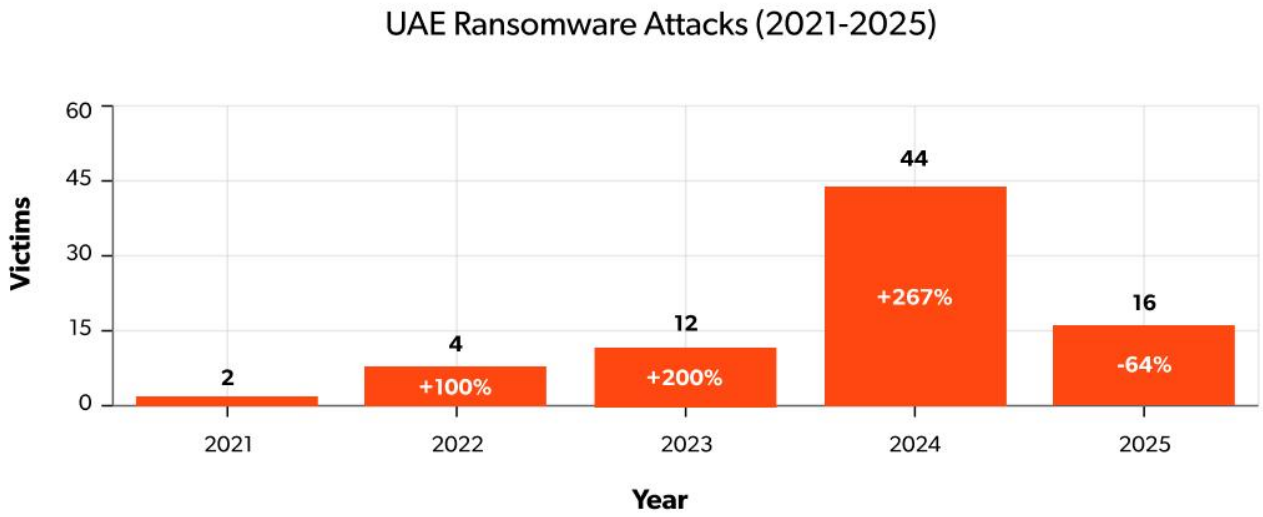
The Evolution of Ransomware in the UAE: A Comprehensive Analysis

By Mario Rojas, Senior Security Researcher, ORYXLABS

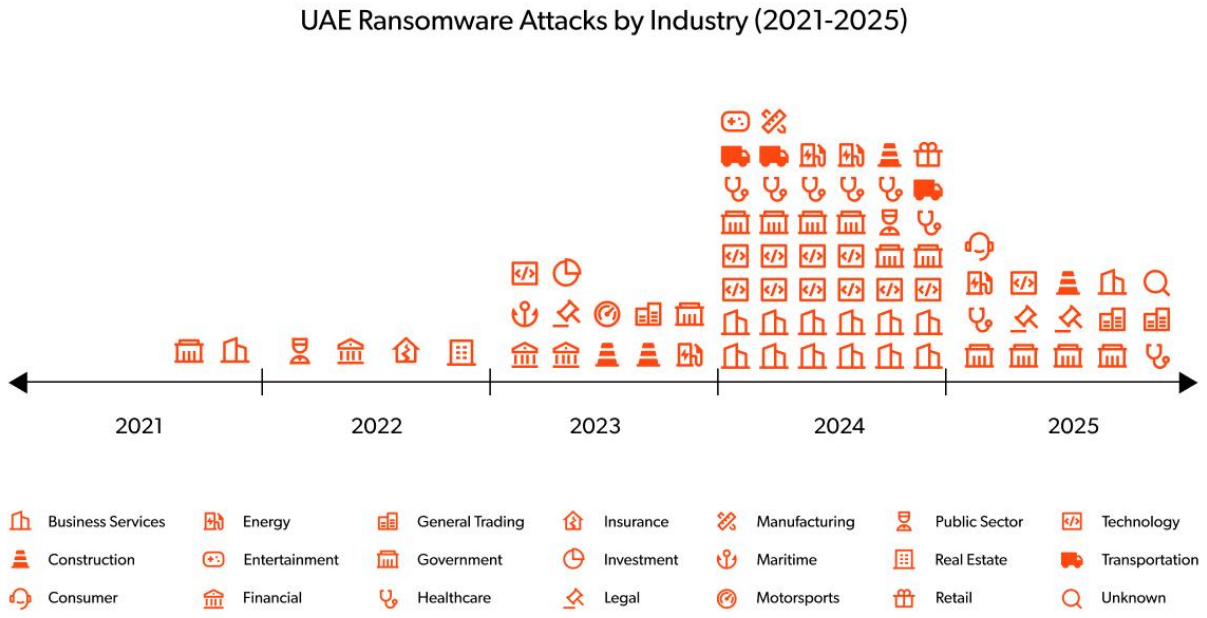
The UAE has experienced a dramatic transformation in its cybersecurity threat landscape, evolving from isolated ransomware incidents to facing sophisticated, large-scale attacks that threaten critical infrastructure and economic stability.

This comprehensive analysis, based on validated attacks, examines how ransomware threats have evolved in the UAE, identifying the most targeted sectors, key threat actors, and the specific attack vectors they exploit.



The UAE's rapid digital transformation and position as a regional economic hub have made it an increasingly attractive target for cybercriminals and nation-state actors. Ransomware attacks in the UAE saw a staggering 267% increase in 2024 compared to the previous year, with 44 incidents reported, up from 12 in 2023. The country now faces approximately 200,000 daily cyberattacks, marking a dramatic escalation from the 50,000 daily attacks recorded in 2024.

Ransomware evolution timeline



Early incidents (2016–2020)

The UAE's encounter with ransomware began with targeted attacks against high-value financial institutions. In 2015, the notorious "Hacker Buba" targeted the UAE Invest Bank, demanding a $3 million ransom for stolen customer data affecting accounts worth over $110 million. This incident marked the beginning of financially motivated ransomware attacks against the UAE's banking sector.

The period from 2015–2020 was characterised by relatively isolated incidents, with attackers focusing on direct financial extortion. However, the groundwork for more sophisticated operations was being laid, as cybercriminal groups began to recognise the UAE's economic value and digital vulnerability.

The pandemic acceleration (2020–2022)

The COVID-19 pandemic dramatically accelerated ransomware activity in the UAE. In 2020, the country experienced a 250% increase in cyberattacks, including 1.1 million phishing attacks. By 2021, ransomware groups started targeting UAE organisations.

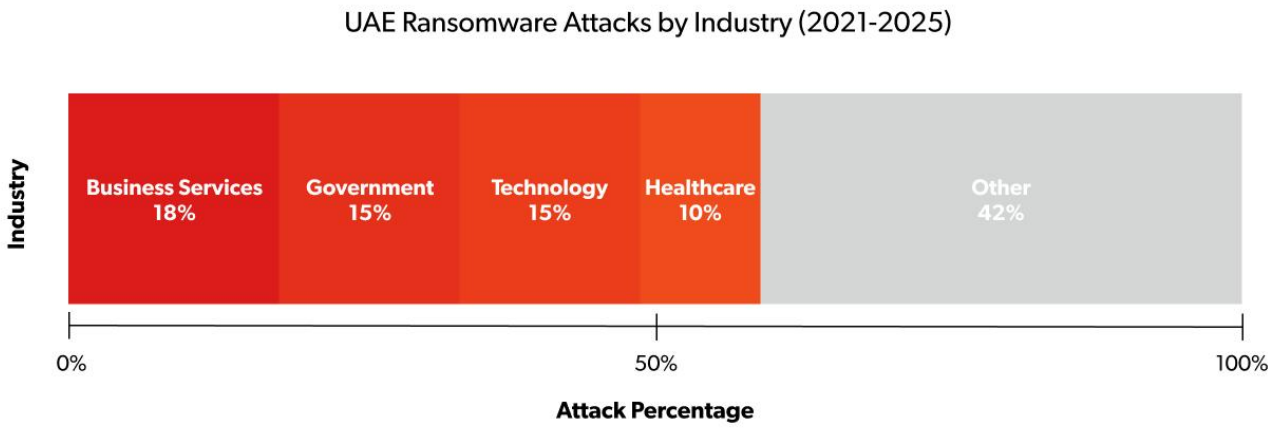
Microsoft Exchange Server vulnerabilities became a critical attack vector during this period. Attacks on MS Exchange grew by 182% in the UAE in August 2021, with cybercriminals exploiting ProxyShell vulnerabilities, including CVE-2021-34473, CVE-2021-34523 and CVE-2021-31207. These vulnerabilities enabled attackers to bypass authentication and execute code as privileged users.

Modern sophisticated operations (2023–2025)

The ransomware landscape has evolved into highly sophisticated, multi-vector attacks characterised by diverse threat actors and advanced techniques. The UAE recorded 44 ransomware incidents in 2024, marking a 267% increase compared to 12 in 2023. This surge reflects the nation's growing prominence on a global stage, positioning it as a prime target for cybercriminals aiming to exploit vulnerabilities in the healthcare, technology, government, and critical infrastructure sectors.

Targeted sectors

Based on our analysis of ransomware attacks targeting the UAE, the sector distribution reveals clear patterns in attacker preferences and strategic targeting.



The top four sectors: business services, technology, government and healthcare, account

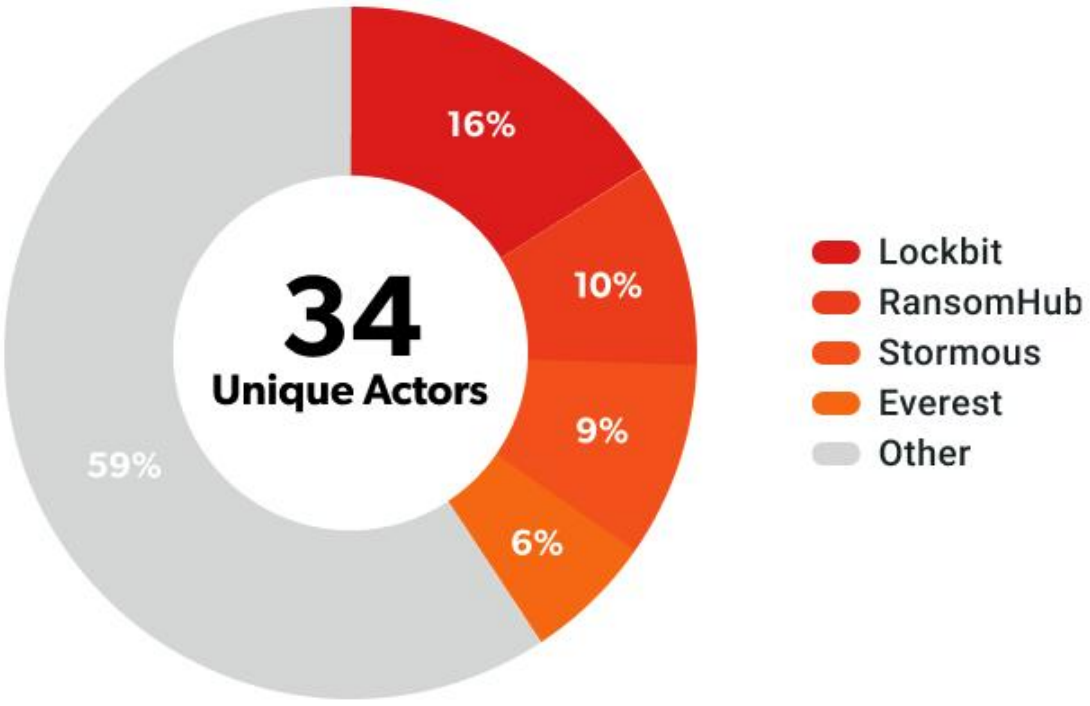
for approximately 58% of all documented ransomware incidents, indicating ransomware groups' strategic focus on organisations with extensive digital dependencies and high operational criticality.

The diverse targeting across 21 sectors demonstrates that no industry in the UAE is immune to ransomware threats, though certain sectors face significantly higher risk levels based on their digital infrastructure, data value, and potential for operational disruption.

This distribution pattern aligns with global ransomware trends, where attackers prioritise targets based on their likelihood to pay ransoms, data sensitivity and potential for maximum impact on business operations.

Main threat actors

Four threat actors have dominated the ransomware scene in the UAE for the last four years, accounting for nearly 40% of the recorded incidents.



LockBit: The dominant force (16%): LockBit has emerged as the most active ransomware group targeting the UAE, responsible for several high-profile attacks, including the February 2024 Etisalat attack, where the actor demanded a $100,000 ransom. In 2024, part of LockBit’s infrastructure was seized in an international law enforcement operation. This has dramatically reduced the actor’s capacity and is likely the reason why LockBit has practically faded from the UAE ransomware scene in 2025.

RansomHub (10%): RansomHub emerged as a formidable Ransomware-as-a-Service

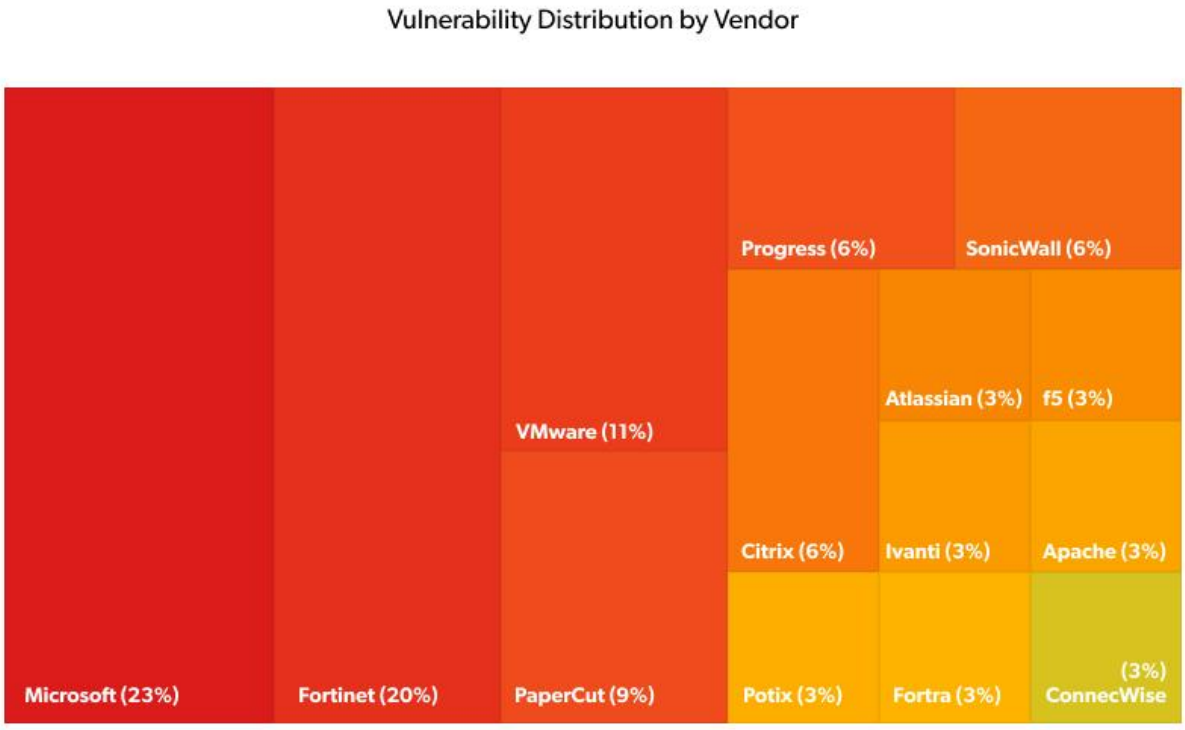
(RaaS) group in February 2024 and quickly established itself as one of the most prolific threats in the global ransomware ecosystem. In 2024, the group saw remarkable growth, with its market share increasing from 2% in Q1 to 14.2% by Q3, making it a dominant force in global ransomware operations. In the UAE, RansomHub accounted for over 16% of ransomware activity in 2024, representing a significant threat to the region's critical infrastructure and enterprises.

Stormous (9%): Stormous ransomware, affiliated with the Five Families' alliance, has emerged as a significant threat actor targeting both UAE government and private-sector entities throughout 2024. The group is part of a sophisticated cybercriminal ecosystem that includes GhostSec, ThreatSec, Blackforums, and SiegedSec.

Everest (6%): Since its establishment in December 2020, Everest ransomware has evolved from a traditional double-extortion ransomware operation to increasingly target the Middle East region, including organisations in the UAE. The group drew significant attention in May 2024 following a series of high-profile attacks, including one on Coca-Cola's Middle East division, which compromised data from nearly 1,000 employees across multiple distribution centres in the region.

Attack vectors and vulnerability trends

Ransomware groups targeting the UAE have consistently exploited vulnerabilities across a broad range of enterprise technologies. These actors' focus on enterprise-level technologies mirrors globally observed trends, with vendors such as Microsoft and Fortinet accounting for 43% of the total vulnerabilities targeted by these groups.



Microsoft ecosystem dominance: LockBit shows a clear preference for Microsoft

technologies, with 29.2% of its attacks targeting Microsoft products, particularly Exchange Server (3 CVEs) and Windows components. This aligns with Microsoft's omnipresence in enterprise environments.

Fortinet infrastructure focus: Three threat actors, including Qilin, Mora_001 and Medusa, show a marked focus on Fortinet products, collectively accounting for three of the five recorded Fortinet-related CVEs. This clustering suggests possible coordinated intelligence sharing or the use of common exploitation toolsets targeting network security infrastructure.

File transfer service targeting: CL0P maintains an exclusive focus on file transfer and document management platforms, such as Progress MOVEit and PaperCut MF, which indicates strategic targeting of data-rich environments conducive to their double-extortion model.

Our analysis also revealed distinct vulnerability type preferences that align with each group's operational strategies:

Threat Actor	Total CVEs	Vendors	Technologies	Vulnerability Types	Top Vulnerability Type	Top Vendor	Top Technology
LockBit	24	12	20	13	Remote Code Execution	Microsoft	Exchange Server
Cl0p	3	2	3	2	SQL Injection	Progress	PaperCut MF
Qilin	3	1	1	2	Authentication Bypass	Fortinet	FortiProxy
Medusa	2	2	2	2	SQL Injection	Fortinet	FortiClient
Mora_001	2	1	1	1	Authentication Bypass	Fortinet	FortiProxy
RansomEXX	1	1	1	1	Use-After-Free	Microsoft	Windows

Remote code execution (RCE) dominance: LockBit favours RCE vulnerabilities, which account for 25% of the group’s exploits, enabling immediate system control for rapid ransomware deployment. The group’s RCE targets include Apache Log4j2 (CVE-2021-44228), Spring Framework, and Exchange Server vulnerabilities.

SQL injection focus: CL0P demonstrates specialised expertise in SQL injection attacks, with 66.7% of its exploits targeting this vulnerability type. The group’s focus on MOVEit Transfer and cloud platforms’ vulnerabilities, such as CVE-2023-34362 and CVE-2023-35036, indicates a strategic emphasis on file transfer services for data exfiltration.

Authentication bypass specialists: Qilin and Mora_001 show remarkable specialisation in authentication bypass vulnerabilities, which account for 66.7% and 100% of their respective portfolios. This preference enables direct security control circumvention without complex attack chains.

Understanding these exploited CVEs provides valuable insight into how attackers gain initial access and escalate privileges within organisations.

Recommendations

- **Prioritise patch management:** Automate patch deployment for high-severity

vulnerabilities, particularly those exploited in the wild, including Microsoft Exchange, Fortinet and file transfer platforms like MOVEit.

- **Strengthen email security posture:**
  - Enforce SPF, DKIM and DMARC policies to reduce the risk of phishing-based initial access.
  - Use solutions such as DISCOVERY to monitor misconfigurations, identify exposed assets and detect compromised credentials across the open and dark web.
- **Isolate and protect critical infrastructure:**
  - Implement strict network segmentation between internet-facing services and operational networks.
  - Regularly audit access permissions and monitor lateral movement attempts.
- **Deploy DNS-based threat detection:** Integrate a DNS FIREWALL to identify and block outbound traffic to known command-and-control infrastructure and suspicious domains. DNS-layer controls provide early detection and containment for ransomware beaconing behaviour.
- **Ensure incident response readiness:**
  - Maintain offline, immutable backups and conduct quarterly tabletop exercises to validate recovery procedures.
  - Incident response runbooks should include predefined actions for ransomware-specific scenarios, including double-extortion and data leak site negotiations.
- **Sector-specific threat modelling:** High-risk sectors such as business services, technology, and healthcare should tailor controls based on prevalent actor TTPs. Use threat intelligence platforms to align defensive investments with observed adversary behaviour.

Conclusion

The noticeable slowdown in ransomware incidents across the UAE in early 2025 reflects a complex interplay of factors. While international law enforcement efforts, such as the takedown of LockBit's infrastructure, have disrupted several major ransomware operations, the UAE's commitment to cybersecurity has played a key role in enhancing national resilience and reducing threat impacts.

Government-led initiatives such as the UAE Cybersecurity Council's national strategies, regulatory frameworks and increased coordination with critical sectors have contributed to raising baseline security standards.

Enhanced public-private collaboration, sector-specific guidance, and greater awareness have all helped to strengthen the defences of high-value targets and reduce the attack surface for opportunistic threat actors.

Defenders must continue to evolve their security postures to keep pace with shifting TTPs, while leveraging both local and international threat intelligence partnerships to stay ahead of adversaries.

Remember, there's always more intelligence to uncover.