SOCRadar®
Your Eyes Beyond

# SAUDI ARABIA

## Regional Threat Landscape Report

SOCRadar®
Your Eyes Beyond

## Table of Contents

# Executive Summary

As a major economic hub in the Middle East and a global leader in the energy sector, Saudi Arabia has emerged as a key target for cyber threats. The country's growing reliance on digital transformation, driven by its Vision 2030 initiatives, has significantly advanced its economic sectors, including oil and gas, finance, healthcare, and technology. However, this rapid digitalization has also exposed critical vulnerabilities, posing significant risks to its infrastructure and national security.

Saudi Arabia faces a persistent barrage of cyber threats from both financially motivated cybercriminals and state-sponsored actors. These attackers frequently exploit weaknesses in the country's digital ecosystem, with notable targets including the energy, finance, and government sectors. The sophistication and frequency of cyber incidents have surged, encompassing ransomware attacks, data breaches, and insider threats. The rise of Ransomware-as-a-Service (RaaS) has further enabled attackers to launch disruptive campaigns with minimal technical expertise.

The Dark Web plays a pivotal role in the cyber threat landscape, facilitating the trade of stolen data, cyber tools, and services. This clandestine ecosystem gives attackers greater anonymity, allowing them to coordinate and execute more advanced attacks against Saudi organizations.

This report analyzes Saudi Arabia's cyber threat landscape in-depth, combining open-source intelligence with proprietary research. It is designed to equip public and private sector stakeholders with actionable insights to enhance their cyber defenses, mitigate risks, and bolster resilience against evolving threats in an increasingly hostile digital environment.

*To access SOCRadar's 2023 Saudi Arabia report, click here.*

# Top Takeaways

**Dark Web Activity:** In 2024, 72 distinct threat actors actively targeted Saudi Arabian entities, making 166 postings on the Dark Web. These activities primarily focused on selling compromised data and unauthorized access credentials, emphasizing the critical need for robust data protection measures.

**Retail Trade Under Threat:** The Retail Trade sector emerged as the most targeted industry, accounting for 22.89% of Dark Web activities. This underscores its strategic importance and susceptibility to cyber threats.

**Ransomware Surge:** Saudi Arabia experienced 88 ransomware incidents in 2024, with attacks increasingly targeting key industries like manufacturing, information, and construction. This highlights the persistent focus of ransomware operators on exploiting vulnerabilities in vital sectors.

**Prominent Ransomware Groups:** Notorious ransomware groups such as LockBit 3.0, Cl0p, and ALPHV (BlackCat) dominated the threat landscape in Saudi Arabia, collectively accounting for most ransomware incidents.

**Stealer Logs Impact:** Extensive use of Stealer Logs in 2024 led to the compromise of sensitive data from high-traffic domains, including 1.8 million email/password combinations and over 57,000 credit card entries, showcasing the severity of credential-based attacks.

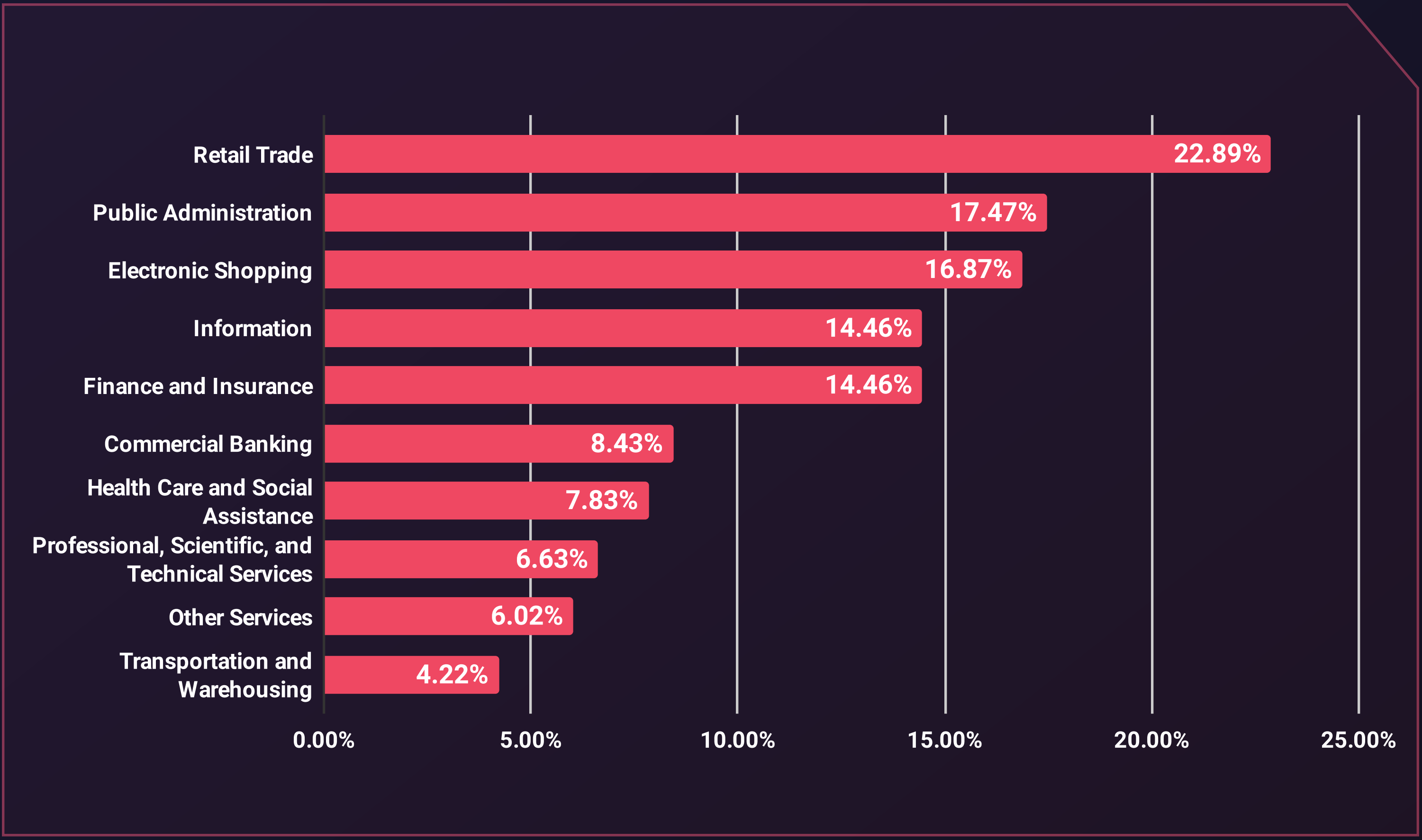
**Record-Breaking DDoS Attacks:** Saudi Arabia faced unprecedented Distributed Denial of Service (DDoS) attacks in 2024. The most significant multi-vector attack utilized 26 techniques and reached a peak bandwidth of 2 Tbps. This illustrates the growing sophistication and intensity of cyber threats.

# Dark Web Threats Targeting Saudi Arabian Entities

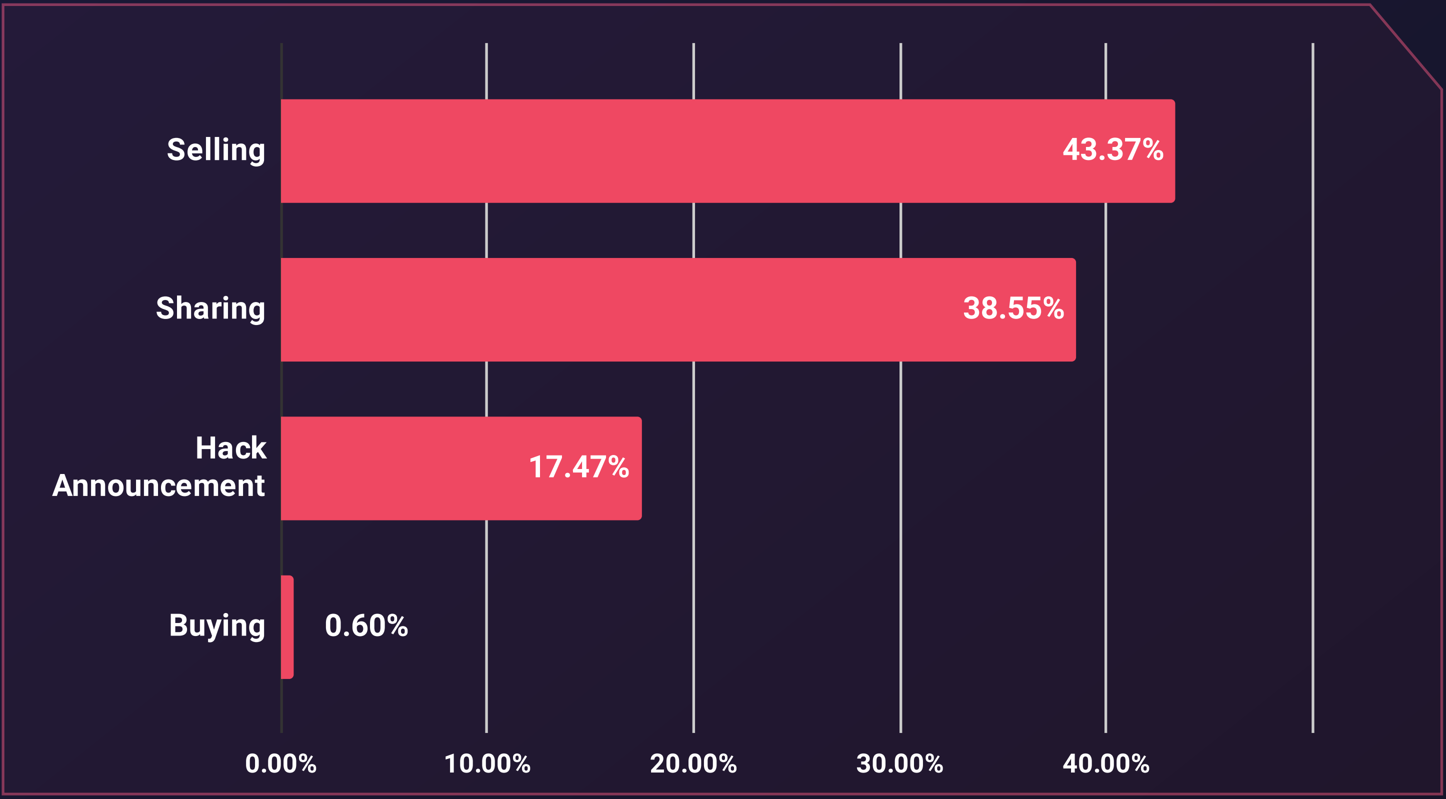
Over the preceding year, SOCRadar's Dark Web Analysts diligently monitored activities within the Dark Web, identifying notable trends and establishing connections between Saudi Arabia enterprises and covert threat actors. Throughout 2024, Saudi Arabian entities encountered a continuous barrage of cyber threats, with various actors attempting to exploit successful intrusions by trading or leveraging their gains in Dark Web forums.

SOCRadar observed 166 Dark Web forum posts linked to 72 distinct threat actors during this period. The Retail Trade industry emerged as the most prominently affected sector, representing **22.89%** of the identified cyber threats during this period. Public Administration followed, accounting for **17.47%,** while Electronic Shopping comprised **16.87%** of the targeted industries. The information, finance, and Insurance sectors accounted for **14.46%,** highlighting the critical vulnerabilities in these areas and the need for enhanced cybersecurity measures.

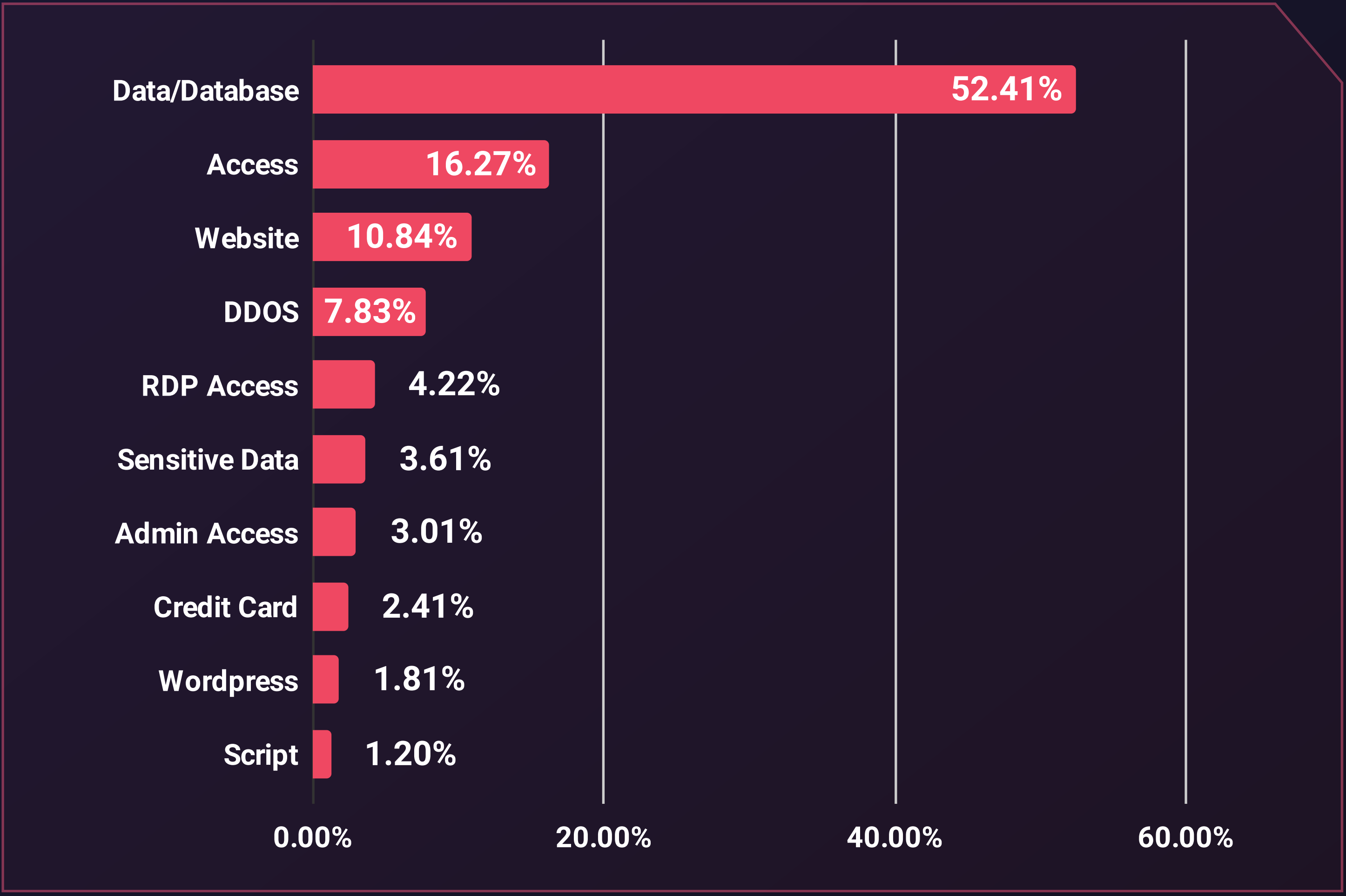
## Industry Distribution of  Dark Web Threats



## Distribution of Dark Web Threats by Post Type

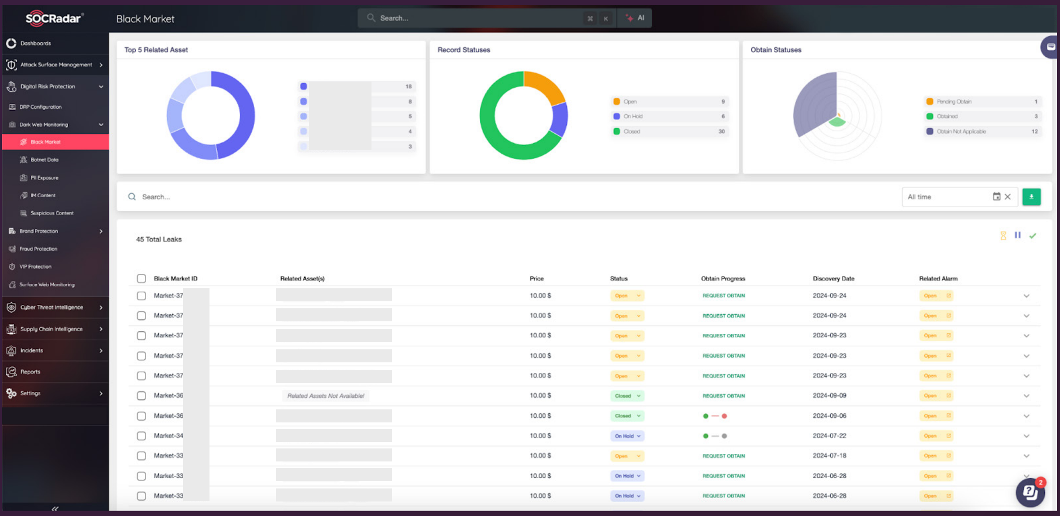


## Distribution of Dark Web Threats by Threat Type



*SOCRadar's Advanced Dark Web Monitoring* provides Saudi Arabian organizations with critical insights into hidden threats targeting their sectors, including Retail Trade, finance, and Insurance, which have faced significant risks over the past year. With real-time tracking of underground chatter and sensitive data exposure, SOCRadar enables proactive defense against Dark Web threats.

Activate your *free demo today* to safeguard your organization’s most valuable assets.



45 Total Leaks

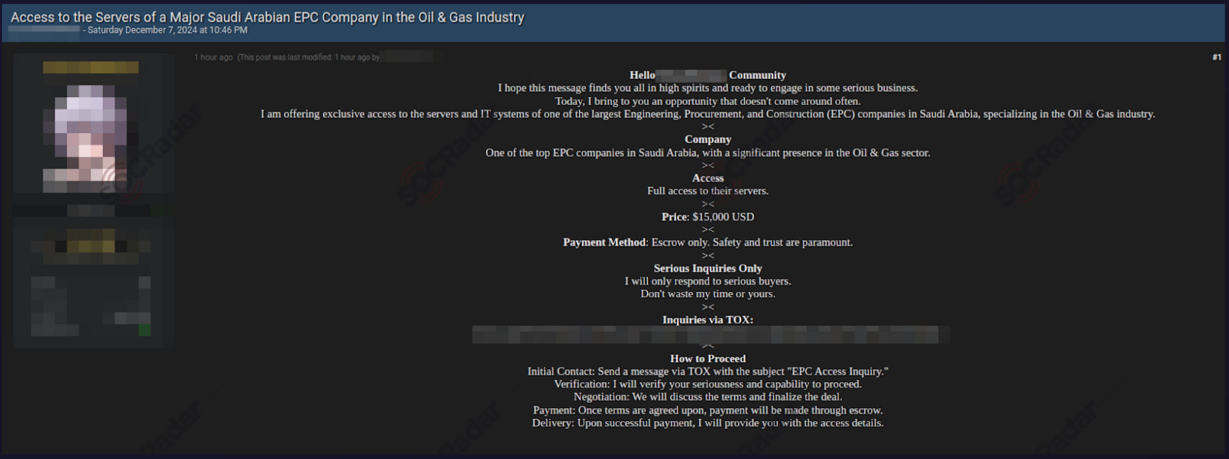
| □ | Black Market ID | Related Asset(s) | Price | Status | Obtain Progress | Discovery Date | Related Alarm |
|---|---|---|---|---|---|---|---|
| □ | Market-37 [redacted] | [redacted] | 10.00 $ | Open | REQUEST OBTAIN | 2024-09-24 | Open |
| □ | Market-37 [redacted] | [redacted] | 10.00 $ | Open | REQUEST OBTAIN | 2024-09-24 | Open |
| □ | Market-37 [redacted] | [redacted] | 10.00 $ | Open | REQUEST OBTAIN | 2024-09-23 | Open |
| □ | Market-37 [redacted] | [redacted] | 10.00 $ | Open | REQUEST OBTAIN | 2024-09-23 | Open |
| □ | Market-37 [redacted] | [redacted] | 10.00 $ | Open | REQUEST OBTAIN | 2024-09-23 | Open |
| □ | Market-36 [redacted] | *Related Assets Not Available!* | 10.00 $ | Closed | REQUEST OBTAIN | 2024-09-09 | Open |
| □ | Market-36 [redacted] | [redacted] | 10.00 $ | Closed | ● — ● | 2024-09-06 | Open |
| □ | Market-34 [redacted] | [redacted] | 10.00 $ | On Hold | ● — ● | 2024-07-22 | Open |
| □ | Market-33 [redacted] | [redacted] | 10.00 $ | Open | REQUEST OBTAIN | 2024-07-18 | Open |
| □ | Market-33 [redacted] | [redacted] | 10.00 $ | On Hold | REQUEST OBTAIN | 2024-06-28 | Open |
| □ | Market-33 [redacted] | [redacted] | 10.00 $ | On Hold | REQUEST OBTAIN | 2024-06-28 | Open |

# Recent Dark Web Activities Targeting Saudi Arabian Entities

## The Alleged Unauthorized Access Sale is Detected for a Saudi Arabian EPC Company

07 Oct 2024

An unauthorized access sale was detected in a hacker forum monitored by SOCRadar. The sale allegedly belongs to a major Saudi Arabian EPC company specializing in Oil and gas. The seller claims full access to the company's servers and is seeking $15,000 USD in exchange for the access credentials.



Access to the Servers of a Major Saudi Arabian EPC Company in the Oil & Gas Industry
[redacted] - Saturday December 7, 2024 at 10:46 PM

1 hour ago (This post was last modified: 1 hour ago by [redacted]

#1

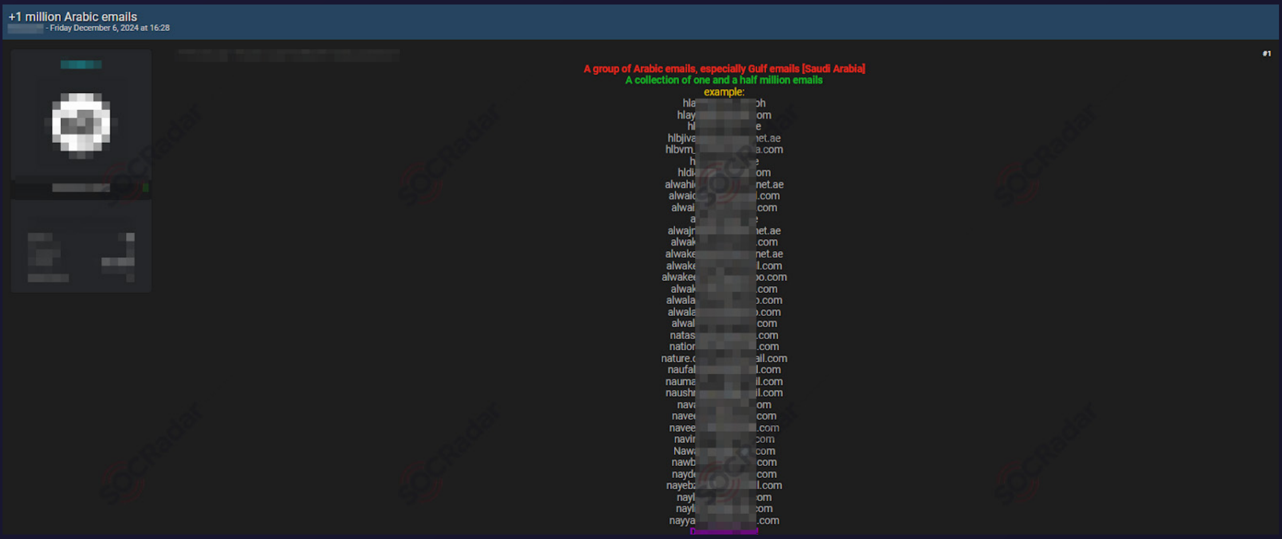
**Hello [redacted] Community**
I hope this message finds you all in high spirits and ready to engage in some serious business.
Today, I bring to you an opportunity that doesn't come around often.
I am offering exclusive access to the servers and IT systems of one of the largest Engineering, Procurement, and Construction (EPC) companies in Saudi Arabia, specializing in the Oil & Gas industry.
><
**Company**
One of the top EPC companies in Saudi Arabia, with a significant presence in the Oil & Gas sector.
><
**Access**
Full access to their servers.
><
**Price**: $15,000 USD
><
**Payment Method**: Escrow only. Safety and trust are paramount.
><
**Serious Inquiries Only**
I will only respond to serious buyers.
Don't waste my time or yours.
><
**Inquiries via TOX:**
[redacted]
><
**How to Proceed**
Initial Contact: Send a message via TOX with the subject "EPC Access Inquiry."
Verification: I will verify your seriousness and capability to proceed.
Negotiation: We will discuss the terms and finalize the deal.
Payment: Once terms are agreed upon, payment will be made through escrow.
Delivery: Upon successful payment, I will provide you with the access details.

*Screenshot of the forum post - Unauthorized access sale*

## The Alleged Email Data of Saudi Arabian Citizens Are Leaked

06 Dec 2024

SOCRadar's monitoring of a hacker forum has uncovered a potential data breach targeting Saudi Arabian citizens, with a collection of 1.5 million alleged email addresses advertised on the dark web. The leaked data, primarily affecting Gulf region email domains linked to Saudi Arabia, includes examples such as "hlatib.bh," "hlayal.com," and "hlbji**e." A link to download the data has also been shared on the forum, raising concerns about its authenticity and potential misuse.



+1 million Arabic emails
[redacted] - Friday December 6, 2024 at 16:28

#1

A group of Arabic emails, especially Gulf emails [Saudi Arabia]
A collection of one and a half million emails
example:

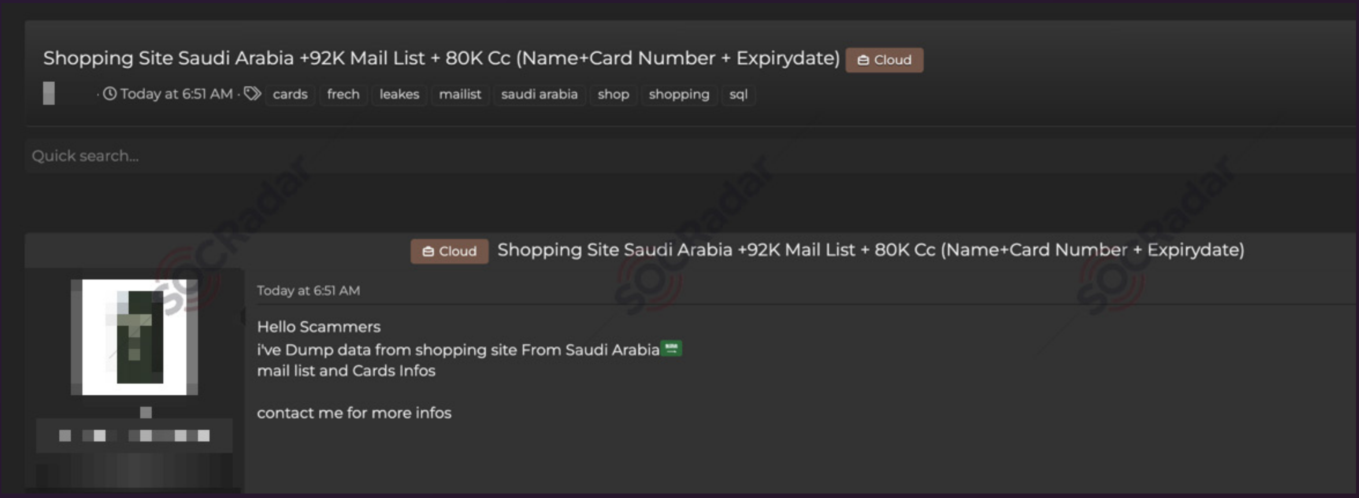
hla[redacted]oh
hlay[redacted]om
hl[redacted]e
hlbjiva[redacted]et.ae
hlbvm_[redacted]a.com
h[redacted]e
hldi[redacted]om
alwahi[redacted]net.ae
alwaic[redacted].com
alwai[redacted]com
a[redacted]e
alwajr[redacted]et.ae
alwak[redacted].com
alwake[redacted]net.ae
alwake[redacted]l.com
alwakee[redacted]o.com
alwak[redacted].com
alwala[redacted].com
alwala[redacted].com
alwal[redacted]com
natas[redacted].com
natior[redacted].com
nature.[redacted]ail.com
naufal[redacted]l.com
nauma[redacted]il.com
naushi[redacted]il.com
nava[redacted]om
navee[redacted]com
navee[redacted].com
navir[redacted]com
Nawa[redacted]com
nawb[redacted]com
nayd[redacted]com
nayeb[redacted]l.com
nayl[redacted]om
nayl[redacted]om
nayya[redacted].com

*Screenshot of the forum post - Saudi Arabia +1 million emails*

## Alleged Database of a Saudi Arabian E-Commerce Company is on Sale

07 Nov 2024

SOCRadar's monitoring of a hacker forum has revealed the alleged sale of a database belonging to a Saudi Arabian e-commerce company, reportedly containing customers' email addresses and card information.



Shopping Site Saudi Arabia +92K Mail List + 80K Cc (Name+Card Number + Expirydate) Cloud
[redacted] · Today at 6:51 AM · cards frech leakes mailist saudi arabia shop shopping sql

Cloud Shopping Site Saudi Arabia +92K Mail List + 80K Cc (Name+Card Number + Expirydate)

Today at 6:51 AM

Hello Scammers
i've Dump data from shopping site From Saudi Arabia 🇸🇦
mail list and Cards Infos

contact me for more infos

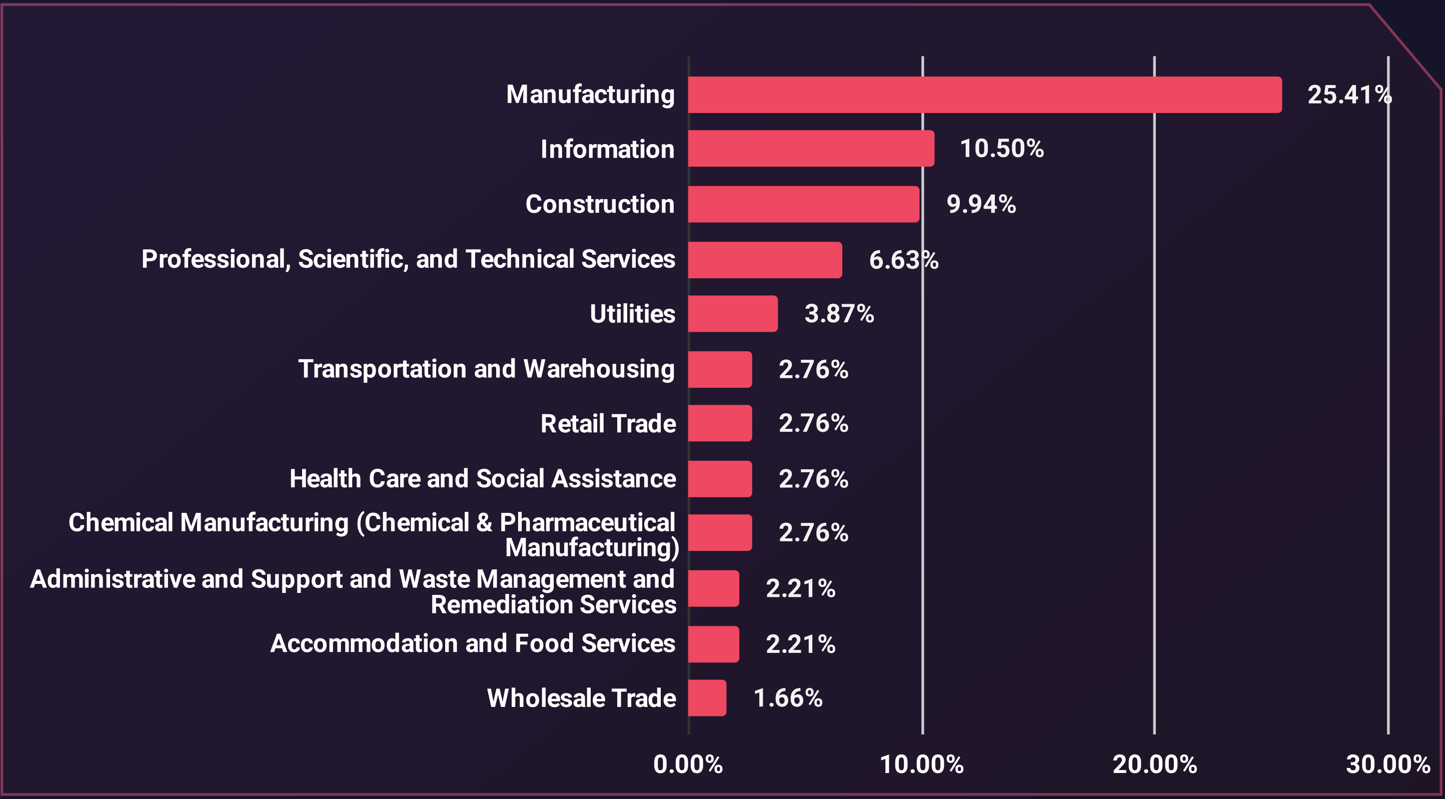
*Screenshot of the forum post - Shopping site Saudi Arabia*

# Ransomware Attacks Targeting Saudi Arabian Entities

Ransomware attacks represent significant threats to organizations, often resulting in dire consequences such as extensive data loss and the exposure of sensitive information. SOCRadar's surveillance has identified 88 ransomware victim notifications attributable to various ransomware threat actors and/or groups.

Manufacturing emerges as the most prominently affected sector among the targeted industries, representing 25.41% of the identified ransomware attacks during this period. Following this, the Information sector accounted for 10.50% of the attacks, while the Construction industry experienced 9.94% of the ransomware incidents.

## Distribution of Ransomware Attacks by Industry

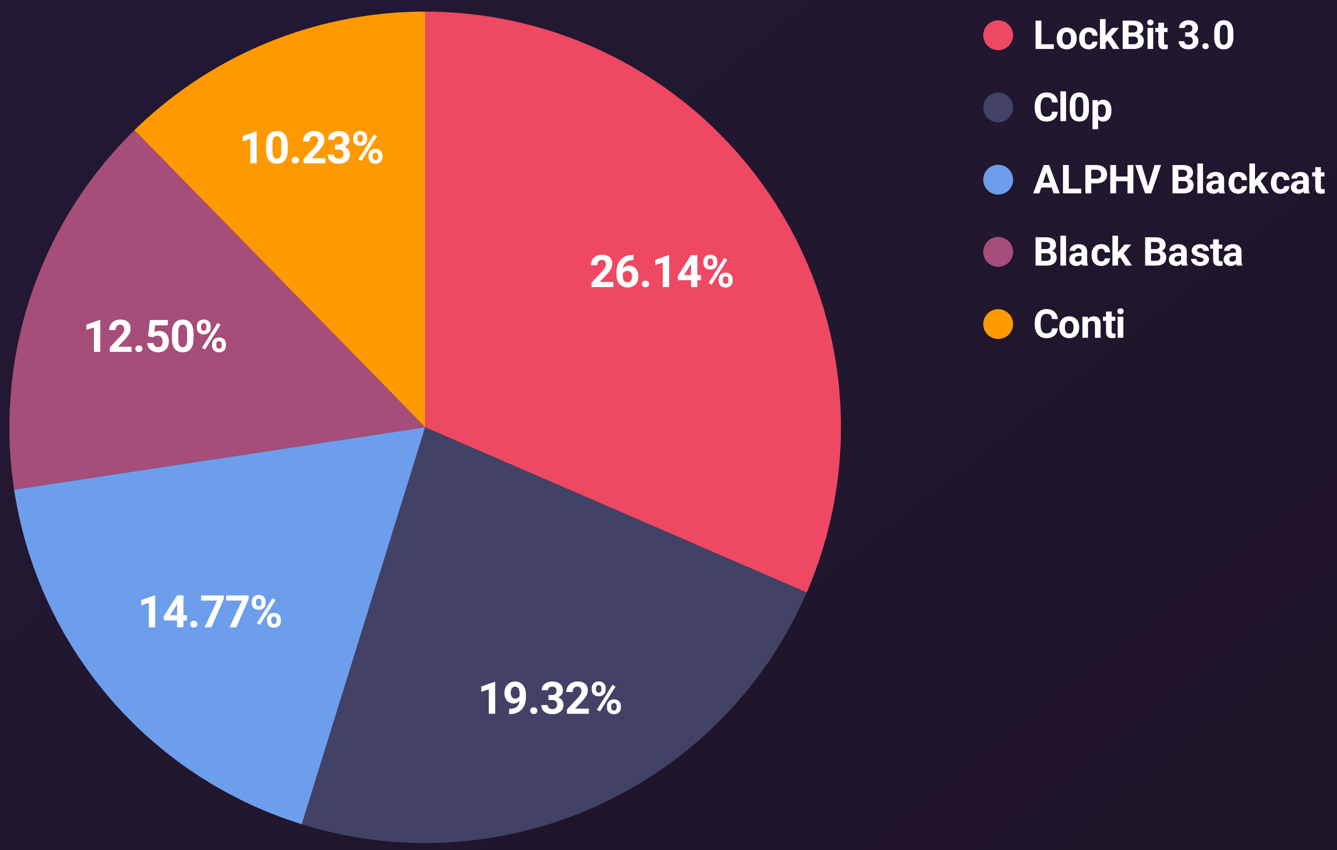


# Top Ransomware Groups Targeting the Nordic Region

When examining the top ransomware groups targeting Saudi Arabia, **LockBit 3.0** emerges as the most prolific threat, accounting for **26.14%** of the attacks. Following this, **Cl0p** represents **19.32%** of the ransomware incidents. **ALPHV BlackCat** accounts for **14.77%,** while **Black Basta** contributes **12.50%.** Lastly, **Conti** accounts for **10.23%** of the ransomware activity.

This analysis highlights the dominant presence of LockBit 3.0, followed by a range of other impactful ransomware groups.

## Top Ransomware Groups Targeting Saudi Arabia

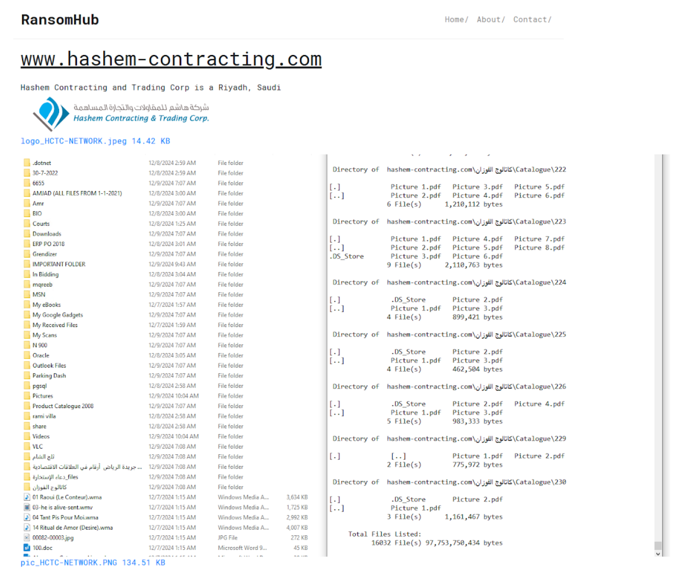


# Recent Ransomware Attacks Targeting Saudi Arabian Entities

## The New Ransomware Victim of ransomhub: www.hashem-contracting.com

13 Dec 2024

SOCRadar's monitoring of the Ransomhub ransomware group website has revealed that Hashem Contracting, a construction and contracting company, has allegedly been listed as a victim. Specializing in project management, engineering, and construction execution, **Hashem Contracting** is known for its commitment to quality and customer satisfaction. Serving various sectors, the company delivers commercial, residential, and infrastructural projects while adhering to industry standards and ensuring timely delivery.



RansomHub

www.hashem-contracting.com

Hashem Contracting and Trading Corp is a Riyadh, Saudi

logo_HCTC-NETWORK.jpeg 14.42 KB

```
.dotnet                                12/8/2024 2:59 AM    File folder
30-7-2022                              12/8/2024 2:59 AM    File folder
6655                                   12/9/2024 7:07 AM    File folder
AMJAD (ALL FILES FROM 1-1-2021)        12/8/2024 3:00 AM    File folder
Amr                                    12/9/2024 7:07 AM    File folder
BIO                                    12/8/2024 3:00 AM    File folder
Courts                                 12/8/2024 1:25 AM    File folder
Downloads                              12/9/2024 7:07 AM    File folder
ERP PO 2018                            12/8/2024 3:01 AM    File folder
Grendizer                              12/9/2024 7:07 AM    File folder
IMPORTANT FOLDER                       12/9/2024 9:43 AM    File folder
In Bidding                             12/8/2024 3:04 AM    File folder
mqreeb                                 12/9/2024 7:07 AM    File folder
MSN                                    12/9/2024 7:07 AM    File folder
My eBooks                              12/7/2024 1:57 AM    File folder
My Google Gadgets                      12/9/2024 7:07 AM    File folder
My Received Files                      12/7/2024 1:59 AM    File folder
My Scans                               12/9/2024 7:07 AM    File folder
N 900                                  12/9/2024 7:07 AM    File folder
Oracle                                 12/8/2024 3:05 AM    File folder
Outlook Files                          12/9/2024 7:07 AM    File folder
Parking Dash                           12/9/2024 7:07 AM    File folder
pgsql                                  12/8/2024 2:58 AM    File folder
Pictures                               12/9/2024 10:04 AM   File folder
Product Catalogue 2008                 12/9/2024 7:07 AM    File folder
rami villa                             12/8/2024 2:58 AM    File folder
share                                  12/8/2024 2:58 AM    File folder
Videos                                 12/9/2024 10:04 AM   File folder
VLC                                    12/9/2024 7:08 AM    File folder
ثلج الشام                               12/9/2024 7:08 AM    File folder
جريدة الرياض  أرقام في العلاقات الاقتصادية ...  12/9/2024 7:08 AM    File folder
دعاء الإستخارة_files                    12/9/2024 7:08 AM    File folder
كاتالوج الفوزان                          12/9/2024 7:08 AM    File folder
01 Raoui (Le Conteur).wma              12/7/2024 1:15 AM    Windows Media A...   3,634 KB
03-he is alive-sent.wmv                12/7/2024 1:15 AM    Windows Media A...   1,725 KB
04 Tant Pis Pour Moi.wma               12/7/2024 1:15 AM    Windows Media A...   2,992 KB
14 Ritual de Amor (Desire).wma         12/7/2024 1:15 AM    Windows Media A...   4,007 KB
00082-00003.jpg                        12/7/2024 1:15 AM    JPG File               272 KB
100.doc                                12/7/2024 1:15 AM    Microsoft Word 9...     45 KB
```

```
 Directory of  hashem-contracting.com\كاتالوج الفوزان\Catalogue\222

[.]            Picture 1.pdf   Picture 3.pdf   Picture 5.pdf
[..]           Picture 2.pdf   Picture 4.pdf   Picture 6.pdf
               6 File(s)      1,210,112 bytes

 Directory of  hashem-contracting.com\كاتالوج الفوزان\Catalogue\223

[.]            Picture 1.pdf   Picture 4.pdf   Picture 7.pdf
[..]           Picture 2.pdf   Picture 5.pdf   Picture 8.pdf
.DS_Store      Picture 3.pdf   Picture 6.pdf
               9 File(s)      2,110,763 bytes

 Directory of  hashem-contracting.com\كاتالوج الفوزان\Catalogue\224

[.]             .DS_Store      Picture 2.pdf
[..]           Picture 1.pdf   Picture 3.pdf
               4 File(s)        899,421 bytes

 Directory of  hashem-contracting.com\كاتالوج الفوزان\Catalogue\225

[.]             .DS_Store      Picture 2.pdf
[..]           Picture 1.pdf   Picture 3.pdf
               4 File(s)        462,504 bytes

 Directory of  hashem-contracting.com\كاتالوج الفوزان\Catalogue\226

[.]             .DS_Store      Picture 2.pdf   Picture 4.pdf
[..]           Picture 1.pdf   Picture 3.pdf
               5 File(s)        983,333 bytes

 Directory of  hashem-contracting.com\كاتالوج الفوزان\Catalogue\229

[.]             [..]           Picture 1.pdf   Picture 2.pdf
               2 File(s)        775,972 bytes

 Directory of  hashem-contracting.com\كاتالوج الفوزان\Catalogue\230

[.]             .DS_Store      Picture 2.pdf
[..]           Picture 1.pdf
               3 File(s)      1,161,467 bytes

    Total Files Listed:
          16032 File(s) 97,753,750,434 bytes
```

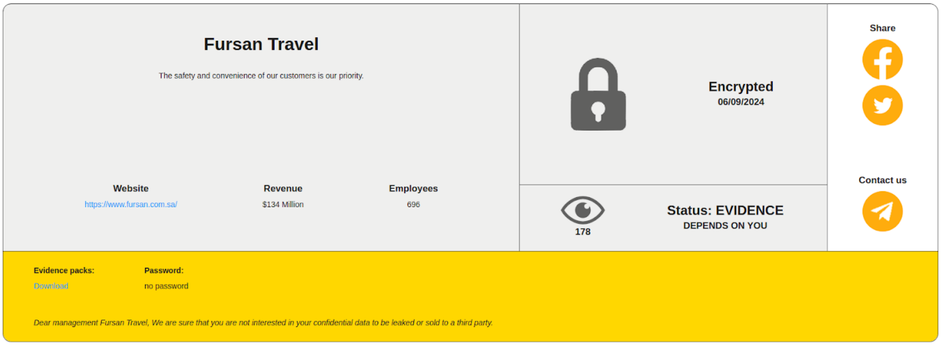
pic_HCTC-NETWORK.PNG 134.51 KB

*Screenshot from ransomhub ransomware group's website*

## The New Ransomware Victim of ransomhouse: Fursan Travel

06 Sep 2024

SOCRadar's monitoring of the ransomhouse ransomware group's website revealed the alleged targeting of Fursan Travel, an unnamed travel agency. The dark web announcement underscores the potential impact on the company and its customers, highlighting the critical importance of safety and convenience.



Fursan Travel

The safety and convenience of our customers is our priority.

| Website | Revenue | Employees |
|---|---|---|
| https://www.fursan.com.sa/ | $134 Million | 696 |

Encrypted
06/09/2024

178

Status: EVIDENCE
DEPENDS ON YOU

Evidence packs: Download

Password: no password

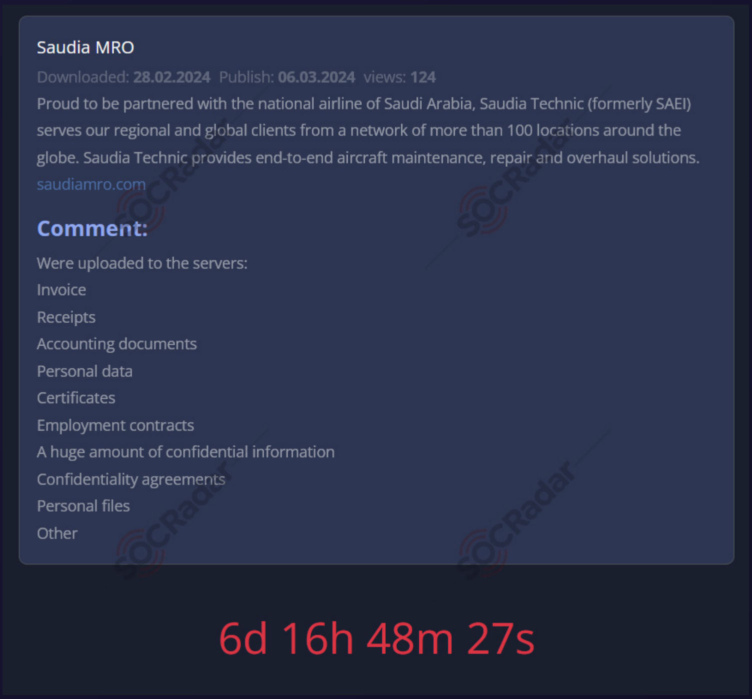
*Dear management Fursan Travel, We are sure that you are not interested in your confidential data to be leaked or sold to a third party.*

*Screenshot from ransomhub ransomware group's website*

## The New Ransomware Victim of 8base: Saudia MRO

28 Feb 2024

> SOCRadar's monitoring of the 8base ransomware group's website revealed the alleged victimization of Saudia MRO, a Saudi Arabian aircraft maintenance company. The ransomware group claims to have stolen and leaked sensitive data, including invoices, accounting documents, personal data, certificates, employment contracts, and other confidential information.



Saudia MRO

Downloaded: **28.02.2024** Publish: **06.03.2024** views: **124**

Proud to be partnered with the national airline of Saudi Arabia, Saudia Technic (formerly SAEI) serves our regional and global clients from a network of more than 100 locations around the globe. Saudia Technic provides end-to-end aircraft maintenance, repair and overhaul solutions.

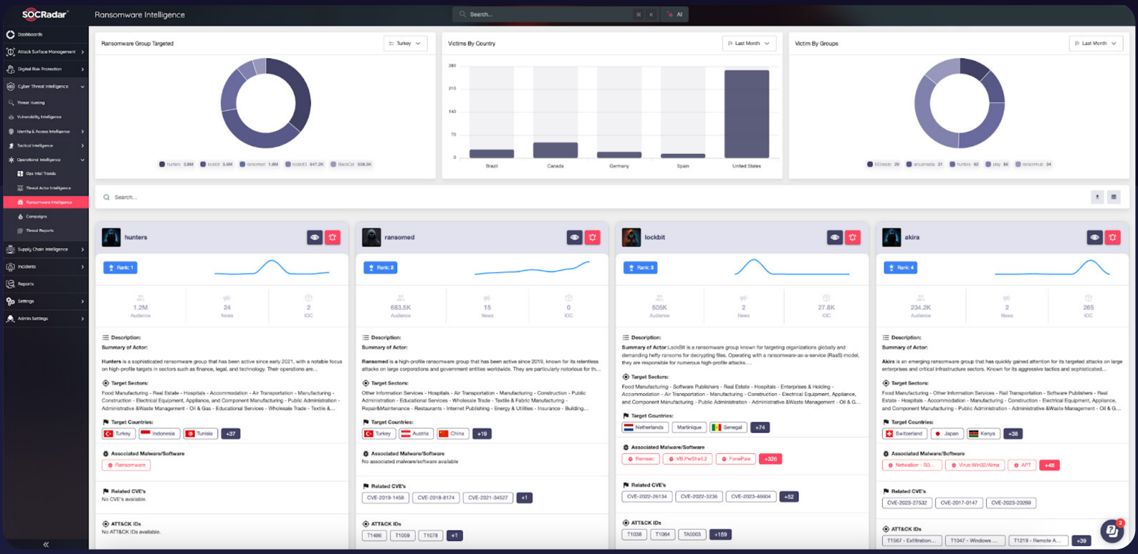
saudiamro.com

**Comment:**

Were uploaded to the servers:
Invoice
Receipts
Accounting documents
Personal data
Certificates
Employment contracts
A huge amount of confidential information
Confidentiality agreements
Personal files
Other

6d 16h 48m 27s

*Screenshot from 8base ransomware group's website*



Explore Ransomware Intelligence Module and gain comprehensive insights with detailed group profiles, MITRE Visualizer, and actionable IOCs. These insights will empower you to stay ahead of evolving threats and enhance your cybersecurity strategy.

# Top Threat Actors Targeting Saudi Arabian Organizations

## Lockbit 3.0 Ransomware Group

LockBit

Country of Origin: Russia

The most successful RaaS group operating since 2019. The group is continuously evolving and is highly active in deploying models such as double-extortion and initial access broker affiliates.

-Ransomware Group-

| | |
|---|---|
| Motivation: | Financial Gain |
| Target Countries: | United States, United Kingdom, Canada, Europe, Thailand, Taiwan |
| Target Sectors: | Manufacturing, Professional Services, IT, Healthcare, Finance, Education, Legal Services |
| Attack Type: | Phishing, RDP and VPN access Exploitation, Ransomware, Data Exfiltration, Double-extortion |

-TTPs-

| | |
|---|---|
| Exploit Public-Facing Application: | T1190 |
| Remote Desktop Protocol: | T1021.001 |
| Data Encrypted for Impact: | T1486 |

LockBit 3.0, a successor to LockBit and LockBit 2.0, operates as a Ransomware-as-a-Service (RaaS) group. Since January 2020, LockBit has shifted to an affiliate-based model, employing various tactics to target businesses and critical infrastructure organizations. They are known for employing strategies like double extortion and initial access broker affiliates, recruiting insiders, and hosting hacker recruitment contests.

With over 1,500 victim announcements on the SOCRadar platform, LockBit emerged as the most active ransomware group in 2022 following Conti's shutdown. As of the first quarter of 2023, they remain the most prolific group, boasting over 300 announced victims.

You can visit our blog post for more detailed Lockbit 3.0 Ransomware Group information.

# Cl0p Ransomware Group

Country of Origin: Russia

A Ransomware group that has been active since 2019 and currently brings up its name by exploiting zero-day vulnerabilities that existed in GoAnyWhere MFT and MOVEit MFT software.

-Ransomware Group-

| | |
|---|---|
| Motivation: | Financial Gain |
| Target Countries: | The US, Canada, The UK, Australia, Colombia, Sweden, Germany, India, Mexico, Turkey |
| Target Sectors: | IT, Healthcare, Finance, Professional Services, Retail, Media, Telecommunication |
| Attack Type: | Spearphishing, Zero-Day Exploitation, Compromised RDP, Ransomware, Data exfiltration, Double-extortion |

-TTPs-

| | |
|---|---|
| Exploit Public-Facing Application: | T1190 |
| Exploitation for Privilege Escalation: | T1068 |
| Exfiltration Over C2 Channel: | T1041 |

Cl0p is a cybercriminal entity recognized for its sophisticated extortion tactics and widespread dissemination of malware across the globe. The word “clop” comes from the Russian word “klop,” which means “bed bug,” a Cimex-like insect that feeds on human blood at night (mosquito). A distinguishing feature of Cl0p is the string “Don’t Worry C|0P” found in the ransom notes.

With a track record of extorting over $500 million in ransom payments, the group focuses on major organizations on a global scale. Gaining infamy in 2019, the Cl0p ransomware group has executed notable attacks, employing extensive phishing initiatives and advanced malware to breach networks and coerce ransom payments. The group leverages the threat of data exposure if demands remain unmet.

You can visit our **blog post** for more detailed Cl0p Ransomware Group information.

# ALPHV Blackcat Ransomware Group

Country of Origin: Russia

BlackCat, or ALPHV, is a ransomware group known for being the pioneer to use Rust and the group first announced its RaaS affiliate program in a dark web forum in December 2021.

-Ransomware Group-

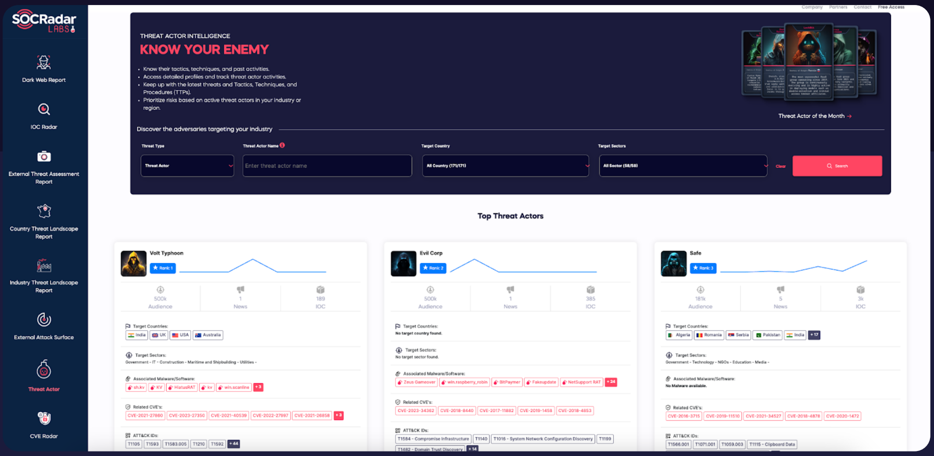
| | |
|---|---|
| Motivation: | Financial Gain |
| Target Countries: | United States, United Kingdom, Canada, Germany, Australia, France, Italy, Spain |
| Target Sectors: | Professional Services, Manufacturing, Healthcare, Finance, Information Technology |
| Attack Type: | Spearphishing, Stolen Credentials, RaaS, Ransomware, Triple-Extortion |

-TTPs-

| | |
|---|---|
| User Execution: Malicious File: | T1204.002 |
| Defacement: | T1491 |
| Data Encrypted for Impact: | T1486 |

BlackCat, or ALPHV, is a ransomware group known for being the first to successfully use Rust—a cross-platform programming language that allows for easy malware customization for different operating systems, such as Windows and Linux. The group has been able to evade detection and successfully encrypt their victims' files by using Rust, which allows them to target multiple operating systems and bypass security controls not designed to analyze malware written in Rust.

You can visit our blog post for more detailed information about the ALPHV BlackCat Ransomware Group.



THREAT ACTOR INTELLIGENCE

KNOW YOUR ENEMY

- Know their tactics, techniques, and past activities.
- Access detailed profiles and track threat actor activities.
- Keep up with the latest threats and Tactics, Techniques, and Procedures (TTPs).
- Prioritize risks based on active threat actors in your industry or region.

Discover the adversaries targeting your industry

Threat Type: Threat Actor
Threat Actor Name: Enter threat actor name
Target Country: All Country (171/171)
Target Sectors: All Sector (58/58)

Top Threat Actors

Volt Typhoon
Rank: 1
500k Audience · 1 News · 189 IOC
Target Countries: India UK USA Australia
Target Sectors: Government - IT - Construction - Maritime and Shipbuilding - Utilities -
Associated Malware/Software: sh.kv KV HiatusRAT kv win.scanline +3
Related CVE's: CVE-2021-27860 CVE-2023-27350 CVE-2021-40539 CVE-2022-27997 CVE-2021-26858 +3
ATT&CK IDs: T1105 T1593 T1583.005 T1210 T1592 +44

Evil Corp
Rank: 2
500k Audience · 1 News · 385 IOC
Target Countries: No target country found.
Target Sectors: No target sector found.
Associated Malware/Software: Zeus Gameover win.raspberry_robin BitPaymer Fakeupdate NetSupport RAT +24
Related CVE's: CVE-2023-34362 CVE-2018-8440 CVE-2017-11882 CVE-2019-1458 CVE-2018-4853
ATT&CK IDs: T1584 - Compromise Infrastructure T1140 T1016 - System Network Configuration Discovery T1199 T1482 - Domain Trust Discovery +14

Safe
Rank: 3
181k Audience · 5 News · 3k IOC
Target Countries: Algeria Romania Serbia Pakistan India +17
Target Sectors: Government - Technology - NGOs - Education - Media -
Associated Malware/Software: No Malware available.
Related CVE's: CVE-2016-3715 CVE-2019-11510 CVE-2021-34527 CVE-2018-4878 CVE-2020-1472
ATT&CK IDs: T1566.001 T1071.001 T1059.003 T1115 - Clipboard Data

SOCRadar enhances cybersecurity measures with its Threat Actor Intelligence Module, which features advanced Threat Actor Tracking capabilities for organizations that want to stay ahead of cyber threats in real time.

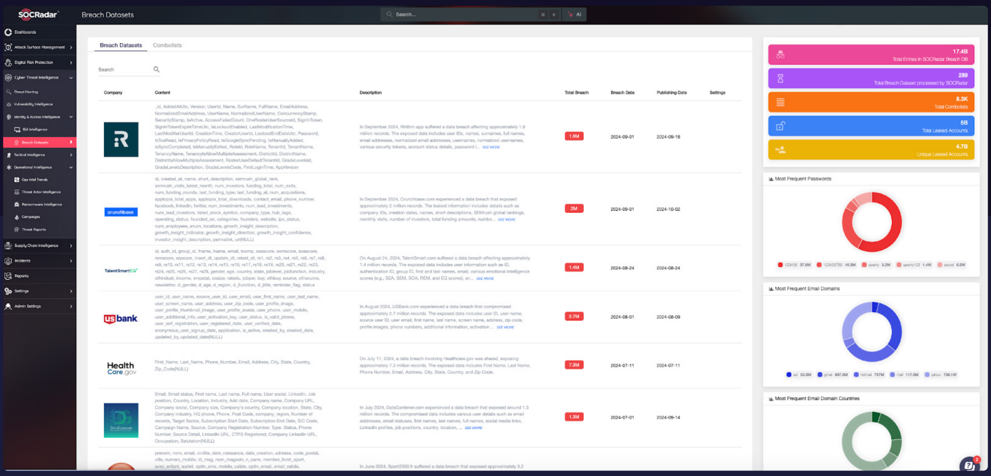
# Stealer Log Statistics

## Top Domains in Saudi Arabia

Throughout 2024, thousands of users' user IDs/email addresses, passwords, credit card data, password hashes, and victim IP address information were compromised via Stealer Logs from users' computers with accounts or access to some of the highest traffic domains in Saudi Arabia.

The table below lists the domains that receive the highest traffic from Saudi Arabia.

| |
|---|
| amazon.sa |
| absher.sa |
| iam.gov.sa |
| haraj.com.sa |
| madrasati.sa |
| timesprayer.sa |
| moe.gov.sa |
| nahdionline.sa |
| altibbi.sa |
| my.gov.sa |

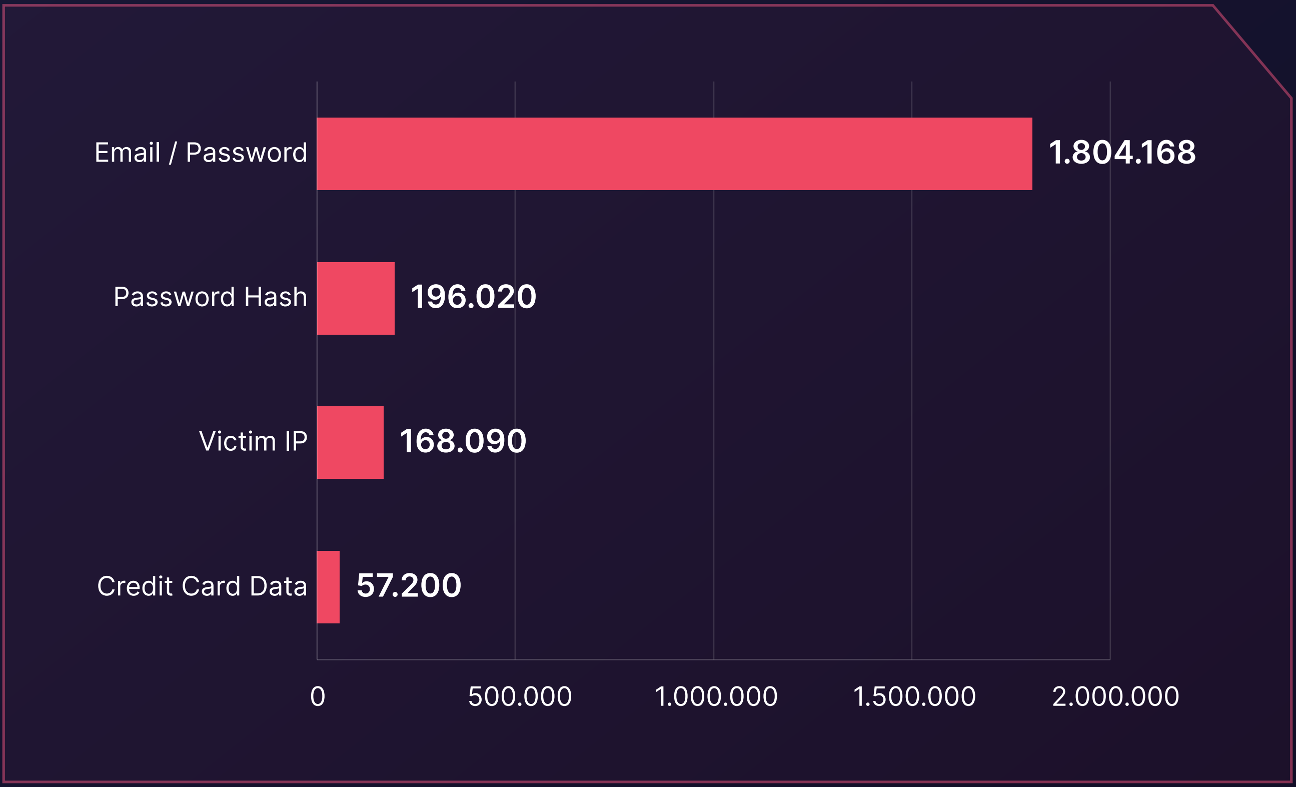


| Company | Content | Description | Total Breach | Breach Date | Publishing Date | Settings |
|---|---|---|---|---|---|---|
| R | _id, AddedAtUtc, Version, UserId, Name, SurName, FullName, EmailAddress, NormalizedEmailAddress, UserName, NormalizedUserName, ConcurrencyStamp, SecurityStamp, IsActive, AccessFailedCount, OneRosterUserSourceId, SignInToken, SignInTokenExpireTimeUtc, IsLockoutEnabled, LastModificationTime, LastModifierUserId, CreationTime, CreatorUserId, LockoutEndDateUtc, Password, IsToaRead, IsPrivacyPolicyRead, IsGoogleSyncPending, IsManuallyAdded, IsSyncCompleted, IsManuallyEdited, RoleId, RoleName, TenantId, TenantName, TenancyName, TenancyIsAllowMultipleAssessment, DistrictId, DistrictName, DistrictIsAllowMultipleAssessment, RosterUserDefaultTenantId, GradeLevelsId, GradeLevelsDescription, GradeLevelsCode, FirstLoginTime, AppVersion | In September 2024, Rhithm.app suffered a data breach affecting approximately 1.9 million records. The exposed data includes user IDs, names, surnames, full names, email addresses, normalized email addresses, usernames, normalized usernames, various security tokens, account status details, password i... SEE MORE | 1.9M | 2024-09-01 | 2024-09-18 | |
| crunchbase | id, created_at, name, short_description, semrush_global_rank, semrush_visits_latest_month, num_investors, funding_total, num_exits, num_funding_rounds, last_funding_type, last_funding_at, num_acquisitions, apptopia_total_apps, apptopia_total_downloads, contact_email, phone_number, facebook, linkedin, twitter, num_investments, num_lead_investments, num_lead_investors, listed_stock_symbol, company_type, hub_tags, operating_status, founded_on, categories, founders, website, ipo_status, num_employees_enum, locations, growth_insight_description, growth_insight_indicator, growth_insight_direction, growth_insight_confidence, investor_insight_description, permalink, url(NULL) | In September 2024, Crunchbase.com experienced a data breach that exposed approximately 2 million records. The leaked information includes details such as company IDs, creation dates, names, short descriptions, SEMrush global rankings, monthly visits, number of investors, total funding amounts, numbe... SEE MORE | 2M | 2024-09-01 | 2024-10-02 | |
| TalentSmartEQ | id, auth_id, group_id, fname, lname, email, tcomp, seascore, semscore, soascore, remscore, eqscore, insert_dt, update_dt, retest_dt, rs1, rs2, rs3, rs4, rs5, rs6, rs7, rs8, rs9, rs10, rs11, rs12, rs13, rs14, rs15, rs16, rs17, rs18, rs19, rs20, rs21, rs22, rs23, rs24, rs25, rs26, rs27, rs28, gender, age, country, state, joblevel, jobfunction, industry, othindust, income, empstat, cosize, ratedu, jobper, buy, othbuy, source, othsource, newsletter, d_gender, d_age, d_region, d_function, d_jtitle, reminder_flag, status | On August 24, 2024, TalentSmart.com suffered a data breach affecting approximately 1.4 million records. The exposed data includes user information such as ID, authentication ID, group ID, first and last names, email, various emotional intelligence scores (e.g., SEA, SEM, SOA, REM, and EQ scores), an... SEE MORE | 1.4M | 2024-08-24 | 2024-08-24 | |
| usbank | user_id, user_name, source_user_id, user_email, user_first_name, user_last_name, user_screen_name, user_address, user_zip_code, user_profile_image, user_profile_thumbnail_image, user_profile_avatar, user_phone, user_mobile, user_additional_info, user_activation_key, user_status, is_valid_phone, user_self_registration, user_registered_date, user_verified_date, anonymous_user_signup_date, application, is_active, created_by, created_date, updated_by, updated_date(NULL) | In August 2024, USBank.com experienced a data breach that compromised approximately 2.7 million records. The exposed data includes user ID, user name, source user ID, user email, first name, last name, screen name, address, zip code, profile images, phone numbers, additional information, activation ... SEE MORE | 2.7M | 2024-08-01 | 2024-08-09 | |
| HealthCare.gov | First_Name, Last_Name, Phone_Number, Email, Address, City, State, Country, Zip_Code(NULL) | On July 11, 2024, a data breach involving Healthcare.gov was shared, exposing approximately 7.3 million records. The exposed data includes First Name, Last Name, Phone Number, Email, Address, City, State, Country, and Zip Code. | 7.3M | 2024-07-11 | 2024-07-11 | |
| DataGardener | Email, Email status, First name, Last name, Full name, User social, LinkedIn, Job position, Country, Location, Industry, Add date, Company name, Company URL, Company social, Company size, Company's country, Company location, State, City, Company industry, HQ phone, Phone, Post Code, company_region, Number of records, Target Sector, Subscription Start Date, Subscription End Date, SIC Code, Campaign Name, Source, Company Registration Number, Type, Status, Phone Number, Source Detail, LinkedIn URL, CTPS Registered, Company LinkedIn URL, Occupation, Salutation(NULL) | In July 2024, DataGardener.com experienced a data breach that exposed around 1.3 million records. The compromised data includes various user details such as email addresses, email statuses, first names, last names, full names, social media links, LinkedIn profiles, job positions, country, location, ... SEE MORE | 1.3M | 2024-07-01 | 2024-09-14 | |
| | prenom, nom, email, civilite, date_naissance, date_creation, adresse, code_postal, ville, numero_mobile, id_mag, nom_magasin, n_carte, membre_livret_sport, avec_enfant, wallet, optin_sms, mobile_valide, optin_email, email_valide, | In June 2024, Sport2000.fr suffered a data breach that exposed approximately 3.2 | | | | |

**SOCRadar's Identity & Access Intelligence Module** can detect stealers on your devices and identify their location, facilitating a secure working environment. Changing passwords without eliminating stealers is insufficient to secure your organization, as it will only provide new passwords to threat actors.

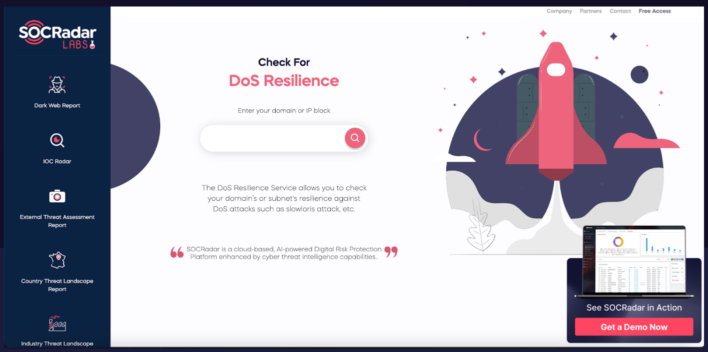
The graph below displays the distribution of compromised user data obtained through Stealer Logs across the domains with the highest traffic from Saudi Arabia.

## Stealer Logs - Distribution of the Compromised Data



The data reveals significant dissemination of compromised information, including **1,804,168 email/password combinations**, **196,020 password hashes**, **168,090 compromised victim IPs**, and **57,200 credit card data entries**, each representing significant instances of compromise.

These discoveries emphasize the gravity of data compromises that impact users, highlighting the urgent need for robust cybersecurity protocols to mitigate such risks efficiently.



The DoS Resilience Service allows you to check your domain's or subnet's resilience against DoS attacks such as slowloris attack, etc.

“SOCRadar is a cloud-based, AI-powered Digital Risk Protection Platform enhanced by cyber threat intelligence capabilities..”

Enhance your DDoS defense with **SOCRadar's DoS Resilience Free Tool**. Our Free DoS Resilience Service allows you to check your domain’s or subnet's resilience against DoS attacks, such as slow loris attacks.

## DDoS Attack Statistics

Saudi Arabia experienced a dynamic DDoS threat landscape marked by considerable cyber activity in 2024.

- The most extensive multi-vector DDoS attack recorded encompassed **26 vectors**, featuring prevalent techniques such as **CLDAP Amplification and COAP Amplification attacks.**
- The maximum bandwidth observed during a DDoS attack reached **2 Tbps** (peak aggregate bandwidth in one minute), indicating the severe capacity of these cyber threats.
- The highest recorded throughput during these incidents was **154 Mpps** (peak aggregate throughput in one minute), underscoring the intense rate at which data packets were sent.
- Each DDoS attack lasted **12.04 minutes** on average, indicating a strategy focused on medium-duration but high-frequency service disruptions.
- **278,324 DDoS attacks** were recorded throughout the year, illustrating the high frequency of cyber-attacks aimed at Saudi Arabian targets.

| Attack Vector | Number of Attacks in 2024 |
|---|---|
| TCP ACK | 135,684 |
| TCP SYN/ACK | 47,677 |
| DNS Amplification | 37,490 |
| ICMP | 27,393 |
| TCP RST | 18,398 |

The ongoing evolution of DDoS tactics underscores the importance of implementing stringent monitoring and resilient defense mechanisms to safeguard essential infrastructures and ensure uninterrupted service delivery.

# Lessons Learned: Key Insights and Strategic Recommendations

Several critical insights have emerged in assessing the cybersecurity challenges faced by organizations in Saudi Arabia. These findings and SOCRadar's capabilities offer a strategic pathway to enhance cyber resilience and safeguard operational continuity. Below are the key takeaways from our analysis:

### Adapting to an Evolving Cyber Threat Landscape

The constantly shifting cyber threat landscape, characterized by rising Dark Web activity and ransomware attacks targeting Saudi Arabia, calls for heightened vigilance. Organizations must evolve their security strategies to stay ahead of emerging threats. By leveraging **SOCRadar's Extended Threat Intelligence solution**, businesses can obtain real-time threat insights and proactively counter cyber adversaries.

### Multi-layered Security Defenses

The broad range of industries targeted by cyber threats necessitates implementing comprehensive, multi-layered security measures. SOCRadar supports these initiatives with its proactive **Threat Intelligence** and **Advanced Dark Web Monitoring** services, ensuring organizations are well-protected across various threats.

### Addressing Ransomware Threats

Ransomware remains a significant threat, emphasizing the importance of robust defensive and responsive strategies. **SOCRadar's Attack Surface Management** capabilities enable businesses to identify potential ransomware vulnerabilities and develop effective countermeasures.

### Strengthening Defenses Against Stealer Malware

Saudi Arabia remains a frequent target of stealer malware, making enhanced defenses against this threat crucial. SOCRadar’s Identity & Access Intelligence Module is vital in detecting and mitigating data breach risks, strengthening the overall security posture.

### Mitigating DDoS Attacks

With the increasing complexity of Distributed Denial of Service (DDoS) attacks, organizations must prioritize robust mitigation strategies. Deploying advanced DDoS protection technologies to absorb high-volume traffic and counter multi-vector attacks is essential. SOCRadar's DoS Resilience Free Tool offers a sophisticated solution to assess and strengthen infrastructure against these threats, utilizing AI and cloud technologies for optimal protection.

## SOCRadar’s Recommendations: Proactive Strategies for Threat Detection, Dark Web Monitoring, and Brand Protection

- Adopting a proactive and comprehensive cybersecurity approach is crucial for Saudi Arabian organizations.
- Partnering with advanced solutions like SOCRadar enhances defenses and helps navigate the evolving cyber threat landscape.
- Building a culture of risk awareness and implementing proactive mitigation strategies fortifies defenses against dynamic threats.
- Utilizing Cyber Threat Intelligence (CTI) empowers teams to respond to immediate threats and confidently prepare for future challenges.
- Collaboration among cybersecurity professionals, supported by robust CTI frameworks, is essential for safeguarding digital assets and maintaining organizational resilience against cyber threats.

By adopting these recommendations, organizations can significantly improve their cyber defense capabilities and navigate the complexities of today’s threat landscape.

# Who is SOCRadar®?

Your Eyes Beyond

SOCRadar provides Extended Threat Intelligence (XTI) that combines: **"Cyber Threat Intelligence, Brand Protection, External Attack Surface Management, and Dark Web Radar Services."** SOCRadar provides the actionable and timely intelligence context you need to manage the risks in the transformation era.

**Trusted by**
**21.000+ companies**
**in 150+ countries**

**Dark Web Monitoring:** SOCRadar's fusion of its unique Dark Web recon technology with the human analyst eye further provides in-depth insights into financially-targeted APT groups and the threat landscape.

**Protecting Customers' PII:** Scan millions of data points on the surface, deep and Dark Web to accurately identify the leakage of your customers' Personally Identifiable Information (PII) in compliance with regulations.

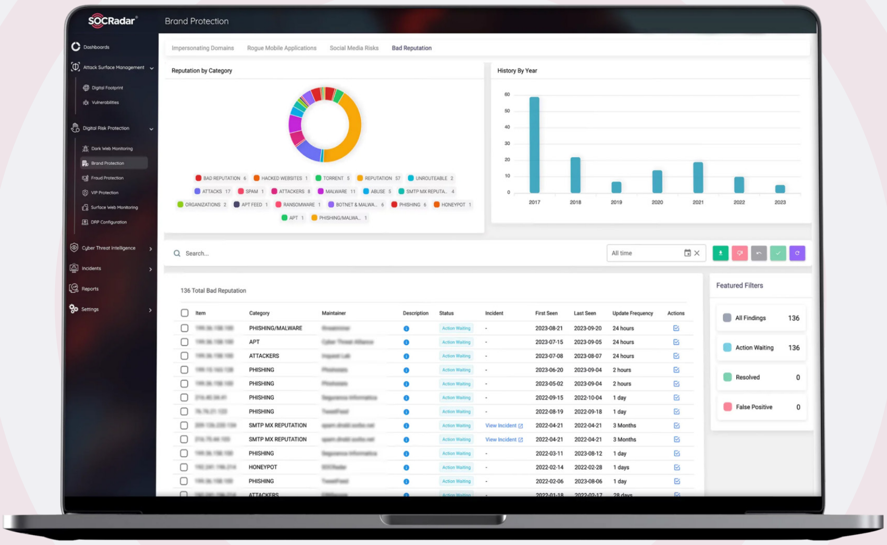
**Credit Card Monitoring:** Enhance your fraud detection mechanisms with automation speed by identifying stolen credit card data on popular global black markets, carding forums, social channels, and chatters.

**360-Degree Visibility:** Achieve digital resilience by maintaining internet-facing digital asset inventory. Significantly accelerate this process by automated discovery, mapping, and continuous asset monitoring.

**GET ACCESS FOR FREE**

## START YOUR FREE TRIAL

Discover SOCRadar's powerful tools and easy-to-use interface to enhance cyber threat intelligence efforts. Schedule a demo with our experts to see it in action, and we'll show you what SOCRadar can do.



136 Total Bad Reputation

| ☐ | Item | Category | Maintainer | Description | Status | Incident | First Seen | Last Seen | Update Frequency | Actions |
|---|---|---|---|---|---|---|---|---|---|---|
| ☐ | [redacted] | PHISHING/MALWARE | [redacted] | ● | Action Waiting | - | 2023-08-21 | 2023-09-20 | 24 hours | ☑ |
| ☐ | [redacted] | APT | [redacted] | ● | Action Waiting | - | 2023-07-15 | 2023-09-05 | 24 hours | ☑ |
| ☐ | [redacted] | ATTACKERS | [redacted] | ● | Action Waiting | - | 2023-07-08 | 2023-08-07 | 24 hours | ☑ |
| ☐ | [redacted] | PHISHING | [redacted] | ● | Action Waiting | - | 2023-06-20 | 2023-09-04 | 2 hours | ☑ |
| ☐ | [redacted] | PHISHING | [redacted] | ● | Action Waiting | - | 2023-05-02 | 2023-09-04 | 2 hours | ☑ |
| ☐ | [redacted] | PHISHING | [redacted] | ● | Action Waiting | - | 2022-09-15 | 2022-10-04 | 1 day | ☑ |
| ☐ | [redacted] | PHISHING | [redacted] | ● | Action Waiting | - | 2022-08-19 | 2022-09-18 | 1 day | ☑ |
| ☐ | [redacted] | SMTP MX REPUTATION | [redacted] | ● | Action Waiting | View Incident | 2022-04-21 | 2022-04-21 | 3 Months | ☑ |
| ☐ | [redacted] | SMTP MX REPUTATION | [redacted] | ● | Action Waiting | View Incident | 2022-04-21 | 2022-04-21 | 3 Months | ☑ |
| ☐ | [redacted] | PHISHING | [redacted] | ● | Action Waiting | - | 2022-03-11 | 2023-08-12 | 1 day | ☑ |
| ☐ | [redacted] | HONEYPOT | [redacted] | ● | Action Waiting | - | 2022-02-14 | 2022-02-28 | 1 days | ☑ |
| ☐ | [redacted] | PHISHING | [redacted] | ● | Action Waiting | - | 2022-02-06 | 2023-08-06 | 1 day | ☑ |
| ☐ | [redacted] | ATTACKERS | [redacted] | ● | Action Waiting | - | 2022-01-18 | 2022-02-17 | 28 days | ☑ |

Featured Filters

| | |
|---|---|
| All Findings | 136 |
| Action Waiting | 136 |
| Resolved | 0 |
| False Positive | 0 |

**Start Your Free Trial**

SOCRadar®

Your Eyes Beyond

**SOCRadar HQ**
HQ Office: 254 Chapman Rd, Ste
208 Newark, Delaware 19702 USA

**Call**
+1 (571) 249-4598

**Email**
info@socradar.io

socradar.io

Virtual Addresses

**London, UK**
167 City Road Old Street,
London EC1V 1AW

**Dubai, UAE**
8W building 5th Floor,
DAFZA, Dubai

**São Paulo, Brasil**
7th & 8th Floors Torre
Joao Salem, Av. Paulista
1079 São Paulo

**Bangalore, India**
The Estate, 8th Floor
Dickenson Road 560042
Bangalore Karnataka