

THREAT LANDSCAPE REPORT

SAUDI ARABIA 2025

© 2025 Cyble Inc. All rights reserved.

Table of **Content**

Executive Summary 3

Initial Accesses on Sale 4

Notable Accesses on Sale 6
- Threat Actor Advertises Network Access to a University 6
- Threat Actor Claims Unauthorized Access to Government Department 7
- Yemen Cyber Army Claims Unverified Breach of Saudi Oil Sector Vendors 7
- Alleged Network Access to Transport Department Publicized for Sale 8
- Alleged Official Government Email Account Publicized for Sale 8

Data Breaches and Leaks 9
- Analysis of the Overall Threat Activity 9

Notable Data Breaches and Leaks 11
- Threat Actor Selling Alleged Data from Four Saudi Organizations 11
- RansomHouse Claims Attack on Saudi Lubricant Manufacturer 11
- Database of Saudi Dairy Giant Advertised For Sale 13
- Threat Actor Leaks Database of Saudi Coffee Retailer 13
- Alleged Database of Saudi Engineering Firm Leaked Online 13

Ransomware Attacks 14

Hacktivism 17
- لواء محمد ﷺ 17
- Laneh | Dark 17
- Cyber Bulletin 18
- Holy league 18
- X Sec 404 TEAM 18

Industry Insights and Analysis 19

Conclusion 21

© 2025 Cyble Inc. All rights reserved.

Executive Summary

Cyble's cyber threat activity report brings to light specific cyber threat activity targeting Saudi Arabia in 2025.

Saudi Arabia faces a multifaceted cyber threat landscape characterized by a high volume of compromised access sales, data breaches, ransomware, and hacktivist operations.

Threat actors disproportionately targeted the IT & ITES, Construction, and Government sectors for initial access sales and data exfiltration, exploiting these entities for supply chain compromises, espionage, and financial gain.

The ransomware ecosystem was highly fragmented yet active, with numerous groups like Ralord and Everest opportunistically deploying multi-extortion attacks against critical industries.

Concurrently, state-aligned actors from China and Iran conducted espionage campaigns, leveraging supply chain attacks against IT providers to infiltrate high-value networks, while a diverse array of hacktivist groups executed geopolitically motivated operations using DDoS attacks and website defacements.

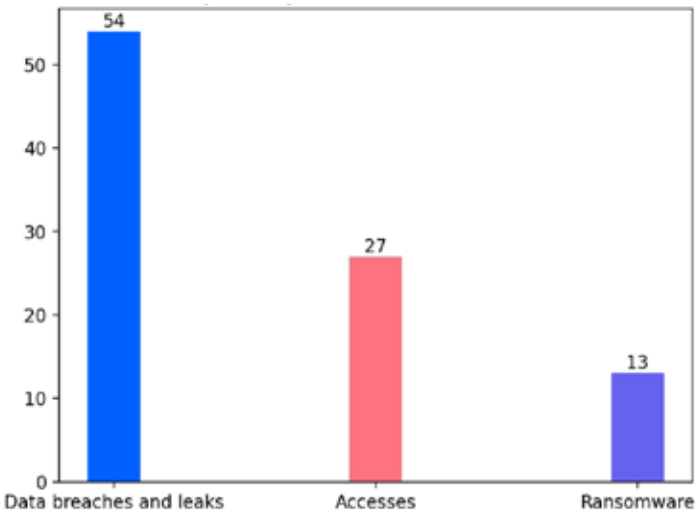


Fig 1: Cybercrime Incidents

This complex environment, marked by a mix of opportunistic cybercriminals, nation-state operators, and ideologically driven groups, demands a comprehensive security posture to defend against persistent threats of data theft, extortion, and operational disruption.

© 2025 Cyble Inc. All rights reserved.

Initial Accesses on Sale

Between January and November 2025, CRIL identified 27 distinct incidents involving the sale of compromised access to organizations in Saudi Arabia.

The IT & ITES sector was the most frequently targeted, with seven incidents, accounting for nearly 26% of the total listings. The Construction industry followed with five observed incidents (18.5%), and Government & Law Enforcement Agencies (LEA) were targeted in three instances (11.1%). Combined, these three sectors represent over 55% of all observed access sales, indicating a concentrated focus by threat actors.

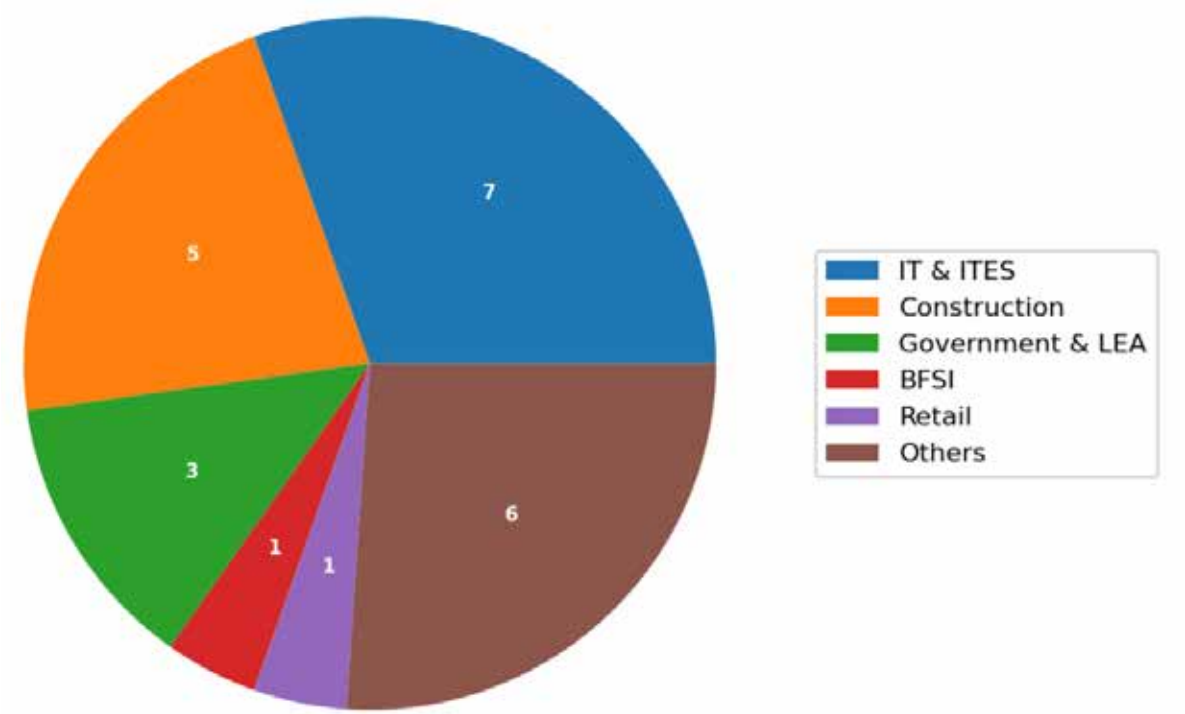


Fig 2: Compromised Accesses Across Saudi Arabian Industries in 2025

The high prevalence of attacks on the IT & ITES sector highlights the risk of supply chain compromises, where initial access could be leveraged to target their extensive client base. Similarly, the focus on Construction and Government entities likely corresponds to their critical

© 2025 Cyble Inc. All rights reserved.

role in national infrastructure and the sensitive project and state data they possess, making them high-value targets for subsequent ransomware or espionage campaigns.

Ultimately, the threat landscape demonstrates that organizations within the IT, Construction, and Government sectors in Saudi Arabia are disproportionately sought after within the compromised access market.

An analysis of threat actor activity within the compromised access market for Saudi Arabia reveals a fragmented landscape. The threat actors dubbed as 'vebxpert' and 'r57' were the most active during the observation period, though each was responsible for only two posts. These two actors collectively accounted for just under 15% of the total access-for-sale listings.

Most of the activity was distributed thinly across more than 20 other distinct threat actors, each advertising a single compromised access. This distribution suggests a market characterized by a wide array of opportunistic, low-volume sellers rather than one dominated by a few established and consistently active players.

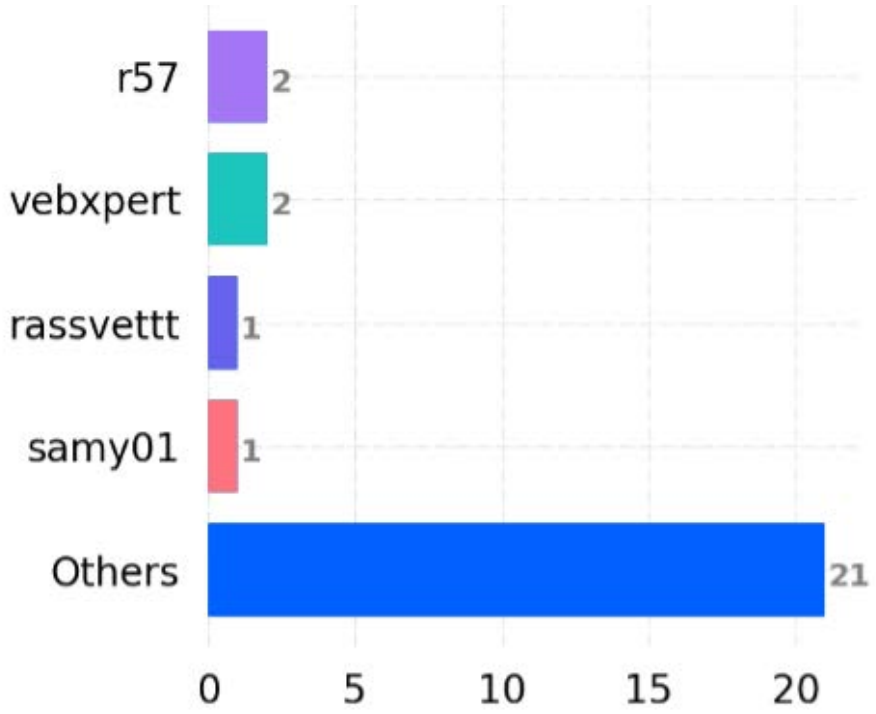


Fig 3: Active Threat Actors Selling Compromised Access

© 2025 Cyble Inc. All rights reserved.

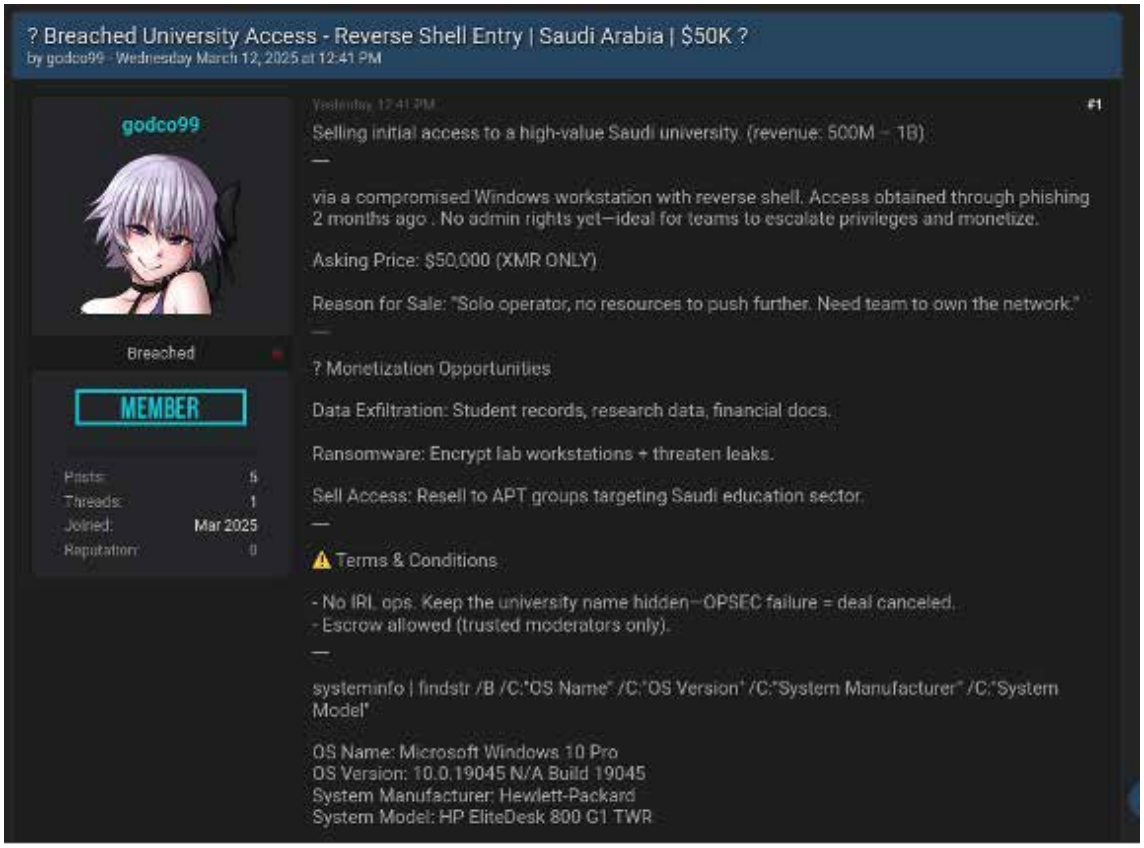
Notable Accesses on Sale

Threat Actor Advertises Network Access to a University

On or around March 12, the threat actor 'godco99' posted an advertisement on the nuovo BreachForums offering backdoor access to an undisclosed university based in Saudi Arabia with reported revenues between 500 million and 1 billion.

The actor claimed to have compromised a Windows workstation via a phishing campaign a couple of months prior, providing access through a reverse shell. The advertisement stated that the access could be used to exfiltrate sensitive information, including student records, research data, and financial documents, or to deploy ransomware.

The threat actor set the price for the access at USD 50,000 and specified Monero (XMR) as the only accepted payment method.



© 2025 Cyble Inc. All rights reserved.

Threat Actor Claims Unauthorized Access to Government Department

On or around July 8, the threat actor going by the name 'eksta' claimed on a dark web forum to have gained unauthorized access to the SSL-VPN portal of a Saudi Arabia ministerial department. According to the actor, this access could be used to manage a wide range of internal systems, including SSH servers, HR and Notaries System, and RDP access. To support this claim, 'eksta' shared a screenshot of an allegedly logged-in Fortinet SSL-VPN portal.

The threat actor also stated they had unsuccessfully attempted to compromise the domain controller and were seeking assistance, with the post suggesting an intent to sell access to interested parties.

Yemen Cyber Army Claims Unverified Breach of Saudi Oil Sector Vendors

In mid-September, the threat group Yemen Cyber Army claimed it had gained access to the CCTV systems of several vendors supplying Oil to a Saudi Oil giant. The group published images and videos purportedly showing scenes from inside these facilities. However, the released media failed to provide a plausible correlation with Saudi oil giant, making the claims dubious. The group's statement positioned the release as a warning and demanded that Saudi Arabia immediately cease its support for rebel forces attacking Yemen.



© 2025 Cyble Inc. All rights reserved.

Alleged Network Access to Transport Department Publicized for Sale

On or around May 23, the threat actor by the name 'shine,' offered unauthorized access allegedly to the country's Transport Department for sale on the English-language cybercrime forum, DarkForums. In the post, the actor claimed that the access was via an SSH key to a Linux-based system. The threat actor did not provide any proof of compromise, and therefore the claims remained unconfirmed.

Alleged Official Government Email Account Publicized for Sale

On or around March 9, the threat actor by the name 'louna' advertised the sale of unauthorized access to an email account belonging to a government official in the Education Department on the nuovo BreachForums. To substantiate their claims, the actor shared multiple screenshots demonstrating access to the compromised inbox. The threat actor listed the access for a price of USD 500 and instructed interested parties to make contact privately.



© 2025 Cyble Inc. All rights reserved.

Data Breaches and Leaks

Analysis of the Overall Threat Activity

CRIL observed 54 data breach and leak incidents impacting Saudi Arabia-based entities in 2025, so far. The Government & Law Enforcement (LEA) sector was the most frequently impacted, with nine incidents representing approximately 17% of the total observed breaches. The Education sector followed as the second most targeted, experiencing six incidents, or 11% of the total.

The persistent targeting of the government sector is likely driven by threat actors seeking to acquire sensitive national security information and citizen Personally Identifiable Information (PII) for espionage or disruptive activities. Similarly, educational institutions remain attractive targets due to their large repositories of student and faculty data, which can be monetized or used in subsequent attacks.

This concentration of incidents highlights a clear focus by threat actors on sectors that serve as centralized hubs for valuable personal and state-related data.

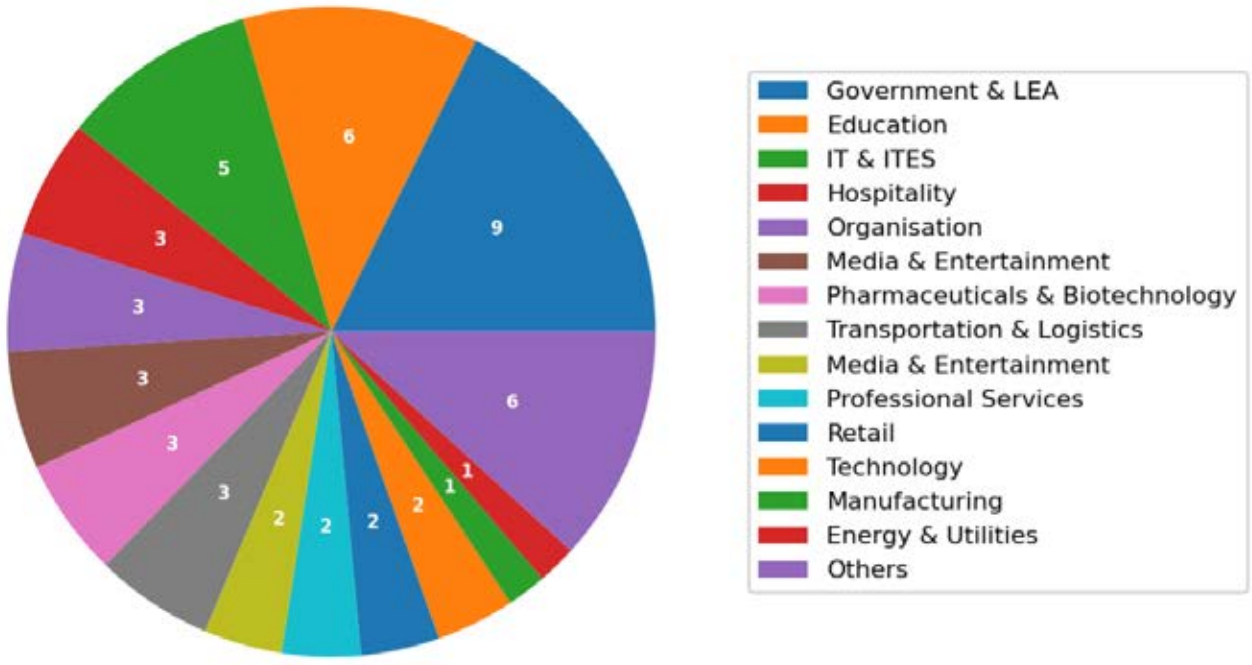


Fig 4: Data Breaches Across Saudi Arabian Industries in 2025

© 2025 Cyble Inc. All rights reserved.

Analysis of threat actor activity reveals a landscape led by a few highly prolific individuals. The threat actors 'zerodayx' and 'bigbrother' were the most prominent, each linked to four distinct data breach incidents targeting the region. The actor 'kazu' was also notably active, with three separate data leak claims.

Below this top tier, a consistent level of activity was maintained by a group of moderately active threat actors—including 'jumbojet,' 'cyber_anonn,' and 'antisocial'. The overall distribution, characterized by a small number of high-volume actors and a long tail of single-post contributors, suggests that while a few persistent threats are a primary concern, the region also faces a broad, opportunistic threat from a diverse range of actors.

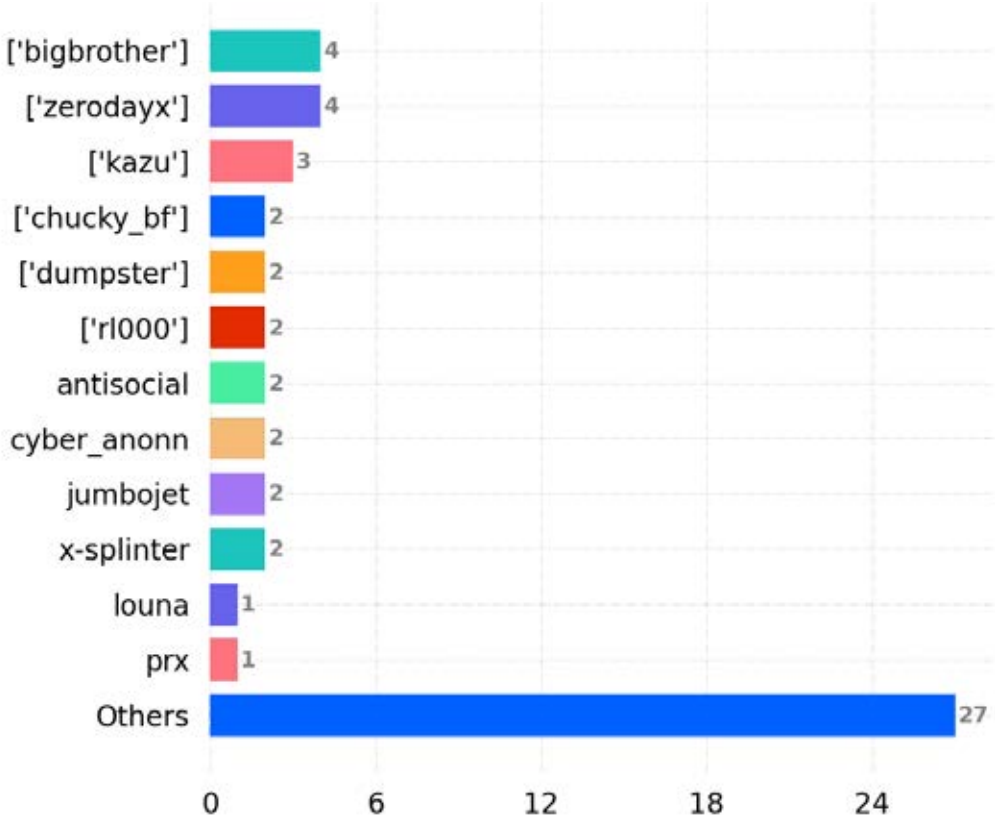


Fig 5: Active Threat Actors Selling Breached Data in 2025

Analysis of the most prominent threat actors reveals highly targeted and temporally concentrated campaigns. The actor 'Cyber_Anonn,' for instance, conducted a brief but focused operation in late Q1 2025, lasting approximately one week. This activity was exclusively directed at the Government and Law Enforcement Agency (LEA) sector within Saudi Arabia.

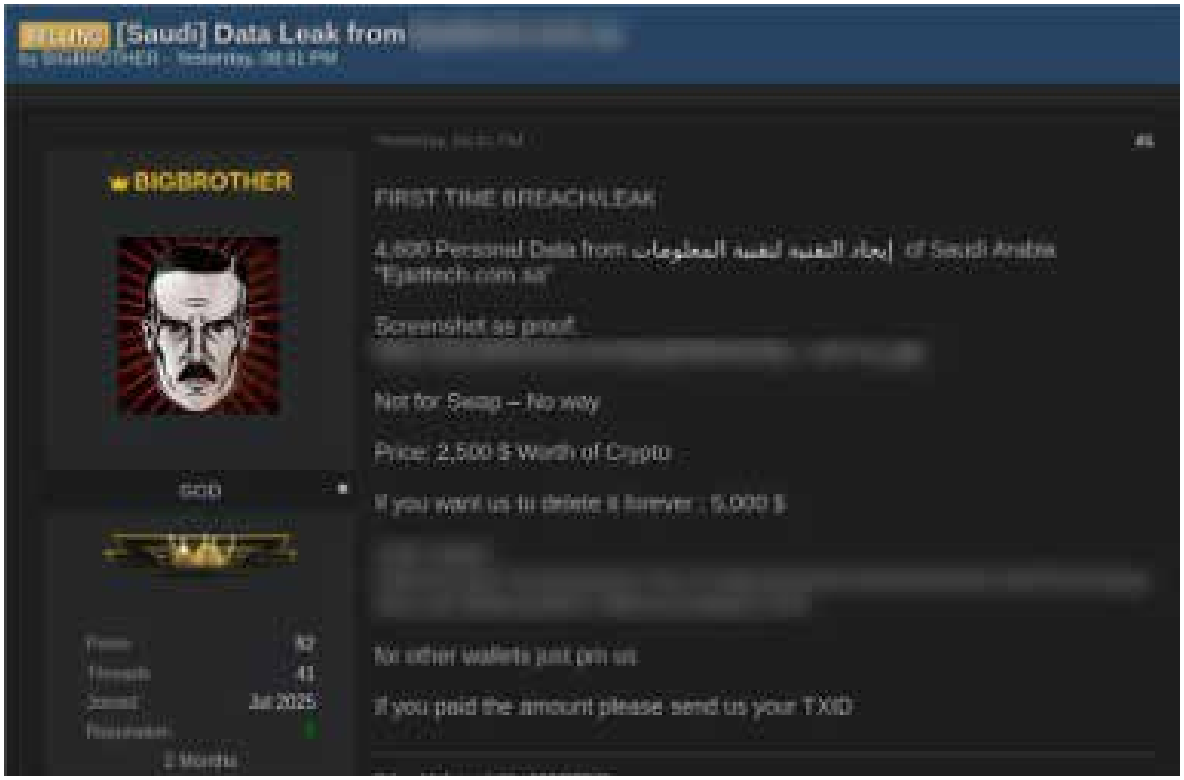
The specific nature of this targeting, both in terms of industry and geography, indicates a deliberate focus on high-value government entities rather than widespread, opportunistic attacks.

© 2025 Cyble Inc. All rights reserved.

Notable Data Breaches and Leaks

Threat Actor Selling Alleged Data from Four Saudi Organizations

In late September, the threat actor known as 'BIGBROTHER' offered datasets for sale on the DarkForums cybercrime platform, allegedly stolen from four organizations in Saudi Arabia. The impacted entities were identified as IT company (4,600 records), an Automobile and Tourism Club (10,000 records), University (2,500 records), and a FinTech (7,217 records). As proof of the breach, the threat actor attached screenshots for each victim, displaying what appeared to be unauthorized access to their respective dashboards.



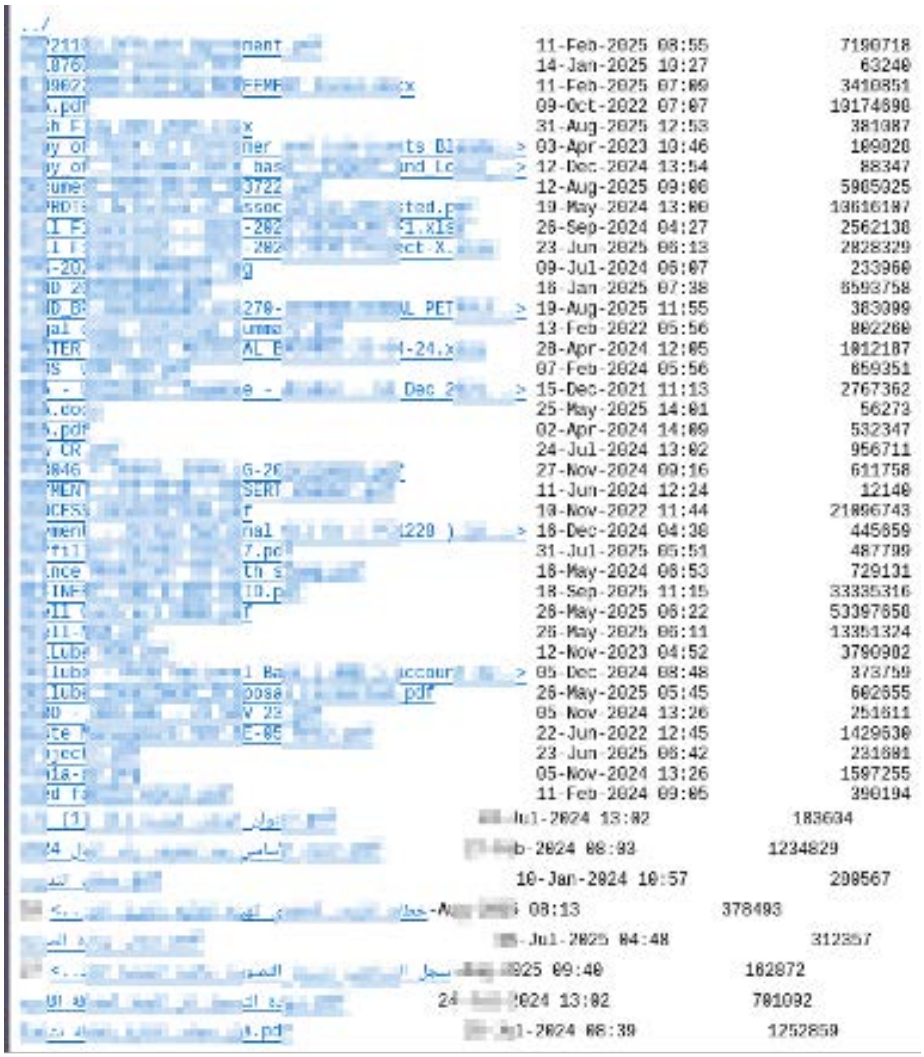
RansomHouse Claims Attack on Saudi Lubricant Manufacturer

Around October 22, 2025, the RansomHouse hacking group claimed responsibility for breaching a lubricant manufacturer and supplier based in Saudi Arabia. To substantiate its claim, the group published a sample of allegedly exfiltrated documents, including financial records, customer

© 2025 Cyble Inc. All rights reserved.

databases, contracts, and internal correspondence dated between 2023 and 2025. At the time of the claim, RansomHouse had not announced a ransom deadline, and the targeted company had not issued a public statement regarding the incident.





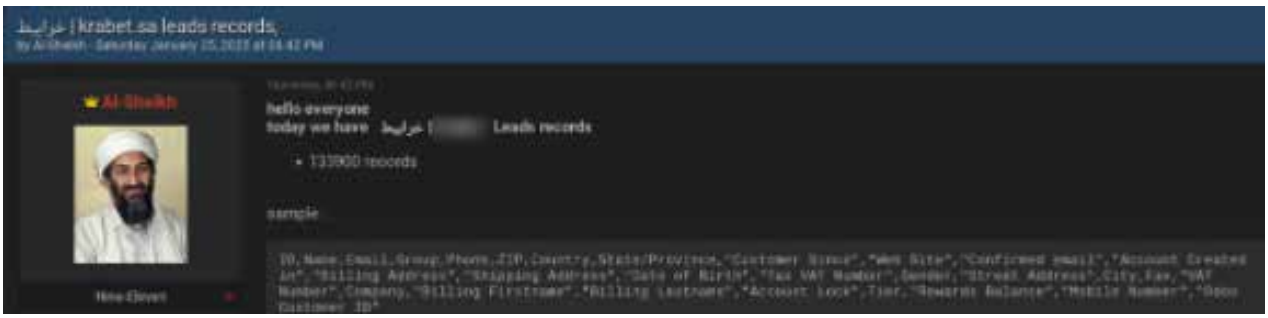
© 2025 Cyble Inc. All rights reserved.

Database of Saudi Dairy Giant Advertised For Sale

On or around June 16, the threat actor 'Satanic' advertised databases allegedly stolen from a dairy company on the DarkForums cybercrime forum. The threat actor claimed to have gained and maintained live access to the Saudi Arabian food and beverage company's database infrastructure, offering to sell this access to a single buyer. To support the claim, the actor shared sample files containing sensitive customer information such as names, addresses, emails, phone numbers, VAT numbers, and geographic coordinates. Additionally, the threat actor provided a file listing the names of approximately 11,534 database tables, indicating the potential scale of the breach.

Threat Actor Leaks Database of Saudi Coffee Retailer

On January 25, the threat actor 'Al-Sheikh' leaked a database on nuovo BreachForums allegedly stolen from a Saudi Arabia-based online retailer specializing in coffee products. The threat actor claimed the database contains 133,900 records and shared sample records to corroborate the claim. The exposed data fields included customer names, email addresses, phone numbers, and physical address information such as country, state, and zip code.



Alleged Database of Saudi Engineering Firm Leaked Online

On or around February 24, the threat actor 'zerodayx1' leaked a database on nuovo BreachForums allegedly belonging to a Saudi Arabian engineering and construction services company. While the threat actor described the victim's business operations, they did not disclose details about the database's contents, instead sharing a direct link to a file hosting service to download a 78.7 MB zip file. The claims surrounding this data leak remain subject to further investigation.

© 2025 Cyble Inc. All rights reserved.

Ransomware Attacks

Cyble Research and Intelligence Labs (CRIL) observed 13 publicly disclosed ransomware attacks targeting organizations in Saudi Arabia in 2025. This activity indicates a consistent and multi-faceted threat to the nation's public and private sectors from various cyber-extortion groups.

Dominant Groups

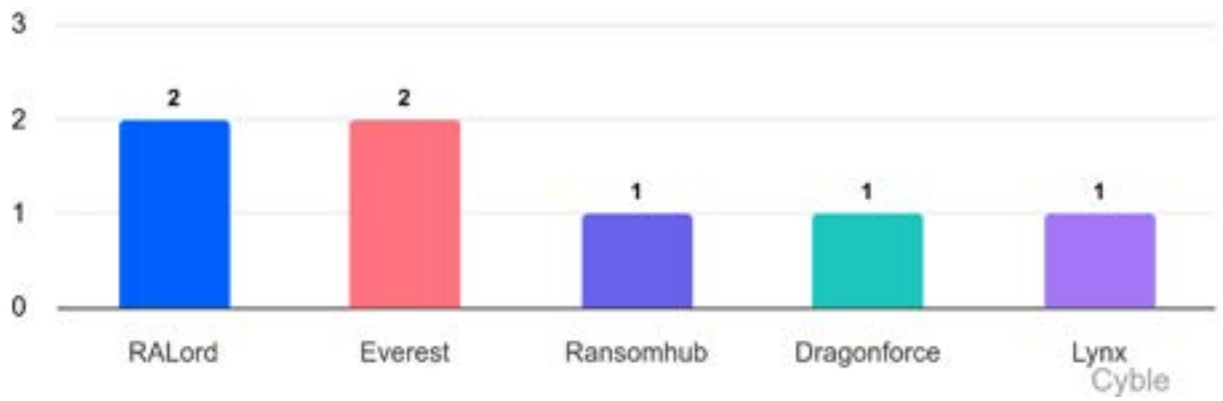


Fig 6: Most Active Ransomware Group in Saudi Arabia in 2025

The ransomware landscape was fragmented, with no single group establishing overwhelming dominance. The most active threat actors were Ralord and Everest, each responsible for two incidents. Collectively, these two groups accounted for over 30% of the total attacks observed in the region.

The remaining attacks were perpetrated by nine other distinct ransomware groups, including RansomHub, DragonForce, Qilin, and Medusa, each claiming a single victim. This wide distribution of threat actors highlights a diverse ecosystem where numerous groups are actively and opportunistically targeting entities within the Kingdom.

© 2025 Cyble Inc. All rights reserved.

Impact Analysis

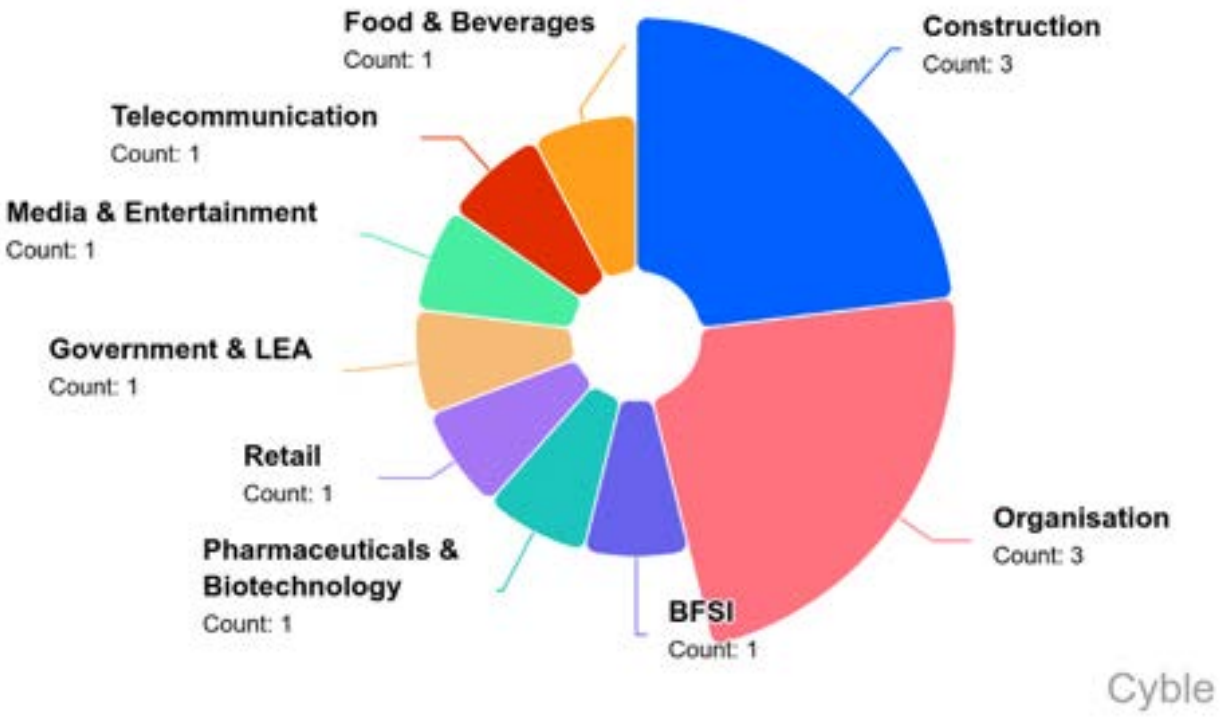


Fig 7: Most Targeted Sectors by Ransomware Actors in Saudi Arabia in 2025

An analysis of victimology data reveals that the Construction sector was one of the most frequently targeted industries, enduring three separate attacks. An equal number of incidents were recorded against entities classified under the general 'Organisation' category, which often includes non-profits and professional associations.

Combined, these two categories represented nearly half of all publicly claimed attacks. Ransomware operators also impacted a wide array of other critical and commercial sectors, with individual attacks noted against BFSI, Pharmaceuticals & Biotechnology, Government & Law Enforcement, Telecommunication, and Retail, demonstrating the broad, opportunistic scope of these campaigns.

Notable Incidents/Trends

A primary trend observed during this period was the significant diversity of participating ransomware collectives. With 11 different groups responsible for 13 attacks, the threat landscape is characterized by a multitude of independent operators rather than a few dominant cartels.

© 2025 Cyble Inc. All rights reserved.

Furthermore, a notable surge in activity occurred in July, which saw four distinct attacks, making it the most active month within the reporting period. The presence of varied groups such as the established Medusa and newer entrants like The Gentlemen points to a dynamic and evolving threat environment.

Overall, the ransomware ecosystem targeting Saudi Arabia in 2025 is defined by opportunistic campaigns from a diverse array of threat actors, with a pronounced impact on the construction sector and a clear trend towards a fragmented, multi-group threat landscape.

DATE	RANSOMWARE GROUP	INDUSTRY
21-Feb-2025	Dragonforce	Construction
01-May-2025	Everest	Pharmaceuticals & Biotechnology
13-Jul-2025	Everest	Organisation
23-Jul-2025	Global	Media & Entertainment
09-Jul-2025	INC Ransom	Government & LEA
17-May-2025	Lynx	Construction
22-Oct-2025	Medusa	Organisation
03-Jul-2025	Qilin	Retail
14-Apr-2025	RALord	Organisation
24-Apr-2025	RALord	Construction
04-Feb-2025	Ransomhub	BFSI
10-Oct-2025	Sinobi	Food & Beverages
29-Sep-2025	The Gentlemen	Telecommunication



© 2025 Cyble Inc. All rights reserved.

Hacktivism

The hacktivism landscape targeting the Kingdom of Saudi Arabia in 2025 was characterized by a steady volume of ideologically and geopolitically motivated cyber incidents. A diverse array of threat actor groups and channels, including 'Ghosts of Palestine™', 'Anonymous KSA', 'X Sec 404 TEAM', and 'لواء محمد ﷺ', were prominently observed orchestrating these campaigns.

The primary attack vectors consisted of website defacements and Distributed Denial-of-Service (DDoS) attacks, aimed at disrupting services and spreading political messaging. While less frequent, data leak and dump incidents were also noted, with approximately seven distinct posts identified during the reporting period.

These operations demonstrated a broad targeting scope, affecting at least 57 unique domains across numerous sectors, with a significant focus on Government & Law Enforcement, Healthcare, Technology, and Telecommunication entities.

لواء محمد ﷺ

The hacktivist channel 'لواء محمد ﷺ', operating in concert with entities identifying as 'Anonymous Lebanon', focused on data exfiltration and network intrusion targeting Saudi Arabian organizations. The group's primary method involved exploiting web application vulnerabilities to access and publicly leak sensitive server configuration files, specifically `.env` files. This tactic exposed database credentials, API keys, and other secrets for entities in the healthcare and education sectors.

In addition to these data leaks, the group also claimed to have compromised SSH servers, identified critical vulnerabilities on government websites, and leaked partial databases from educational institutions while openly disdaining less sophisticated methods like DDoS attacks.

Laneh | Dark

The hacktivist channel 'Laneh | Dark' engaged primarily in data extortion and the sale of allegedly stolen information targeting entities within Saudi Arabia. The group's activity centered on the infrastructure and energy sectors, with specific claims of having breached and exfiltrated several terabytes of data from the oil and gas gaints and other infrastructure service organizations. '

Laneh | Dark' advertised sensitive data for sale, including details on 18,000 engineers, infrastructure data maps for power, oil, and gas lines, and confidential contracts. Their stated methodology involved attempting to negotiate with victim organizations before offering the data for sale

© 2025 Cyble Inc. All rights reserved.

on public channels and forums when those talks failed. The group's posts indicate a financial motivation, coupled with a stated intent to damage the credibility of entities described as "Saudi capitalists."

Cyber Bulletin

The 'Cyber Bulletin' channel primarily operated as a news aggregator, reporting on cyber incidents targeting Saudi Arabian entities conducted by various threat actors. The channel's activity included publicizing a website takedown of a manufacturer in the wholesale building materials sector.

It also reported on third-party ransomware and data breach incidents, such as a claimed RansomHub ransomware attack and a BreachForums member's alleged data leak from a legal services platform. Additionally, 'Cyber Bulletin' amplified claims of data sales, noting an instance where a threat actor was reportedly selling 590GB of data allegedly belonging to the Saudi military and government. The reported incidents impacted the manufacturing, diversified industrial, legal, and government sectors.

Holy league

Throughout the observed period, the hacktivist channel 'Holy league' and its affiliates primarily claimed responsibility for Distributed Denial-of-Service (DDoS) attacks targeting Saudi Arabian entities. The group's campaigns heavily focused on the government sector. Other targeted sectors included finance, media, and tourism. The channel's content indicates 'Holy league' operates as part of a coalition, sharing posts from and receiving support from groups like 'Keymous,' 'TEAM FEARLESS,' and 'red wolf cyber.' The stated motivation for these cyberattacks is geopolitical, with one post explicitly referencing support for Yemen as a reason for targeting the Kingdom.

X Sec 404 TEAM

The hacktivist channel 'X Sec 404 TEAM' conducted operations against Saudi Arabian entities, citing a pro-Palestinian motivation and accusing the country of betraying the Palestinian cause. The group's activities observed during this period consisted of information operations through hostile messaging and issuing threats to penetrate Saudi "sensitive infrastructure" and attack government websites. The channel also claimed responsibility for a data breach and subsequent leak impacting the media sector. This attack was attributed in the post to an actor identified as "CYBER LAMI."

© 2025 Cyble Inc. All rights reserved.

Industry Insights and Analysis

DragonForce Attacks Critical Infrastructure to Exfiltrate Data and Halt Operations, 27-Feb-2025

The DragonForce ransomware group has targeted critical infrastructure in Saudi Arabia with their ransomware. The attack aimed to exfiltrate data and disrupt operations. The group, known as DragonForce, launched a significant cyberattack on the infrastructure, causing potential harm and financial losses. The malware used in the attack was identified as DragonForce ransomware, specifically designed to target operating systems in Saudi Arabia.

Chinese Hackers Deploy MarsSnake Backdoor in Multi-Year Attack on Saudi Organization, 20-May-2025

A multi-year cyber attack on a Saudi organization by a China-aligned threat actor group called UnsolicitedBooker was noted by some publications. The group used a backdoor named MarsSnake and targeted governmental organizations in Asia, Africa, and the Middle East. The attack involved spear-phishing emails with flight tickets as decoys. The group also shared overlaps with other threat clusters like Space Pirates. The activities of these threat actors indicate ongoing cyber espionage and data exfiltration operations in different regions.

Ransomware 2.0 How AI-Powered Attacks Are Evolving

Ransomware attacks have evolved into AI-powered ransomware attacks, becoming more sophisticated and dangerous. Ransomware 2.0 introduces tactics like double extortion and triple extortion, where data theft and DDoS attacks are combined with encryption to maximize pressure on victims. Threat actors like Medusa, DragonForce, and LockBit have been active in targeting various industries in different countries. AI is being used to enhance reconnaissance, targeting, and scalability of attacks. Organizations are advised to adopt AI-powered defense mechanisms effectively.

© 2025 Cyble Inc. All rights reserved.

Iran-Linked Threat Actors Cyber Fattah Claim Leak of Visitors and Athletes' Data from Saudi Games

Iran-linked threat actors known as 'Cyber Fattah' claimed alleged leak of thousands of records on athletes and visitors from past Saudi Games. The data breach likely involved unauthorized access to phpMyAdmin and exfiltration of stored records. The incident is seen as part of a broader information operation conducted by Iran to create insecurity and destabilize peace in the region. The stolen data included personally identifiable information, International Bank Account Numbers (IBANs), and medical examination certificates. The threat actors aimed to capitalize on tensions between Israel and Iran, targeting major sports events to spread anti-US, anti-Israel, and anti-Saudi propaganda.

Red Sea Cable Cuts Cause Azure Outage and Global Traffic Disruptions

A disruption in submarine cables in the Red Sea impacted Microsoft Azure, causing a surge in network latency and affecting internet traffic between continents. Microsoft reported a disruption in submarine cables near Jeddah, Saudi Arabia, impacting multiple cloud services. The incident affected key submarine cables like SMW4, IMEWE, FALCON GCX, and Europe-India Gateway.

Microsoft rerouted traffic to alternative routes, but latency spiked sharply. NetBlocks observed reduced speeds and connectivity disruptions across multiple countries. Cloudflare reported a drop in traffic between Delhi-London and Mumbai-Frankfurt. The outage was likely caused by a merchant vessel damaging the cables, not deliberate sabotage. Repair efforts were expected to take months due to the presence of armed conflict in the affected zone.



© 2025 Cyble Inc. All rights reserved.

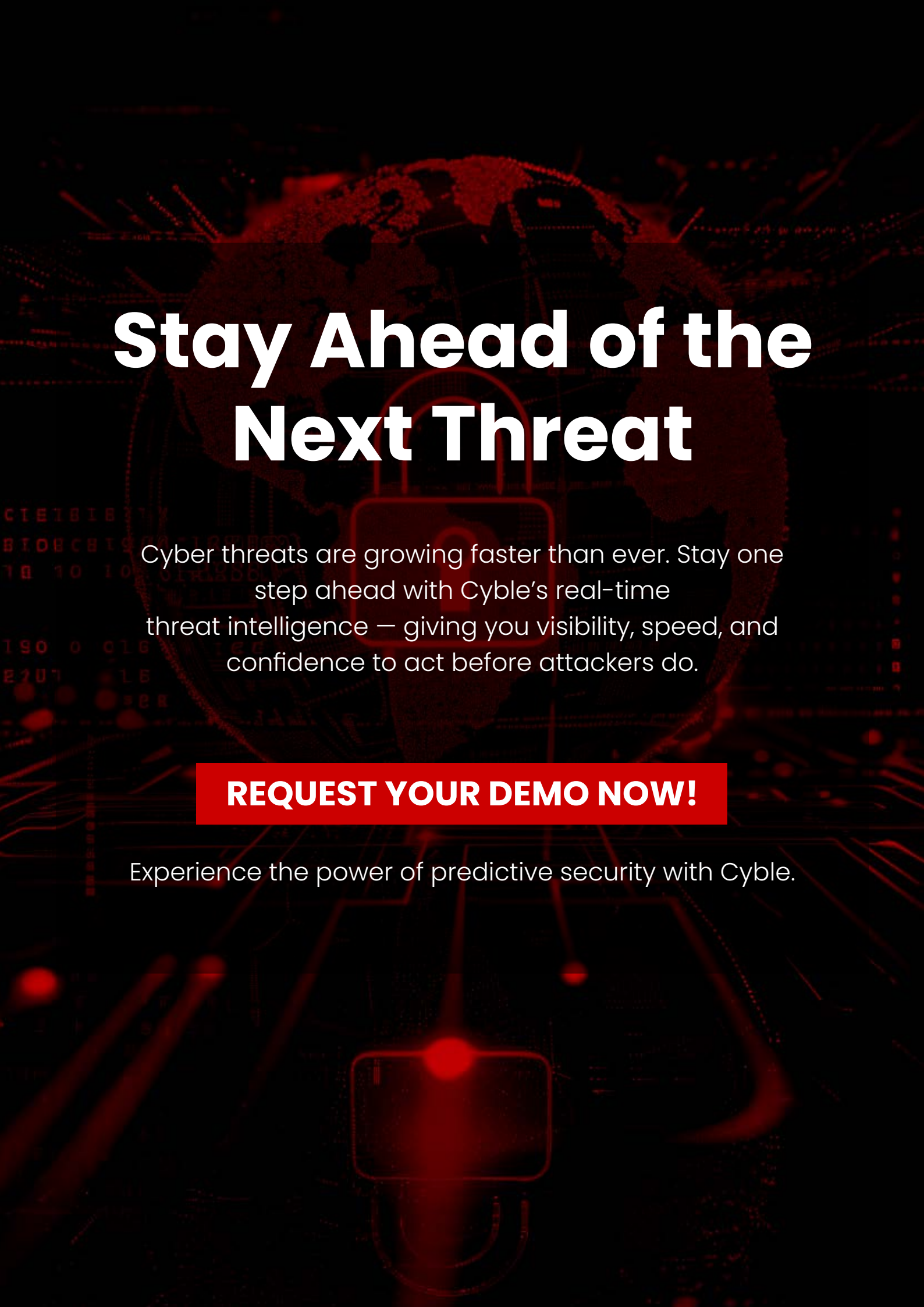
Conclusion

Cyber threat activity targeting Saudi Arabia in 2025 revealed a multi-faceted and dynamic landscape where the Government, IT & ITES, and Construction sectors were disproportionately targeted across multiple threat vectors.

The threat actor ecosystem was notably fragmented and opportunistic in the ransomware and initial access markets, while data breach activity was more concentrated, driven by a few prolific individuals. A significant trend observed was the high risk of supply chain compromises, with adversaries targeting IT providers to pivot to their customers.

Motivations ranged from financial gain, evident in numerous ransomware attacks and data sales, to geopolitical and ideological drivers behind hacktivist campaigns that primarily utilized DDoS and defacement. The landscape was further complicated by sophisticated espionage operations attributed to China- and Iran-linked threat actors highlighting that the Kingdom faces a complex convergence of criminal, hacktivist, and nation-state threats.




Stay Ahead of the Next Threat
Cyber threats are growing faster than ever. Stay one step ahead with Cyble's real-time threat intelligence — giving you visibility, speed, and confidence to act before attackers do.
REQUEST YOUR DEMO NOW!
Experience the power of predictive security with Cyble.

Industry Recognition

Cyble's capabilities are highly praised by global analysts, industry critics, and cybersecurity leaders

Gartner

Cyble Recognized in **Three Gartner® Hype Cycle™ Reports** for the **Second Consecutive Year 2025, TechScape 2025 & More**

FROST & SULLIVAN



Cyble Named Leader in Frost Radar™ Cyber Threat Intelligence 2024

Y Combinator

Cyble featured among AI startups backed by Y Combinator (YC) 2025

FORRESTER®

Cyble has been recognized in Forrester's Q1 2025 report on Extended Threat Intelligence Service Providers (ETISPs) and in the Q2 2024 Forrester Attack Surface Management Landscape report.

QKS Group

SPARK Matrix™ 2025

LEADER

Cyble Named as a Leader in Digital Threat Intelligence Management

AMERICA'S BEST STARTUP EMPLOYERS | Forbes 2024

Recognized as one of America's Best Startup Employers by Forbes



Cyble Secures Four Prestigious Honors at the 2025 Global Infosec Awards

Gartner Peer Insights.

Ranked No. 1 among the top Security Threat Intelligence Providers.

4.8/5



Cyble Named in America's Greatest Startup Workplaces 2025, By Newsweek



Cyble Wins Three Top InfoSec Innovator 2025 Awards



G2

Named a leader in the G2 Grid for Dark Web Monitoring and Threat Intelligence

Cyble, the world's first AI-native cybersecurity company, today announced its commanding presence in the **G2 Fall 2025 Report**, earning **24 prestigious badges across 8 strategic categories**. This unprecedented recognition validates Cyble's breakthrough **Agentic AI architecture** and positions the company as the definitive leader in autonomous cybersecurity intelligence.



OUR INVESTORS

BLACKBIRD · KING RIVER · SUMMIT PEAK · Singtel innov8 · Bizlabs · Y Combinator · SPIDER CAPITAL · svb Silicon Valley Bank

10080 North Wolfe Road, Suite SW3-200, Cupertino, CA 95014 | contact@cyble.com | +1 888 673 2067

All Rights Reserved | www.cyble.com