomware attacks

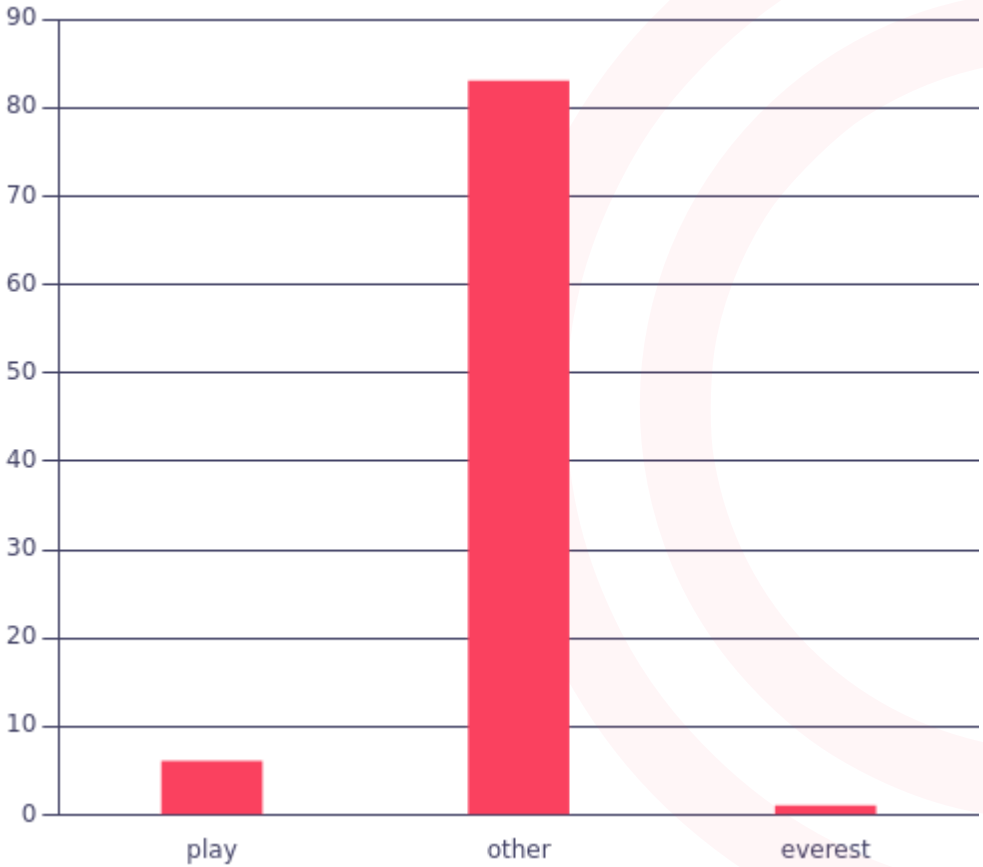
in Energy & Utilities .

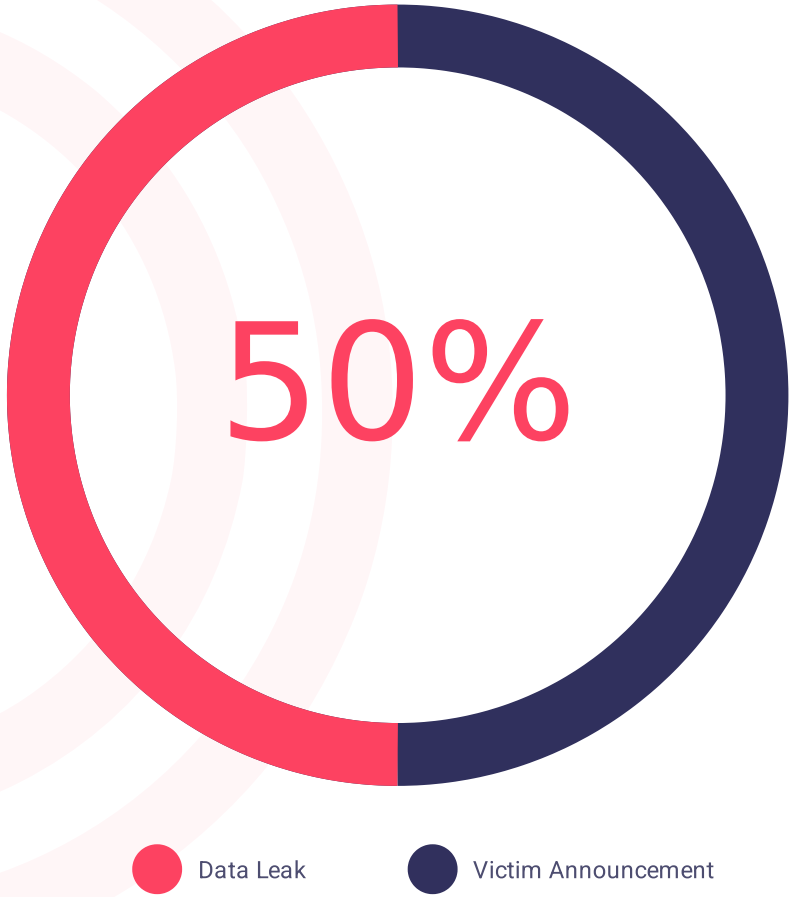
Ransomware attacks are among the most critical cyber attacks an organization can experience. The results can be destructive for an organization and lead to massive data loss and leaks of the victim company's sensitive data.

41 Ransomware Gangs

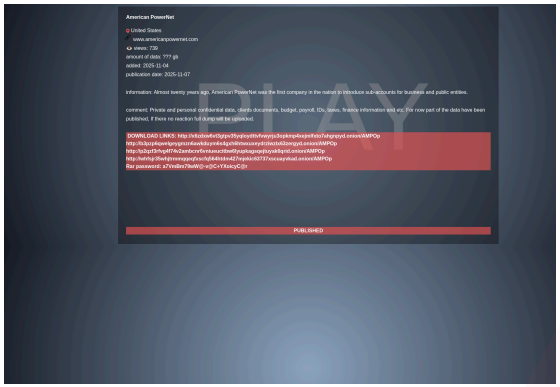
- qilin
- play
- sinobi
- blacksuit
- hunters

Ransomware Threats





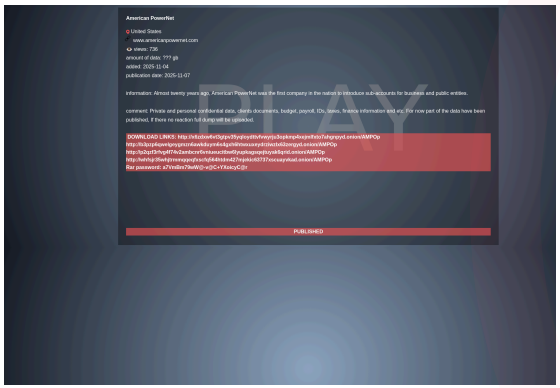
Ransomware Threats



The New Ransomware Victim of play: American PowerNet

2025-11-08

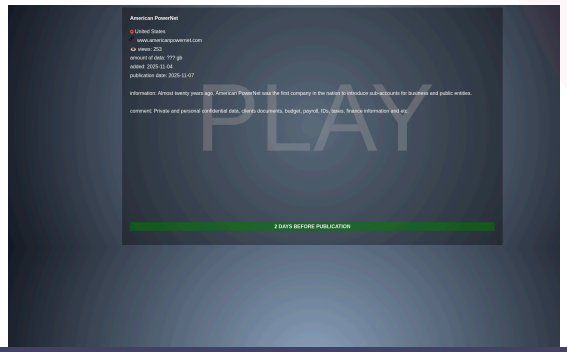
In the play ransomware group website monitored by SOCRadar, a new ransomware victim allegedly announced as American PowerNet https://image.socradar.com/screenshots/2025/11/07/ea6f6514-1727-43b5-b267-e75fc376df7d.pngUnited States



The New Ransomware Victim of play: American PowerNet

2025-11-08

In the play ransomware group website monitored by SOCRadar, a new ransomware victim allegedly announced as American PowerNet https://image.socradar.com/screenshots/2025/11/07/2052e91d-00e7-4fc7-880d-89a7a09745d5.pngUnited States

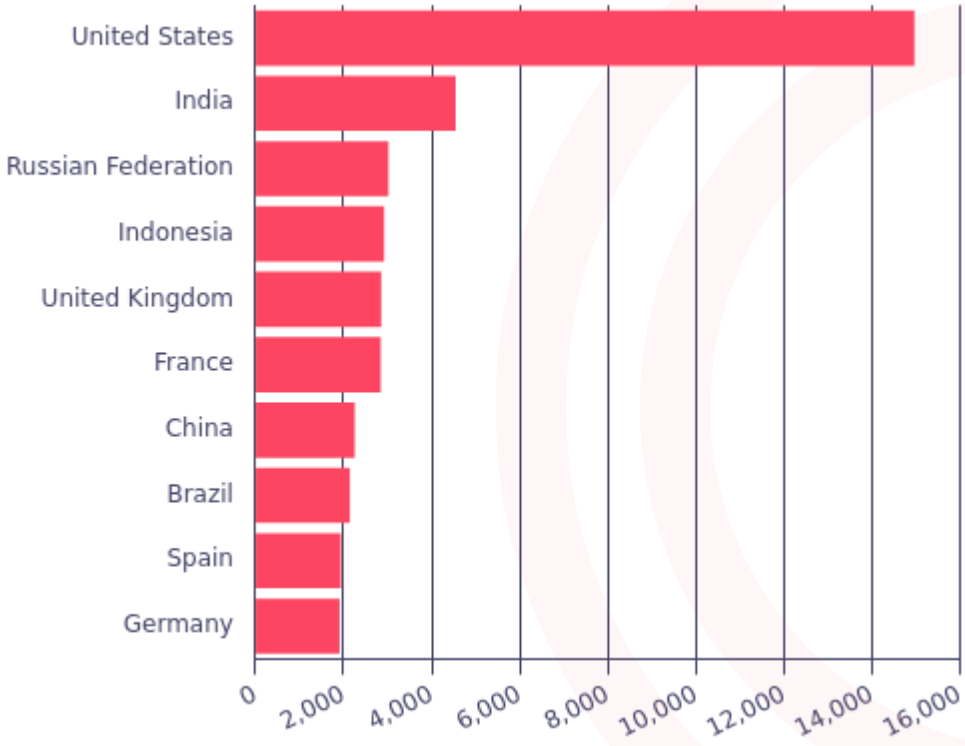


The New Ransomware Victim of play: American PowerNet

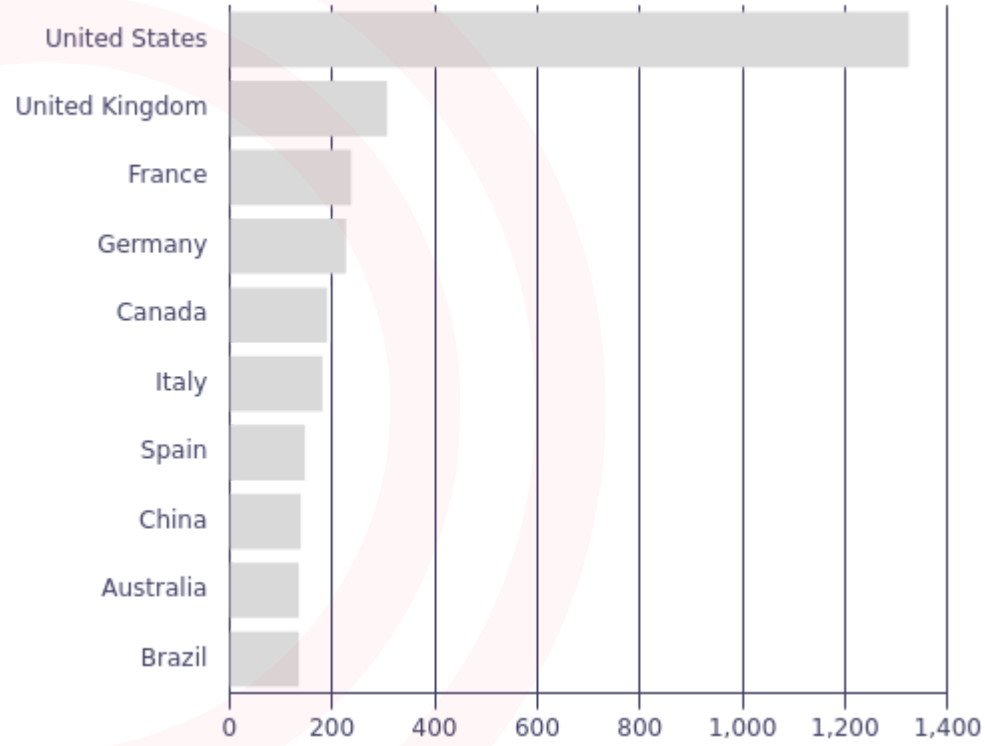
2025-11-06

In the play ransomware group website monitored by SOCRadar, a new ransomware victim allegedly announced as American PowerNet https://image.socradar.com/screenshots/2025/11/05/03c9c31e-15a1-4b5c-a0ca-5d39b0573be5.pngUnited States

239 Different industries targeted in Energy & Utilities



Dark Web Industry Threats



Ransomware Industry Threats

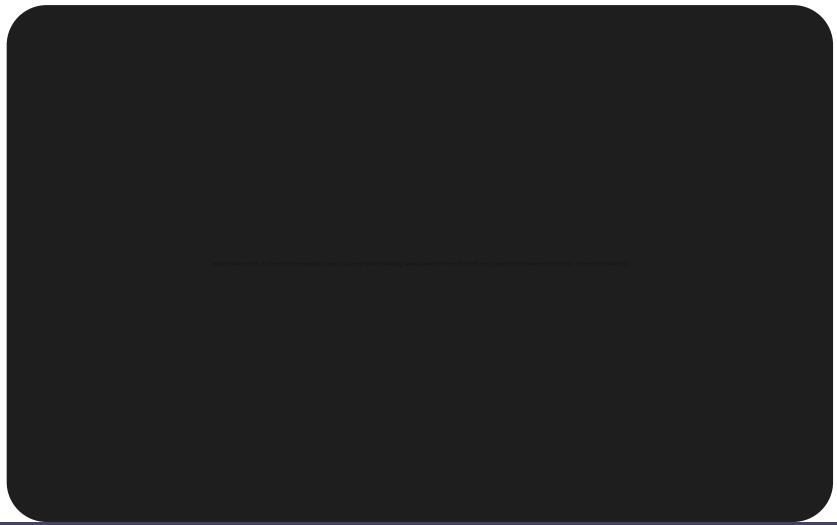
Phishing Threats

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
focusplusenergy[.]com	Energy & Util...	2025-11-12
focusplusenergy[.]com	Energy & Util...	2025-11-12
focusplusenergy[.]com	Energy & Util...	2025-11-12
focusplusenergy[.]com	Energy & Util...	2025-11-12
quantum-mesh-shell[.]com	Energy & Util...	2025-11-12
phase-shell-sequence-sign...	Energy & Util...	2025-11-12
phase-shell-sequence-sign...	Energy & Util...	2025-11-12
quantum-mesh-shell[.]com	Energy & Util...	2025-11-12

+992 Phishing Threats

1164 phishing domains detected in Energy & Utilities



68 apt groups found in Energy & Utilities

Group Name	Aliases	Country
Operation Titan Rain	Operation Titan Rain	Philippines , USA ...
AridViper	DESERTVARNISH , Desert Falcon , Big Bang APT UNC718 ...	Lebanon , Russian Federation ...
APT 29	Swallowtail , Sednit , SilverFish Blue Dev 5 ...	Ireland , Singapore ...
HAZY TIGER	Orange Yali , TA397 , Bitter G1002 ...	Madagascar , Saudi Arabia ...
Careto	Mask , The Mask , Ugly Face Careto	Spain , Lithuania ...
LYCEUM	Chrono Kitten , Lyceum , Hexane siamesekitten ...	Singapore , Nicaragua ...
APT 28	Swallowtail , Sednit , FANCY BEAR IRON TWILIGHT ...	World Anti-Doping Agency , Poland ...
Volt Typhoon	DEV-0391 , BRONZE SILHOUETTE , UNC3236 Voltzite ...	Singapore , USA ...

+60 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