CYBER THREAT LANDSCAPE REPORT – UNITED ARAB EMIRATES (UAE) - CYFIRMA

Archived: 2026-04-02 12:32:58 UTC

Published On : 2025-10-08

Executive Summary

In 2025, the United Arab Emirates (UAE) experienced a significant surge in cybercriminal activity, particularly in the dark web ecosystem. Threat actors targeted critical government institutions, financial services, and digital platforms, resulting in multiple high-profile data breaches. Sensitive information, including personally identifiable information (PII), financial data, and corporate records, was exposed and offered for sale on underground forums. Ransomware activity also surged, with Russia-linked groups such as Everest, Medusa, and Embargo leading attacks against UAE entities. The evolving threat landscape highlights the urgency for enhanced cybersecurity measures, robust regulatory compliance, and proactive threat intelligence initiatives.

Key Findings

Government and Public Sector Breaches

- Dubai's Ports, Customs, and Free Zone Corporation (PCFC) experienced a leak of 1.94 TB of data, including passports and Emirates IDs.
- Dubai Municipality systems, including JIRA tickets and Confluence documents, were compromised and made available on dark web forums.

Financial Sector Exposure

- Emirates NBD, Commercial Bank of Dubai, and other financial institutions had customer databases, credit card, and brokerage information leaked.
- Insurance platforms such as Lookinsure were targeted, with CRM and transaction data exposed, enabling risks of identity theft, financial fraud, and synthetic identity attacks.

Digital Services Breaches

- Digital Dubai Pulse records of 22,000 individuals were compromised, exposing personal and professional details.

Dark Web Market Trends

- Cybercriminal forums actively facilitated the sale of stolen data, typically ranging from USD 257 to USD 50,000 per database.
- Government and financial sectors were the most frequently targeted, followed by airlines and digital service providers.

Ransomware Threat Landscape

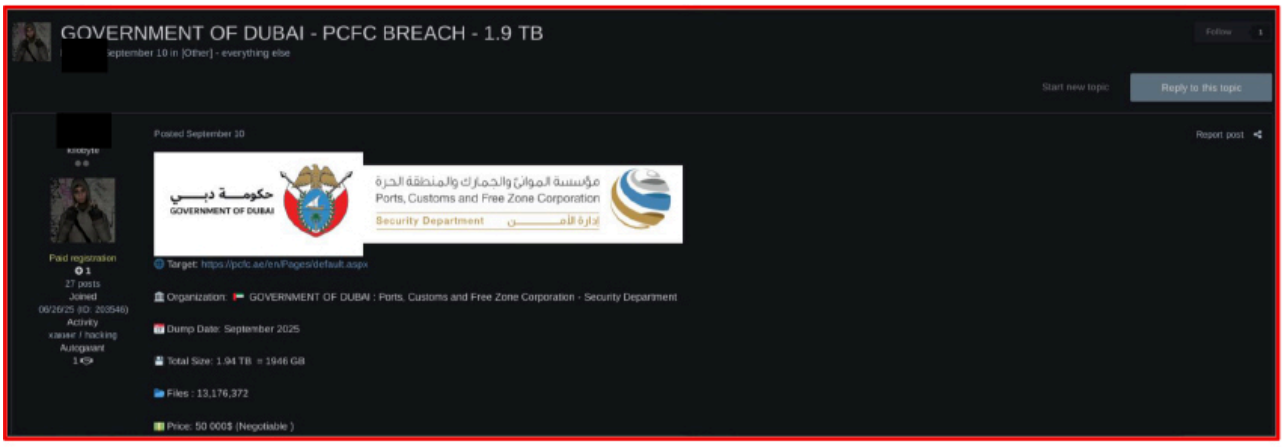
- Everest ransomware was the most active in 2025, with Medusa and Embargo also conducting significant attacks.
- Common tactics included phishing, privilege escalation, lateral movement, double extortion, and use of AI-enhanced malware for evasion.
- Smaller ransomware groups (e.g., DragonForce, Devman, Gunra) contributed to the broader threat landscape.

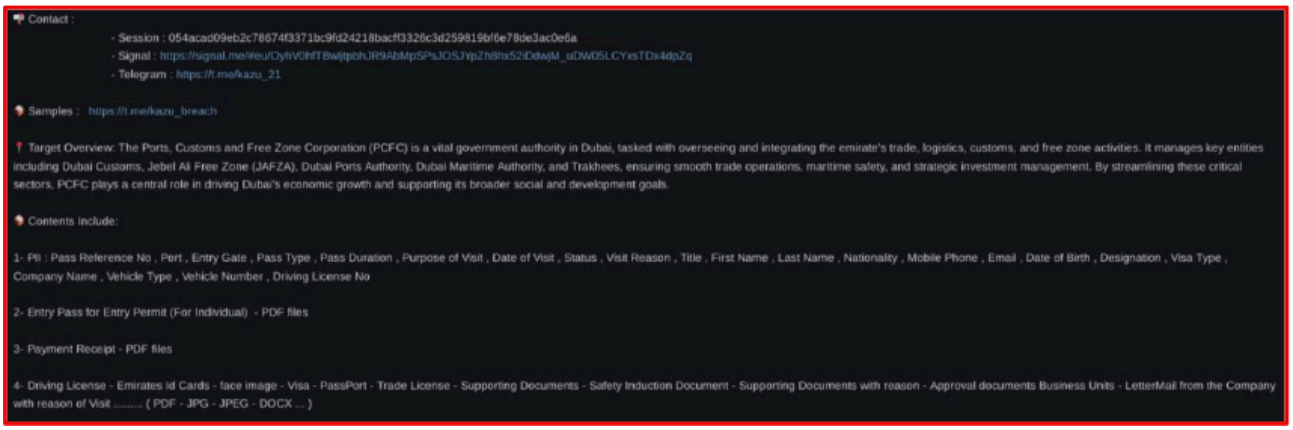
"The authenticity of these breaches remain unverified at the time of reporting, as the claims originates solely from the threat actor.

Major Dark Web Incidents of 2025

Dubai's Ports, Customs and Free Zone Corporation (PCFC) data is on sale

On September 10, 2025, CYFIRMA tracked activity on a popular Russian-speaking cybercriminal forum, where a threat actor known as "Kazu" claimed to have gained unauthorized access to the Government of Dubai's Ports, Customs, and Free Zone Corporation (PCFC). The actor allegedly leaked 1.94 TB of data and is reportedly selling sensitive information, including passports, Emirates IDs, and other personally identifiable information (PII). The threat actor has demanded USD 50,000 and instructed interested parties to contact them via Tox, Signal, or Telegram. The exposure of such data presents a significant risk, as it may be leveraged for targeted social engineering, phishing campaigns, and other follow-on malicious activities.

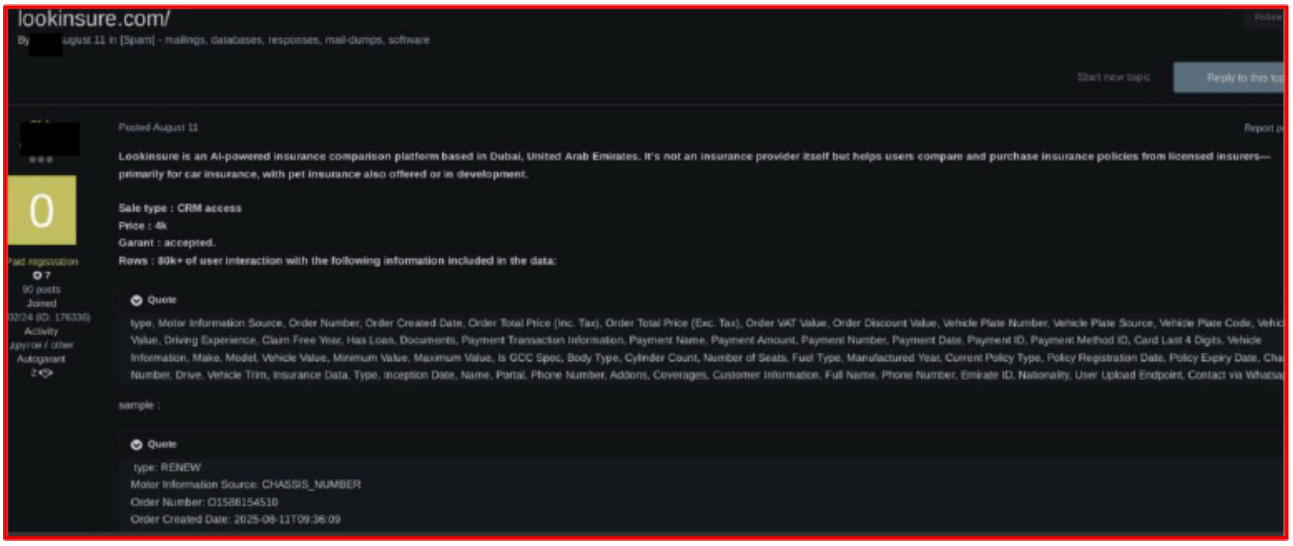




Database of an Insurance platform Operating in the UAE is on Sale

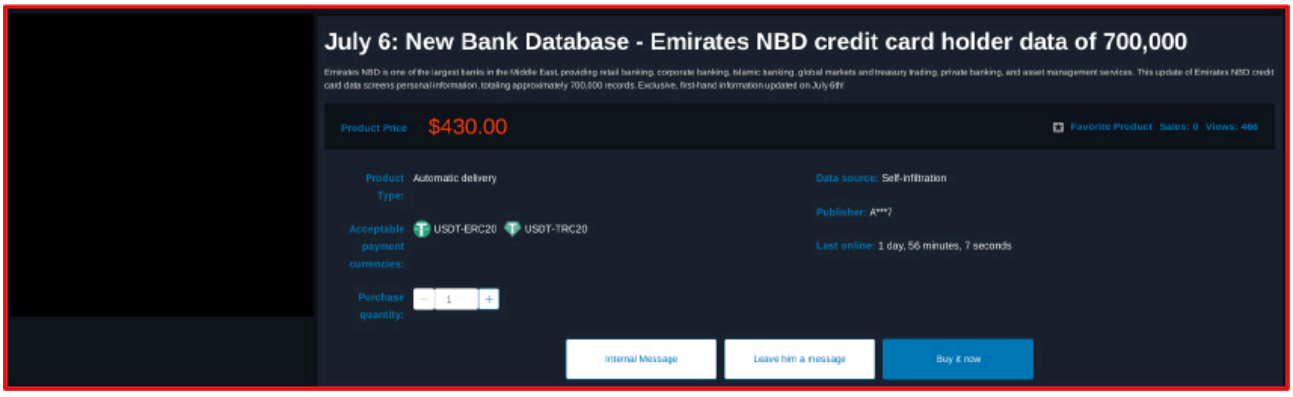
On August 11, 2025, a threat actor identified as “0kb” attempted to sell unauthorized access to the Customer Relationship Management (CRM) system of Lookinsure, an insurance aggregator and digital platform headquartered in the United Arab Emirates. The access was advertised for $4,000. According to the actor’s claims, the compromised data included loan documents, payment transaction records, insurance information, customer profiles containing full names, phone numbers, Emirate IDs, nationalities, and other sensitive details.

This compromise enables targeted phishing and social-engineering, identity theft and synthetic-identity fraud, account takeover and SIM-swap attacks, financial/insurance fraud, extortion, and resale of customer data — posing high regulatory, financial, and reputational risk.



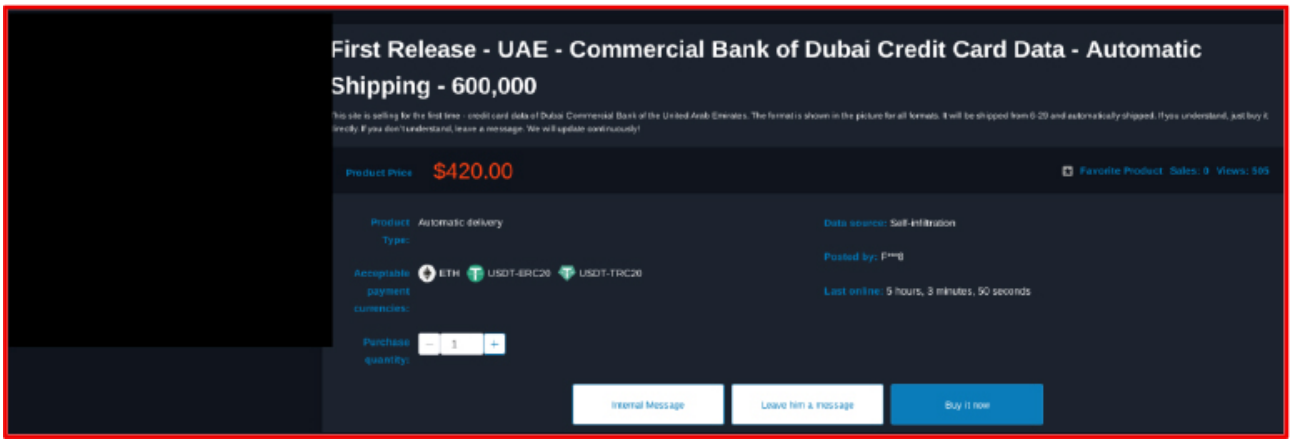
Database of Emirates NBD Offered For Sale

On July 6, 2025, a threat actor on a popular Chinese forum claimed to have leaked a database associated with Emirates NBD. The actor allegedly exposed the credit holder data of 700,000 including first names, last names, mobile numbers, email address and card details. The leak was reportedly offered for USD 430.



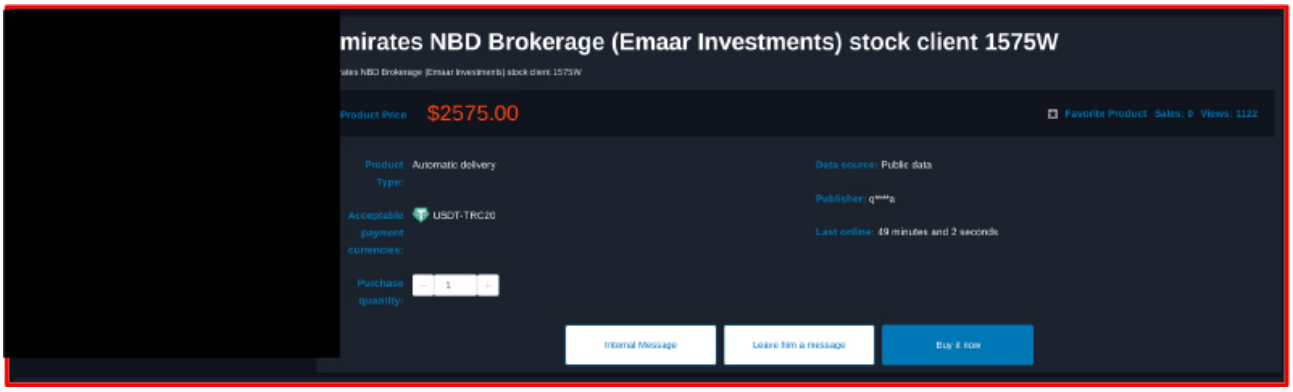
Database of UAE – Commercial Bank of Dubai Credit Card Data Offered For Sale

On August 29, 2025, a threat actor on a popular Chinese forum claimed to have leaked a database associated with Commercial Bank of Dubai Credit Card Data. The actor allegedly exposed the client details including first names, last names, and email address. The leak was reportedly offered for USD 420.



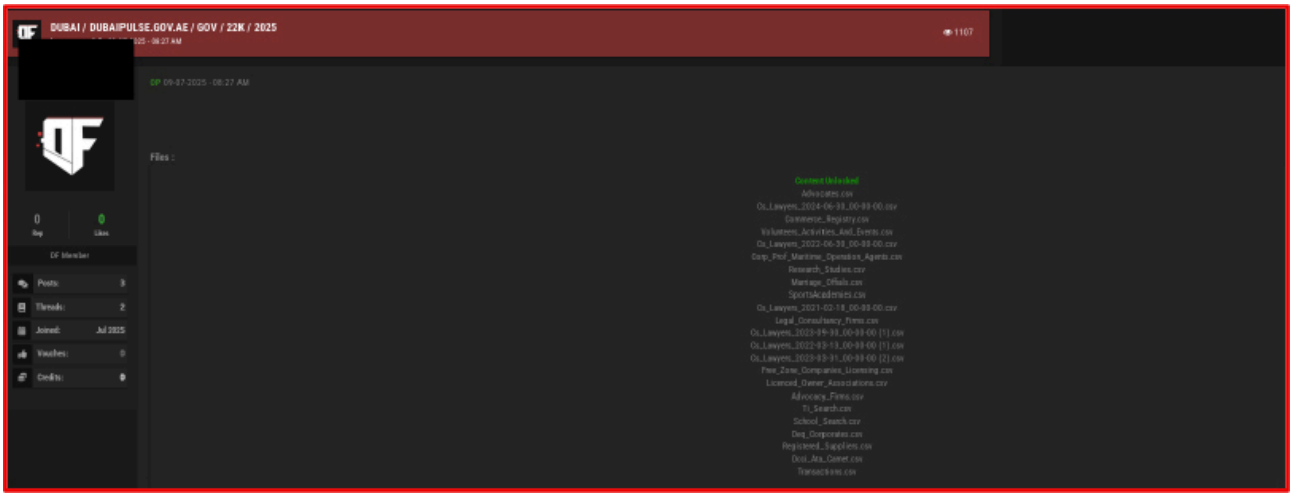
Database of Emirates NBD Brokerage Offered For Sale

On September 1, 2025, a threat actor on a popular Chinese forum claimed to have leaked a database associated with Emirates NBD brokerage (Emaar Investments). The actor allegedly exposed the client details including first names, last names, email address and card details. The leak was reportedly offered for USD 2575.



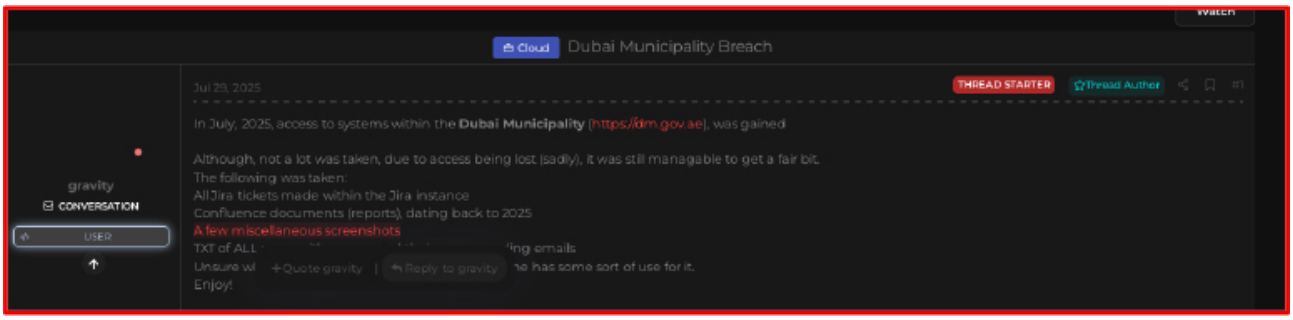
Database of Digital Dubai Pulse Offered For Sale

On July 9, 2025, a threat actor using the alias “auen_greyfall” claimed to have leaked a database of 22,000 records from Dubai Pulse. The leaked database includes first names, last names, designations, and addresses. The threat actor instructed interested parties to contact them via their TOX ID.



Database of Dubai Municipality Offered For Sale

On July 29, 2025, a threat actor named “Gravity” claimed to have gained unauthorized access to the systems of Dubai Municipality (https[:]//dm.gov.ae). The threat actor managed to gain access to all JIRA tickets, confluence documents, and a few miscellaneous screenshots.

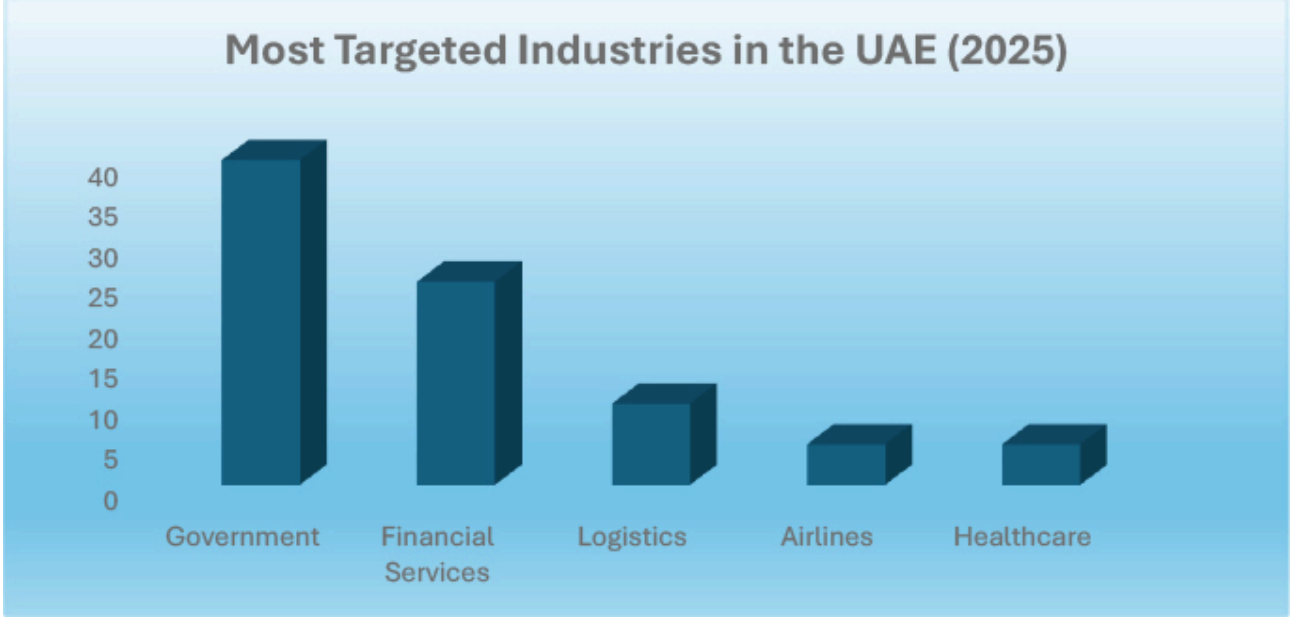


Dark Web Threats Statistics

The dark web serves as a central underground hub where hackers and threat actors actively communicate and trade information. Our analysis of dark web activity focused on identifying trends related to targeted countries and industries.

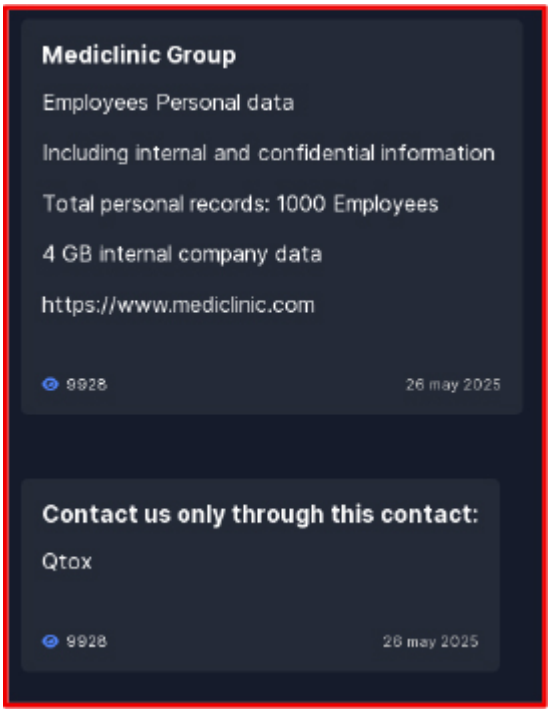
The CYFIRMA research team detected several posts from different threat actors targeting enterprises in the UAE. The majority of these posts involved the sale of customer databases and unauthorized access to the networks of UAE-based organizations.

Government institutions and financial services emerged as the most frequently targeted sectors, followed by the airline industry. These findings highlight the increasing risks faced by critical sectors in the UAE and emphasize the need for enhanced cybersecurity measures.

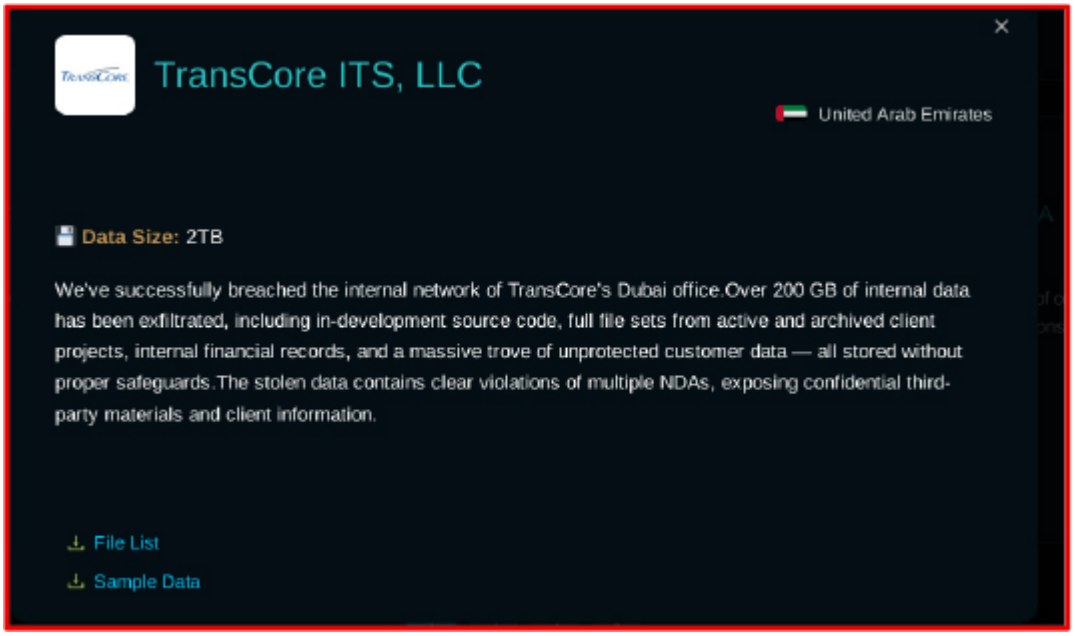


Major Ransomware Incidents in UAE – 2025

On May 26, 2025, Mediclinic Group, a South Africa–based healthcare company that also operates in the United Arab Emirates, was targeted by the Everest ransomware group. The attackers claim to have obtained 4GB of the company’s internal data, including the personal information of approximately 1,000 employees.



On July 20, 2025, a U.S.-based company named TransCore, which operates in Dubai, was affected by the Crypto24 ransomware group. The group claimed to have breached the internal network of TransCore's Dubai office. More than 200 GB of internal data was exfiltrated, including in-development source code, complete file sets from active and archived client projects, internal financial records, and a large volume of unprotected customer data. The stolen information includes clear violations of multiple NDAs, exposing confidential third-party materials and client information.



Top Ransomware Gangs Targeting United Arab Emirates

Everest Ransomware:

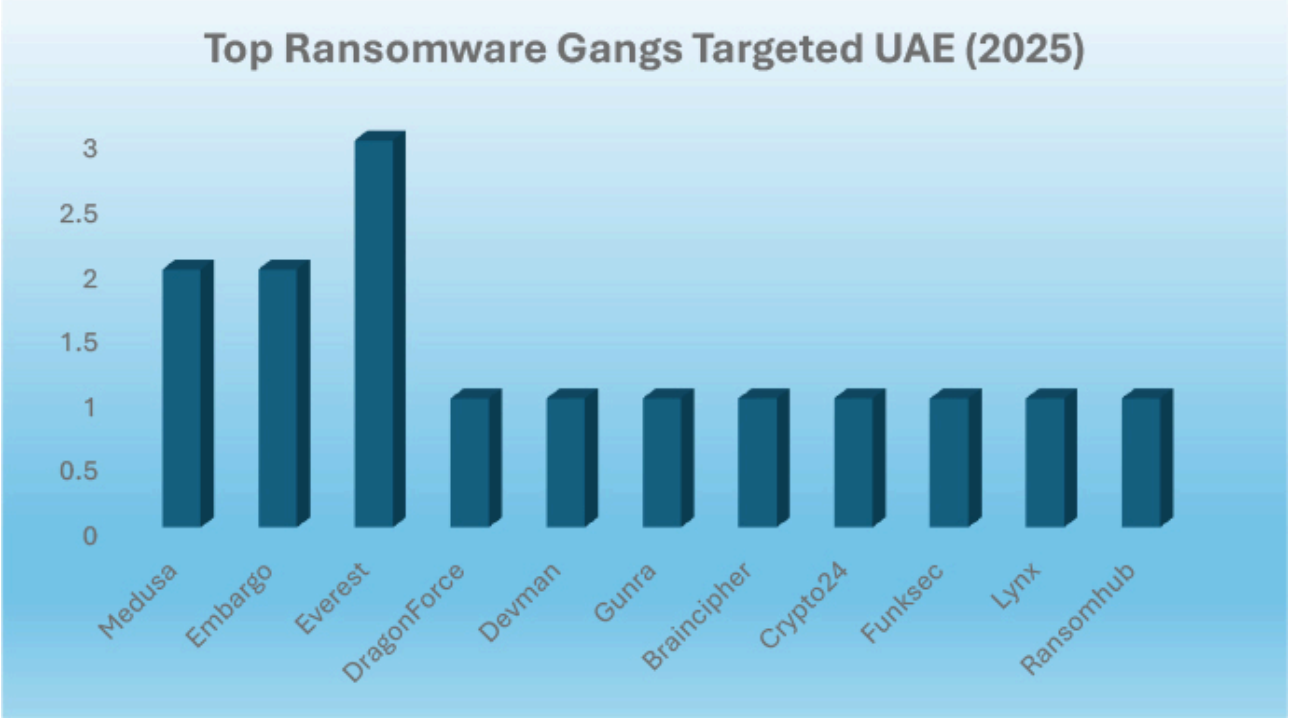
- Everest ransomware is a Russia-linked ransomware-as-a-service (RaaS) operation active since 2020.
- It typically spreads through phishing campaigns, malicious downloads, exploit kits, and exposed RDP services.
- Once inside, the threat actor performs lateral movement, network scanning, and privilege escalation before encrypting files with the ".everest" extension.
- The malware disables security/recovery tools, exfiltrates sensitive data, and employs double extortion tactics by threatening to leak data on its Tor-based site.

Embargo Ransomware:

- Embargo ransomware, a Ransomware-as-a-Service (RaaS) group that emerged in April 2024, has quickly become a significant cybercrime threat, linked to over USD 34 million in transactions.
- The group uses Rust-based malware, double extortion tactics, and advanced defense evasion.
- Its sophistication possibly enhanced by AI and subdued branding help it operate effectively while evading detection.

Medusa Ransomware:

- Medusa ransomware is a Russia-linked ransomware operation active since late 2022.
- It spreads via initial access brokers, phishing campaigns, and exploiting public-facing vulnerabilities.
- Once inside, operators perform lateral movement, privilege escalation, and credential dumping before encrypting files with the ".MEDUSA" extension.
- The group exfiltrates sensitive data and uses double extortion, threatening to leak data on its dark web blog while pressuring victims through public platforms like Telegram and X.



In 2025, ransomware activity in the UAE was led by Everest, which recorded the highest number of incidents, making it the most active group of the year. Medusa and Embargo followed, both showing notable levels of

attacks against UAE targets.

Other groups including DragonForce, Devman, Gunra, Braincipher, Crypto24, Funksec, Lynx, and Ransomhub each registered fewer incidents but still contributed to the overall ransomware threat landscape.

Overall, the 2025 data highlights Everest as the dominant ransomware gang, while also showing that the UAE faced threats from a diverse set of smaller but persistent actors.

Conclusion

The UAE's cyber threat landscape in 2025 demonstrates a critical need for vigilance across all sectors. The combination of targeted data breaches, dark web data trafficking, and ransomware attacks highlights the persistent risk to national security, financial stability, and public trust. Government and private organizations must recognize that cyber threats are not isolated incidents but part of a coordinated, global ecosystem of criminal activity.

Recommendations

Strengthen Cybersecurity Infrastructure

- Implement multi-layered security measures, including endpoint detection and response (EDR), network segmentation, and zero-trust architecture.
- Regularly patch and monitor critical systems to reduce vulnerability exposure.

Enhance Threat Intelligence and Monitoring

- Continuously monitor dark web forums and underground marketplaces for early warning of potential breaches.
- Integrate threat intelligence feeds into incident response protocols to anticipate emerging threats.

Improve Data Protection and Compliance

- Encrypt sensitive data both at rest and in transit.
- Ensure compliance with UAE data protection regulations and international cybersecurity standards.

Employee Awareness and Training

- Conduct regular cybersecurity awareness programs focusing on phishing, social engineering, and safe data handling.
- Promote a culture of reporting suspicious activity and incidents promptly.

Incident Response and Business Continuity

- Develop and regularly test comprehensive incident response plans, including ransomware-specific playbooks.
- Establish rapid recovery and backup systems to minimize operational and reputational impact.

Collaborative Cybersecurity Initiatives

- Encourage public-private partnerships for information sharing on cyber threats.
- Participate in regional and global cyber defence collaborations to enhance preparedness against sophisticated threat actors.
