جامعة نايف العربية
للعلوم الأمنية
NAIF ARAB UNIVERSITY
FOR SECURITY SCIENCES
تاسست ١٩٧٨ Est. 1978

Ransomware Trends Report in Arab Countries

2025

Centre for Cybercrime and Economic Crime

جامعة نايف العربية
للعلوم الأمنية
NAIF ARAB UNIVERSITY
FOR SECURITY SCIENCES
تاسست ١٩٧٨ Est. 1978

Ransomware Trends Report in Arab Countries

2025

Centre for Cybercrime and Economic Crime

Naif University Press
2026

Table of Contents

Executive Summary	4
Introduction	6
Scope and Data Coverage	8
Ransomware Hit Organizations	9
Ransomware Hit Industries	10
Countries Affected in the Arab Region	12
Industry-Specific Insights in Context of Geographic Distribution in 2025	16
Ransomware Actors	17
AI-Driven Trend Evolution of Ransomware in Arab Countries (2020–2025)	19
AI-Driven Policy and Regulatory Implications	20
The Use of Artificial Intelligence in Ransomware Attacks	20
Observed ATT&CK Tactics and Techniques	22
Conclusion and Summary of Findings for 2025	24
Appendices	25
Ransomware Group Analysis - CL0P	25
Ransomware Group Analysis - QILIN	27
Ransomware Group Analysis - Kill Security	30
Tactics, Techniques, and Procedures (TTPs)	32
Glossary of Terms	34
References	36

Ransomware Trends Report in Arab Countries 2025

Abdulrazaq Al-Morjan, Kyounggon Kim, Seokhee Lee, Mostafa Moallim and Ibrahim Alzahrani

Centre for Cybercrime and Economic Crime, Naif Arab University for Security Sciences, Saudi Arabia.

تقرير اتجاهات برامج الفدية في الدول العربية لعام 2025

عبد الرزاق المرجان، كيونغون كيم، سوخوي لي، مصطفى معلم، إبراهيم الزهراني

مركز الجرائم السيبرانية والاقتصادية، جامعة نايف العربية للعلوم الأمنية، المملكة العربية السعودية.

pISBN: 978-603-93836-4-2
pDeposit: 1447/14017
eISBN:978-603-93836-5-9
eDeposit: 1447/14020

doi: 10.26735/978-603-93836-5-9

All ideas expressed in this work represent the opinion of the author and do not necessarily reflect the University’s viewpoint.

EXECUTIVE SUMMARY

The 2025 Ransomware Trend Report in Arab Countries builds on the 2023 edition, which recorded 92 victims across 13 Arab countries, with ransomware activity concentrated in the Commercial Facilities, Critical Manufacturing, and Energy sectors and was dominated by LockBit and BlackCat (ALPHV) groups. In 2025, ransomware activity expanded significantly, with higher victim counts, broader geographic impact, and a shift in dominant threat actors. While Commercial Facilities and Critical Manufacturing remain the most targeted sectors, Financial Services has emerged as a key target. At the same time, CL0P, Qilin, and Kill Security have become the most active ransomware groups in the region.

In 2025, the ransomware threat landscape affecting Arab countries expanded in scale and demonstrated clear patterns in targeting, sectoral impact, and attacker tradecraft:

- 147 organizations were identified as ransomware victims across Arab countries in 2025, based on analysis of dark web leak sites and incident reporting sources.
- 12 CISA critical infrastructure sectors were impacted by ransomware activity. The most targeted sector was Commercial Facilities, followed by Critical Manufacturing and Financial Services, reflecting attackers' preference for economically sensitive and operationally dependent organizations.
- 14 Arab countries were affected by ransomware attacks in 2025. The most targeted countries were the United Arab Emirates, Saudi Arabia, and Egypt, together accounting for the majority of recorded incidents.
- 48 ransomware groups were observed targeting organizations in Arab countries during 2025. Despite this broad actor landscape, activity was concentrated among a smaller subset of groups, with CL0P, Qilin, and Kill Security emerging as the most active ransomware actors in the region
- 28 distinct ransomware tactics, techniques, and procedures (TTPs) were identified across the three most active ransomware groups. The most frequently employed techniques reflect a highly standardized ransomware playbook dominated by phishing-based initial access, user-driven execution, scheduled task persistence, credential dumping, remote service–based lateral movement, and data encryption for impact.

Ransomware in Arab countries (2020-2025) evolved rapidly through three phases.

2020–2021

opportunistic, manual attacks (phishing, exposed services) on commercial and industrial sectors.

2022–2023

consolidation and scaling via RaaS (e.g., LockBit, BlackCat) with standardized playbooks and automation.

2024–2025

fragmentation and fast growth as new groups (CL0P, Qilin, Kill Security, RansomHub) adopt AI-augmented techniques, driving higher-volume, higher-value attacks concentrated in the UAE, Saudi Arabia, and Egypt. The region now faces greater scale and sophistication, requiring prioritized defensive actions.

INTRODUCTION

Ransomware is a form of malicious software (malware) that restricts access to a victim's systems or data and demands a ransom for restoration. It continues to represent one of the most severe and rapidly evolving cyber threats, posing significant risks to governments, critical infrastructure, and private-sector organizations worldwide. This report presents a detailed assessment of the 2025 ransomware landscape in Arab countries, examining key trends, dominant threat actors, affected sectors, and emerging operational patterns, while outlining strategic considerations for mitigating ransomware risks across the region.

The 2025 findings indicate a continued escalation of ransomware activity in Arab countries, characterized by a higher volume of victim organizations, increased operational maturity among ransomware groups, and more focused targeting of high-impact sectors. Ransomware operations have further consolidated into a profitable and structured criminal ecosystem, with a smaller number of highly active gangs responsible for a disproportionate share of attacks. Commercial Facilities and Critical Manufacturing remained the most targeted sectors, while Financial Services emerged as a prominent target, reflecting attackers' growing focus on financially and operationally sensitive organizations.

A defining feature of the 2025 ransomware threat environment is the expanding integration of artificial intelligence (AI) into attacker tactics, techniques, and procedures. Ransomware groups increasingly leverage automation, data-driven reconnaissance, and advanced social engineering to improve reconnaissance accuracy, phishing effectiveness, and evasion of security controls. At the same time, organizations across the Arab region are accelerating the adoption of AI-enabled detection, response, and resilience capabilities, contributing to a dynamic and competitive offensive–defensive landscape.

The primary objective of this report is to provide decision-makers, policymakers, and cybersecurity practitioners with actionable intelligence to better understand and respond to the evolving ransomware threat. By analyzing recent trends, identifying sectoral and geographic risk concentrations, and mapping observed activity to the MITRE ATT&CK framework, the report aims to support informed strategic planning and strengthened cyber resilience. The findings presented here are derived from a combination of open-source intelligence (OSINT), darknet monitoring, and data shared through the Cyber Threat Intelligence (CTI) platform operated by NAUSS. Experts from the Centre for Cybercrime and Economic Crime have played a key role in collecting, validating, and interpreting the data used in this report.

This report covers the following areas:

1. Analysis of ransomware incidents in 2025: Examines ransomware attack patterns across Arab countries, including analysis by victim organization, industry sector, geographic distribution, and observed tactics, techniques, and procedures (TTPs).

2. Status of major ransomware gangs in 2025: Assesses the activity, targeting behavior, and operational methods of the most active ransomware groups in the region, including CL0P, Qilin, and Kill Security, while noting shifts in prominence and the relative decline of previously dominant actors such as LockBit.

3. Ransomware preparedness and damage recovery in 2025: Presents strategic and operational measures for ransomware prevention, incident response, and post-incident recovery, with emphasis on organizational resilience and continuity.

4. AI in ransomware threats and defense: Explores the dual role of AI in the 2025 ransomware landscape, examining how threat actors leverage AI to enhance attack effectiveness, and how defenders deploy AI-driven technologies to detect, mitigate, and respond to ransomware incidents in near real time.

Scope and Data Coverage

This report analyzes ransomware activity affecting Arab countries during the period 1 January to 31 December 2025, covering 14 Arab countries. The unit of analysis is the distinct victim organizations publicly named on ransomware leak sites. Victim counts reflect claims posted by ransomware actors, corroborated through open-source intelligence and NAUSS CTI analyst validation, rather than legal confirmation of compromise.

The final analytical dataset consists of 147 distinct victim organizations identified during 2025. These figures represent observed and validated cases within the defined scope and should be interpreted as a conservative estimate of regional ransomware activity.

Data Collection Sources:

- Dark-web leak portals monitored by NAUSS (primary)
- OSINT: vendor reports, media/regulatory disclosures
- NAUSS CTI submissions and expert validation

Classification & Counting Rules:

- Sectors follow the CISA taxonomy for year-over-year consistency
- Country: the victim organization's country named in the leak post; for multinationals, the country explicitly named or the most directly impacted local subsidiary is used.
- Deduplication: multiple posts about the same organization/event count once; re-extortion reposts do not increase totals
- Actors follow self-identification on leak sites; conflicting attributions are flagged "uncertain"
- TTPs are mapped to MITRE ATT&CK where available in source material

Limitations

Ransomware leak-site data does not represent full incident visibility. Under-reporting, selective disclosure, and actor posting bias are expected. Accordingly, victim counts presented in this report should be interpreted as a lower bound of true ransomware activity in the region.

2025 Geographic Orientation

During 2025, ransomware activity was concentrated in a subset of countries. The most affected countries by observed victim count were the United Arab Emirates (38), Saudi Arabia (31), and Egypt (24). A full country-level breakdown is provided in the Victim Country section.

Ransomware Hit Organizations

In 2025, a total of 147 victim organizations in Arab countries were reported on the darknet as having been targeted by ransomware gangs. This represents a significant increase compared to the 96 organizations identified in 2024, continuing the year-over-year upward trajectory that has been evident since 2020, as shown in Figure 1.

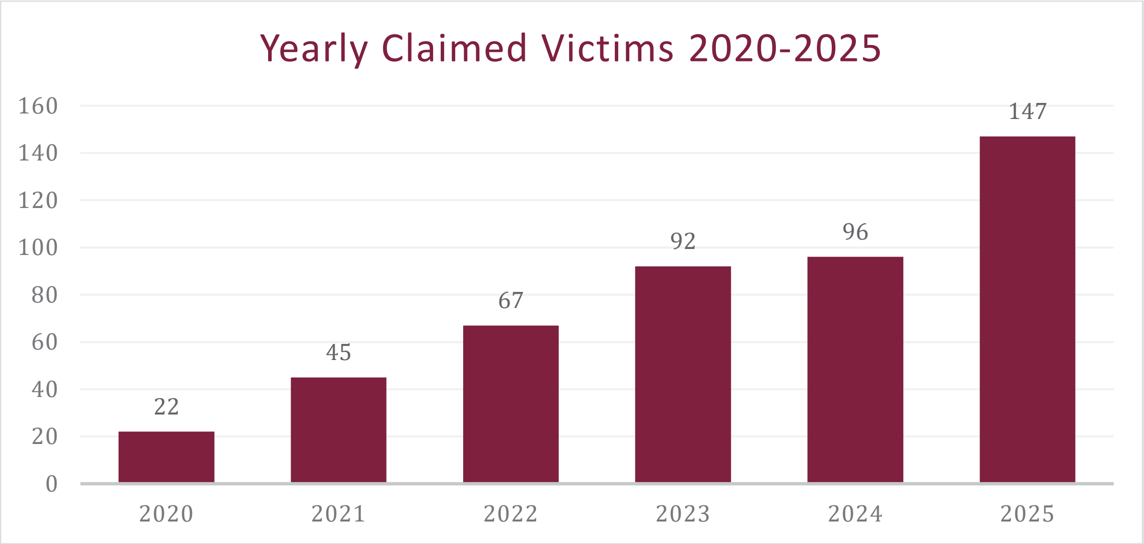


Figure 1. Claimed victim organizations by Ransomware

The monthly statistics for 2025 reveal that ransomware incidents were distributed throughout the year, highlighting that such threats are not confined to specific seasons or timeframes. However, the 2025 data shows a clear Q4 increase, with a notable steady rise beginning around September–October. November 2025 is the peak month with a clear spike in activity. This pattern is consistent with operational realities such as reduced staffing during holidays, year-end change freezes, and intensified commercial activity, as shown in Figure 2.

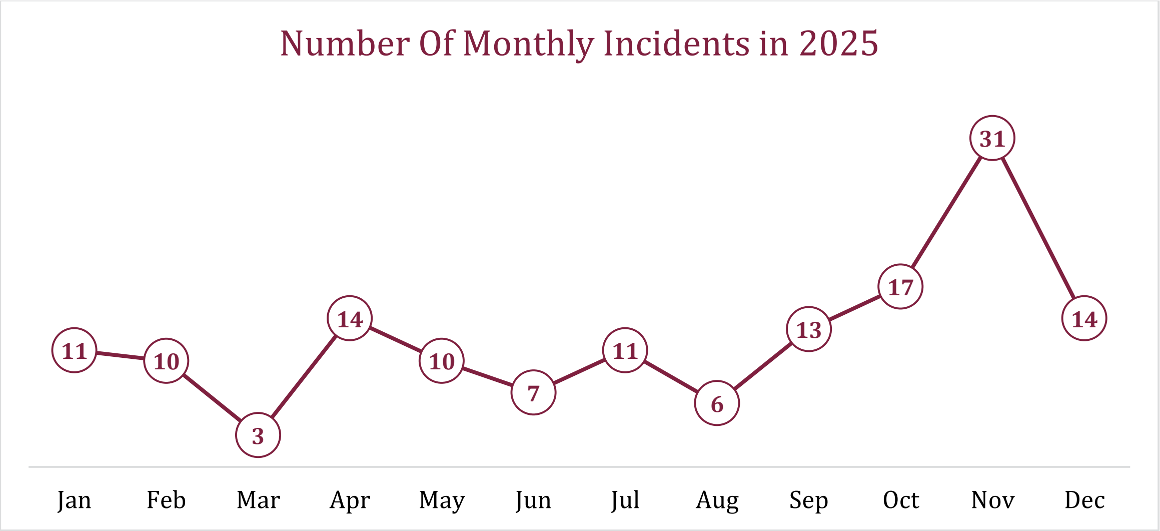


Figure 2. Number of Monthly Incidents in 2025

In 2024, the impact of these attacks extended beyond operational disruption to include large-scale exposure of sensitive and personal data. In 2025, compromised data included usernames, passwords, national IDs, bank statements, client records, employee details, medical records, and photographs, mirroring the patterns of data leakage reported in 2023, particularly within the Government Facilities sector. These breaches demonstrate the consistent risks ransomware poses to both institutional security and individual privacy, reinforcing the urgent need for stronger data protection and incident response measures.

Ransomware Hit Industries

In 2025, ransomware attacks in Arab countries affected 12 CISA-defined industry sectors, reflecting a broad but uneven distribution of threat activity across critical economic domains, as illustrated in Figure 3. The Commercial Facilities sector emerged as the most heavily targeted, accounting for 44 incidents, representing the single largest concentration of ransomware activity. This was followed by Critical Manufacturing with 23 incidents, and Financial Services with 16 incidents. Together, these three sectors accounted for the majority of ransomware cases reported in 2025, underscoring attackers' continued focus on organizations with high operational dependency and strong ransom-paying capacity.

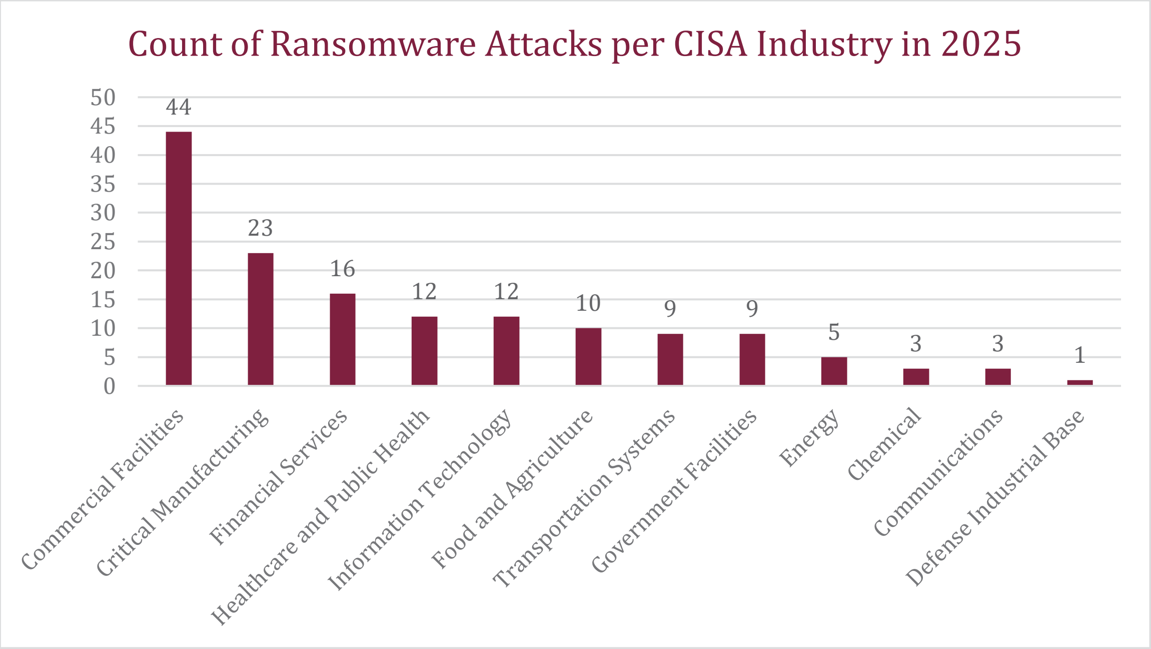


Figure 3. Number of Ransomware Attacks per CISA Industry in 2025

Figure 4 shows a comparison with 2024, highlighting a clear shift in targeting priorities. In 2024, ransomware activity was more evenly distributed across sectors, with Critical Manufacturing (21 incidents) and Commercial Facilities (20 incidents) occupying the top positions, followed by Government Facilities (11 incidents) and Information Technology (8 incidents). The Energy sector, which recorded 6 incidents in 2024, experienced a relative decline in 2025, both in absolute numbers and ranking. Conversely, Financial Services showed a marked increase, rising from 7 incidents in 2024 to 16 incidents in 2025, signaling a renewed focus on financially driven targets.

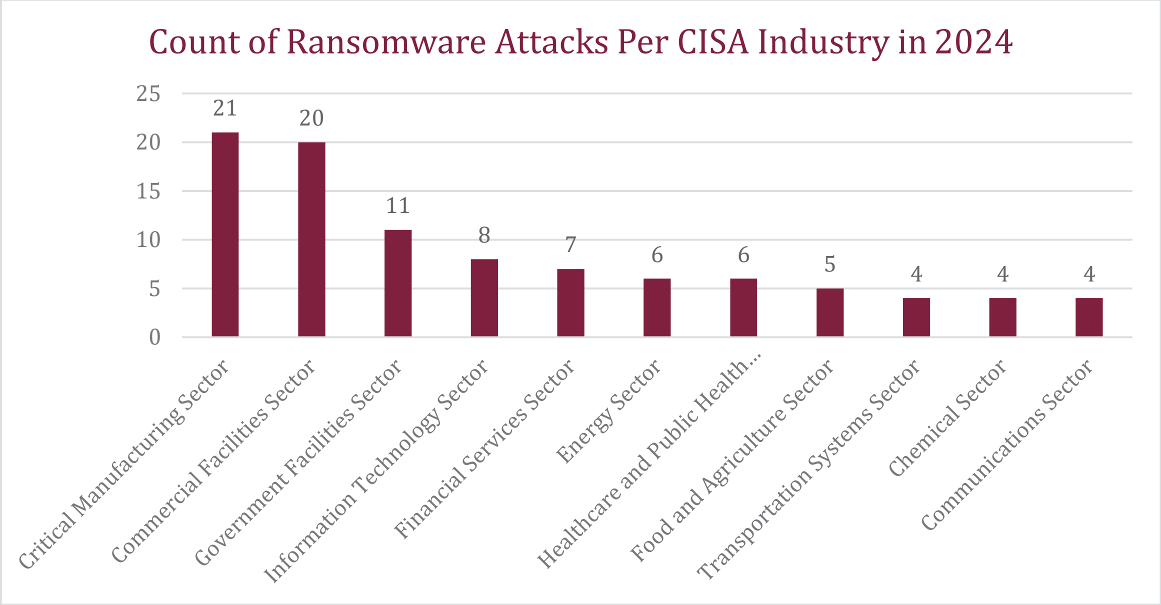


Figure 4. Number of Ransomware Attacks per CISA Industry in 2024

Overall, the 2024–2025 comparison demonstrates that ransomware targeting in Arab countries is not static but adaptive. Sectoral exposure fluctuates in response to economic value, defensive maturity, and geopolitical relevance, reinforcing the need for sector-specific cybersecurity strategies, proactive threat intelligence sharing, and resilience planning tailored to each industry's operational context.

Across the period from 2020 to 2025, ransomware targeting patterns in Arab countries reveal a clear and evolving focus on sectors where operational disruption yields maximum leverage, as shown in Figure 5. Commercial Facilities have remained a consistently high-value target throughout the years, experiencing fluctuations but maintaining sustained exposure through 2024 and 2025. Critical Manufacturing showed significant volatility, declining sharply after 2020 before resurging strongly in 2025 to become the most targeted sector, reflecting renewed attacker interest in industrial environments and supply chains. Government Facilities emerged as a notable target beginning in 2024 and remained relevant in 2025, signaling increased ransomware pressure on public institutions. Overall, these shifts highlight the adaptive nature of ransomware groups and emphasize the necessity of sector-specific defenses, continuous threat intelligence, and resilience strategies aligned with changing attacker priorities.

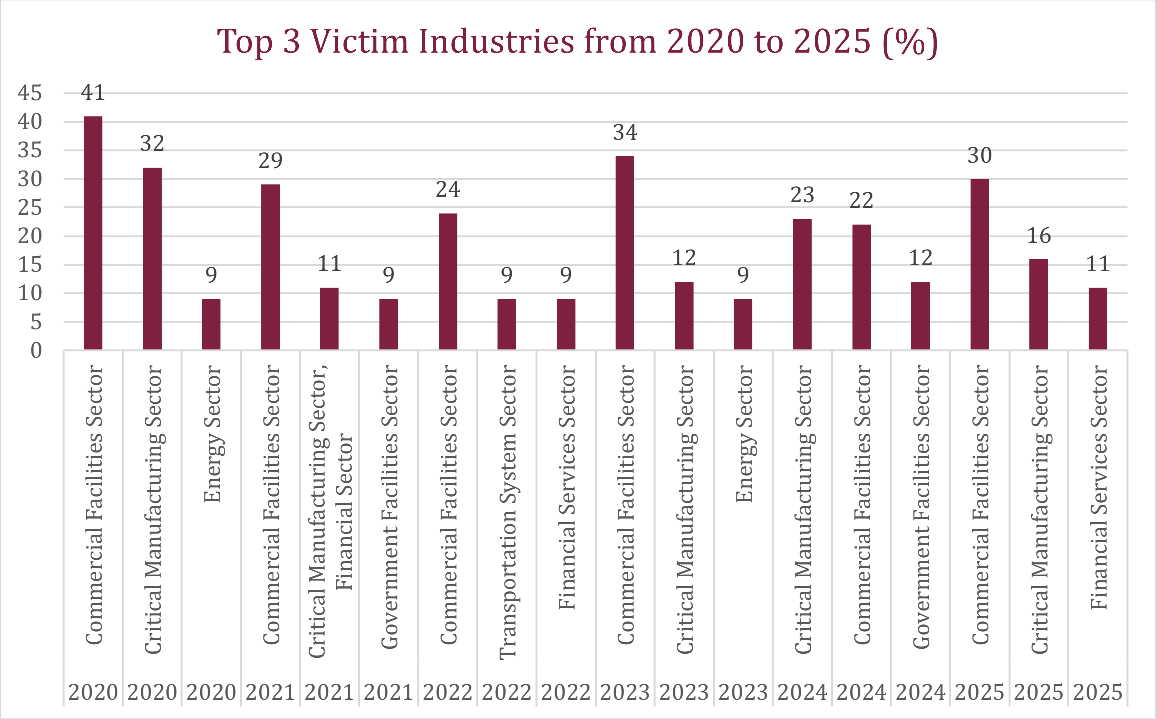


Figure 5. Top 3 victim industry sectors from 2020 to 2025

Countries Affected in the Arab Region

In 2025, ransomware gangs targeted organizations across 14 Arab countries, underscoring the continued regional spread and intensification of ransomware activity, as illustrated in Figure 6. The United Arab Emirates recorded the highest number of incidents with 38 confirmed attacks, followed by Saudi Arabia with 31 and Egypt with 24, together accounting for a substantial share of all reported cases. Jordan and Morocco each experienced 10 attacks, while Kuwait reported 8 incidents. Tunisia and Oman followed with 6 and 5 attacks, respectively. Lower but still notable activity was observed in

* Note: Our classification is based on information derived from the Cybersecurity and Infrastructure Security Agency (CISA).

Bahrain (4), Qatar (3), and Algeria (3). Lebanon and Iraq each recorded 2 incidents, while Palestine reported 1 attack. Overall, the 2025 distribution reflects both a concentration of ransomware activity in economically and digitally mature states and a persistent threat presence across the wider region, reinforcing the need for coordinated regional preparedness and intelligence sharing.

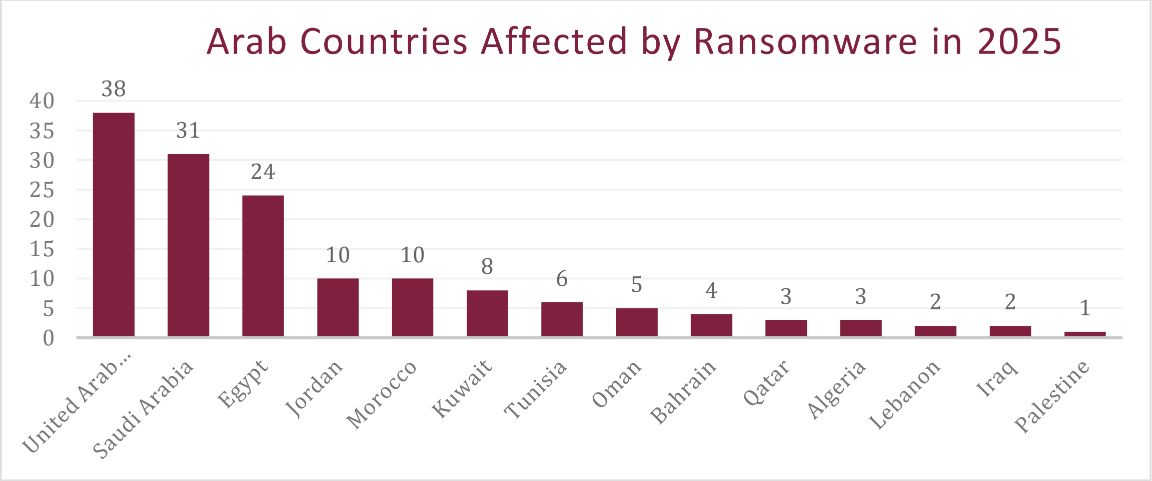


Figure 6. Arab Countries Affected by Ransomware in 2025

In 2024, ransomware gangs targeted organizations across 15 Arab countries, highlighting the widespread nature of the threat in the region, as shown in Figure 7. The United Arab Emirates experienced the highest number of attacks, with 26 confirmed incidents, followed by Saudi Arabia with 17, and Egypt with 11. Oman reported 9 attacks, while Lebanon faced 7. Tunisia followed closely with 6 incidents. Both Kuwait and Libya recorded 4 attacks each. Qatar, Sudan, and Yemen each experienced 2 attacks. Meanwhile, Jordan, Morocco, Djibouti, and Iraq reported the fewest cases, with 1 attack each.

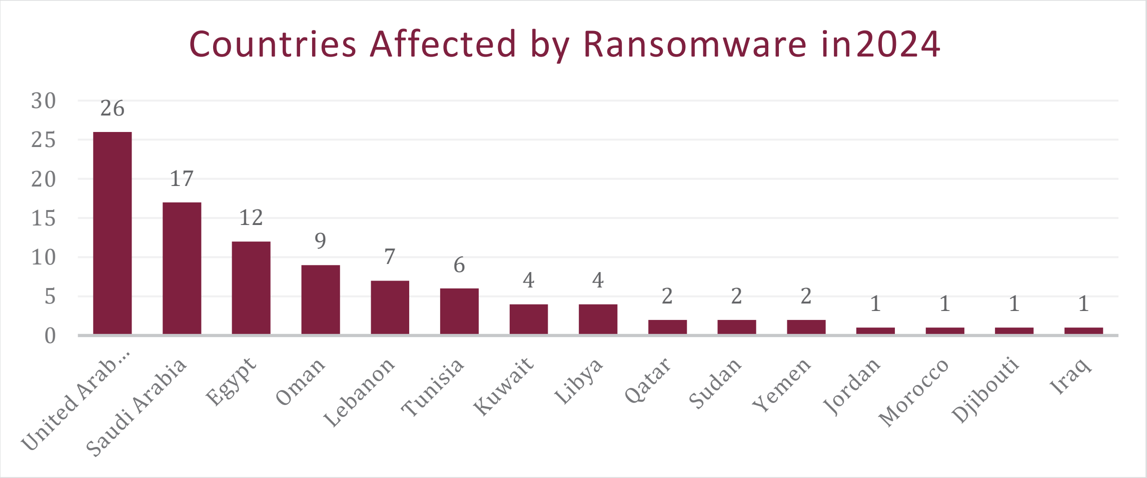


Figure 7. Arab Countries Affected by Ransomware in 2024

Figure 8 illustrates the evolution of ransomware targeting patterns across the Arab region from 2020 to 2025. The United Arab Emirates (UAE) experienced a notable decline in its share of attacks from 55% in 2020 to 27% in 2022, while remaining the most frequently targeted country. This share increased to 34% in 2023 before decreasing to 27% in 2024. In 2025, although the absolute number of incidents rose substantially, the UAE accounted for approximately 26% of all reported attacks, reaffirming its position as the primary ransomware target in the region.

Saudi Arabia exhibited a gradual upward trend over the observed period, increasing from 14% in 2020 to 17% in 2022 and reaching 18% in 2024. In 2025, Saudi Arabia's share rose further to approximately 21%, indicating a clear escalation in ransomware exposure. Egypt, which shared third place in 2020 alongside Oman at 9%, emerged as the second most targeted country in 2024 with approximately 13% of recorded incidents and continued this upward trajectory in 2025, accounting for about 16% of attacks. Overall, these trends demonstrate an increasing concentration of ransomware activity within a small number of key regional states, underscoring the need for sustained, coordinated cybersecurity strategies and enhanced regional intelligence sharing to address the evolving threat landscape.

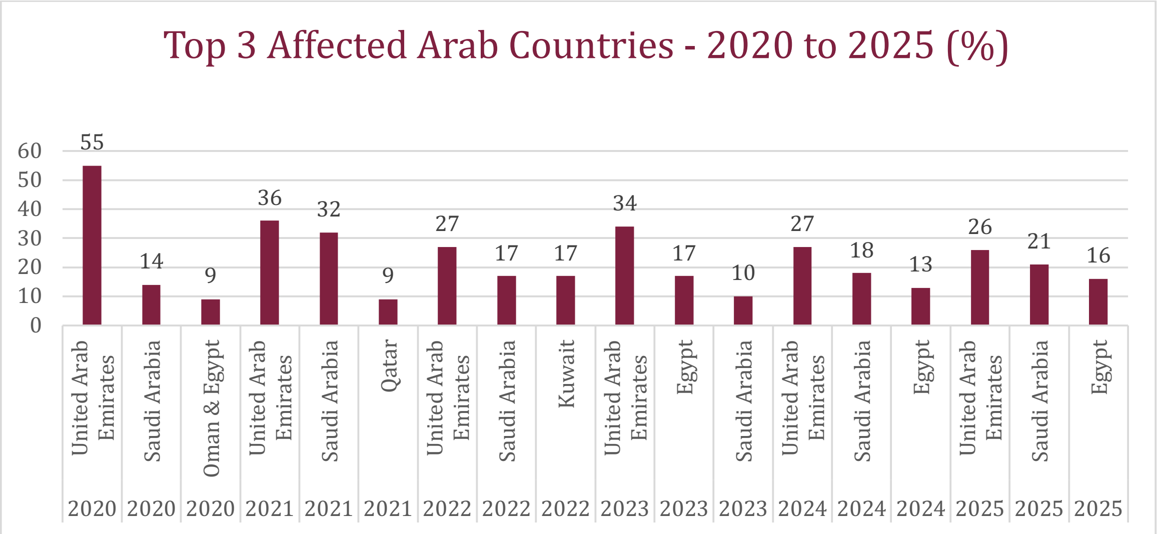
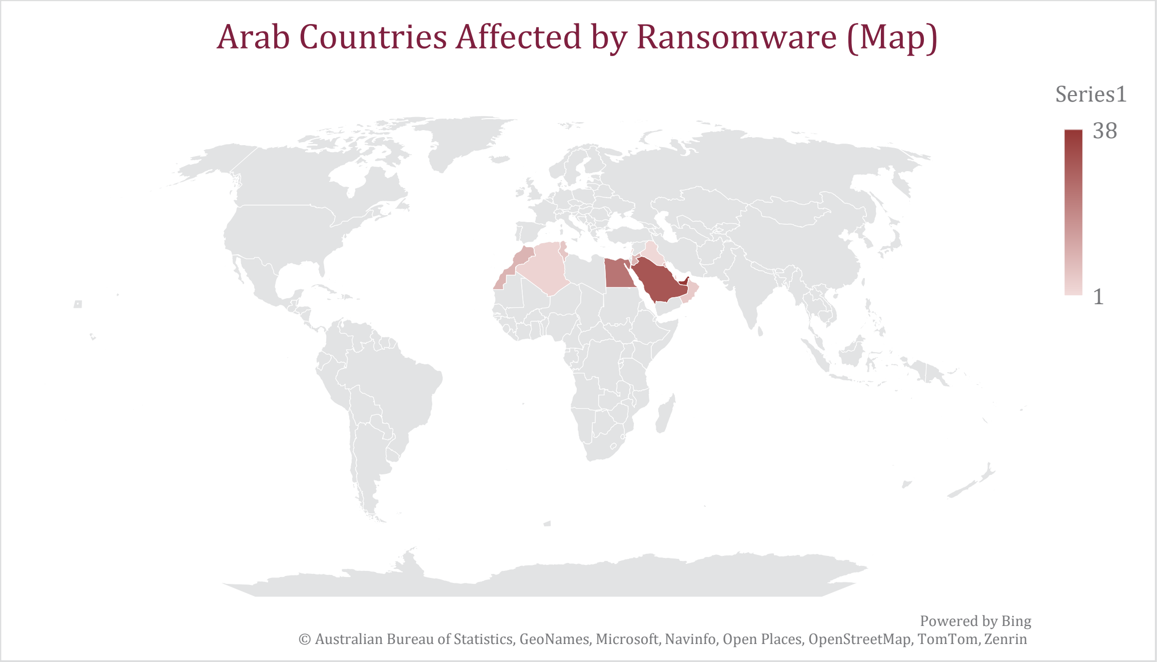


Figure 8. Top 3 Affected Arab countries by Ransomware from 2020 to 2025

A closer examination of the provided data reveals a complete picture of ransomware attacks across the Arab World. The map shown in Figure 9 highlights countries that have been targeted by such attacks, including the United Arab Emirates, Saudi Arabia, Egypt, Iraq, Jordan, Kuwait, Lebanon, Morocco, Oman, Qatar, Saudi Arabia, Tunisia, and Djibouti. The intensity of attacks is depicted by darker shades on the map, indicating a widespread impact across the region.



Arab Countries Affected by Ransomware (Map)
Series1
38
1
Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

Figure 9. Arab Countries Affected by Ransomware (Map)

Industry-Specific Insights in Context of Geographic Distribution in 2025

In 2025, the geographic distribution of ransomware attacks continued to closely reflect the concentration of high-value industries across the Arab region. The United Arab Emirates, Saudi Arabia, and Egypt remained the most heavily targeted countries, with ransomware activity concentrated in Commercial Facilities, Critical Manufacturing, Financial Services, Healthcare and Public Health, and Government Facilities. This pattern indicates a deliberate focus on sectors whose disruption carries significant economic, operational, and societal impact.

In the UAE, ransomware groups primarily targeted commercial facilities, including retail, hospitality, logistics, and financial services, particularly in major economic hubs. Saudi Arabia experienced expanded targeting across critical manufacturing, energy-adjacent sectors, commercial enterprises, and government entities, reflecting attackers' interest in both economic leverage and sensitive institutional data. In Egypt, ransomware activity remained more diversified, with attacks spanning commercial, financial, transportation, and government sectors, underscoring growing exposure as digital transformation accelerates.

These regional trends align with broader EMEA findings in Verizon's 2025 DBIR, where financially motivated external actors dominate system intrusion and social engineering attacks. Overall, the 2025 data confirms that ransomware groups are strategically prioritizing countries with dense clusters of economically and operationally critical sectors, reinforcing the need for sector-specific defenses, cross-border intelligence sharing, and coordinated regional response strategies.

Ransomware Actors

As shown in Figure 10, CL0P, Qilin, and Kill Security were the three most active ransomware groups targeting Arab countries in 2025. CL0P emerged as the leading actor, maintaining a high operational tempo and continuing its focus on large-scale, high-impact intrusions across multiple sectors, particularly through exploitation of public-facing applications and data exfiltration–driven extortion. Qilin followed closely, demonstrating sustained activity and a consistent reliance on phishing and exposed remote services to compromise organizations across commercial, government, and critical infrastructure sectors.

Kill Security also stood out as a major threat actor in 2025, reflecting the growing fragmentation and diversification of the ransomware ecosystem. Its activity across healthcare, commercial facilities, and information technology sectors highlights how newer or rebranded groups are filling the operational space left by previously dominant actors. In contrast, LockBit, which dominated earlier reporting periods, showed a clear decline in regional activity. This reduction is likely linked to the exposure and international sanctioning of its leadership in 2024, which significantly disrupted its operational capacity.

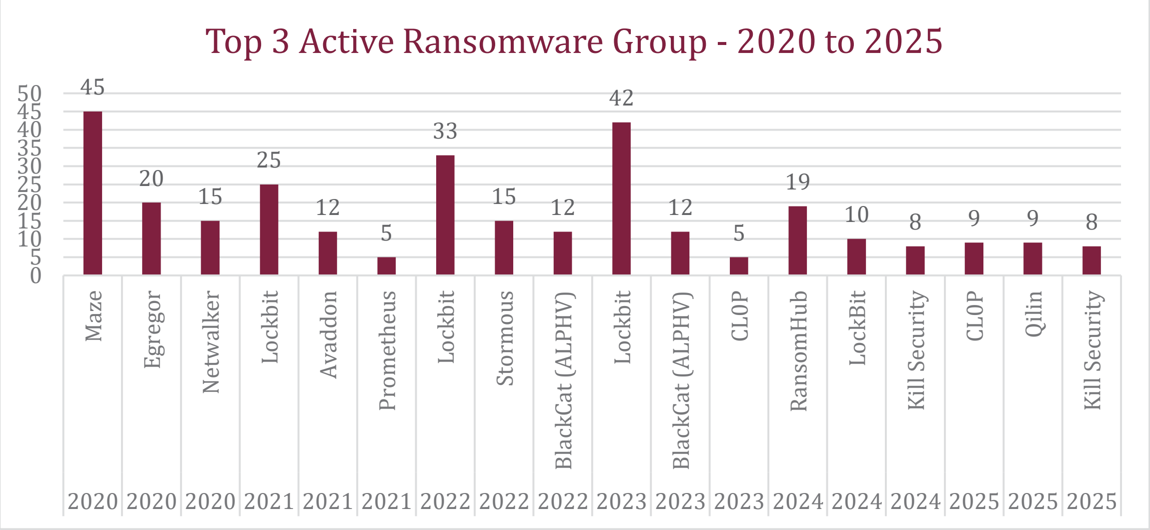


Figure 10. Top 3 active Ransomware Groups from 2020 to 2025

The year 2025 marked a further reshaping of the ransomware threat landscape in the Arab world, as shown in Figure 11. CL0P and Qilin emerged as the most active ransomware groups, each linked to 9 confirmed attacks across multiple countries and sectors. Close behind, INC Ransom and Kill Security each accounted for 8 attacks, highlighting a highly competitive and fragmented ransomware ecosystem rather than dominance by a single actor, all highlighted below.

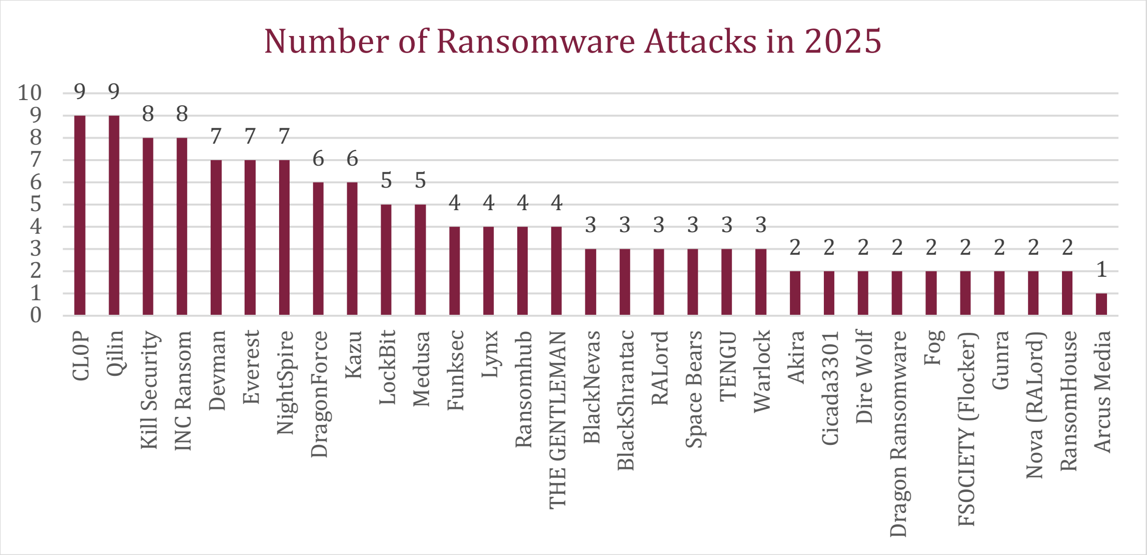


Figure 11. Number of Ransomware Attacks in 2025

In 2024, Ransomhub emerged as the most active ransomware group, responsible for 19 confirmed attacks across various sectors in the Arab world. LockBit, though previously dominant, ranked second with 10 attacks, followed by Kill Security with 9 attacks. Other notable groups include DragonForce, DarkVault, Qilin, and Sarcoma Group, each linked to 4–5 incidents,as shown in Figure 12. While many ransomware gangs conducted only a handful of attacks, the rising activity of groups like Ransomhub and Kill Security signals a shift in the threat landscape. These groups are not only targeting high-profile industries but are also expanding their reach to a broader set of sectors and countries.

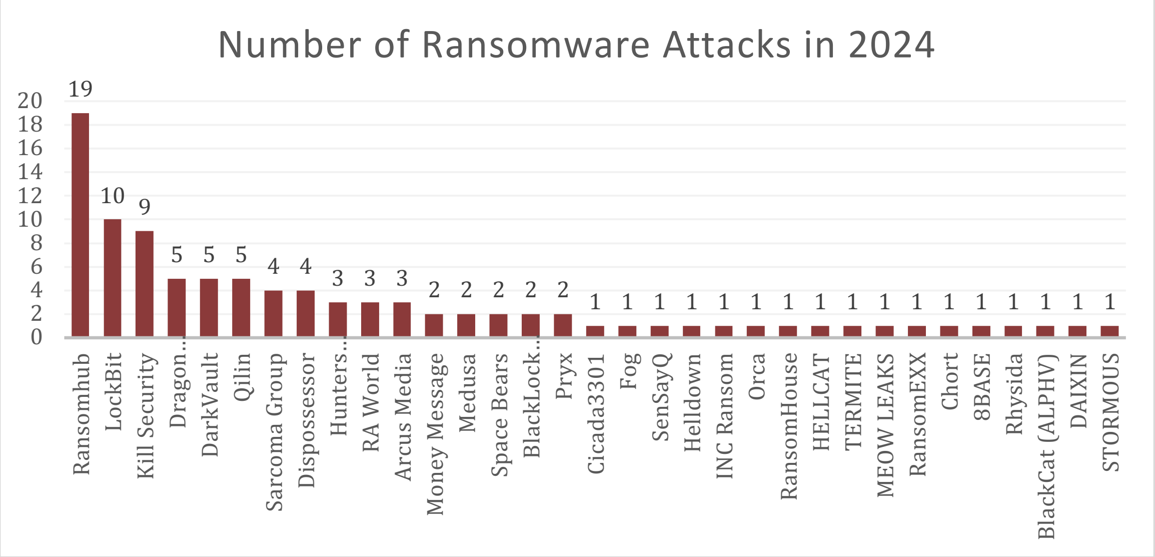


Figure 12. Number of Ransomware Attacks in 2024

AI-Driven Trend Evolution of Ransomware in Arab Countries (2020–2025)

Ransomware activity in Arab countries between 2020 and 2025 demonstrates a clear evolution in scale, organization, and technological sophistication, as shown in Figure 13. The data reveals three overlapping phases that reflect how ransomware operations matured and how AI increasingly shaped attacker behavior.

From 2020 to 2021, ransomware activity remained relatively limited and opportunistic. Attacks were largely manual, relying on basic phishing, exposed services, and publicly known vulnerabilities. Groups such as Maze and Egregor focused on commercially active sectors, particularly Commercial Facilities and Critical Manufacturing, with minimal automation and little evidence of AI-enabled tooling.

Between 2022 and 2023, ransomware operations entered a consolidation phase marked by rapid growth in victim numbers and the dominance of structured ransomware-as-a-service (RaaS) ecosystems. LockBit and BlackCat (ALPHV) exemplified this shift, benefiting from standardized attack playbooks, affiliate networks, and improved operational efficiency. While AI was not yet central, automation became more visible through scripted reconnaissance, credential harvesting, and scalable phishing campaigns.

The 2024–2025 period represents a decisive transformation. Following the disruption of major legacy gangs, the ransomware ecosystem fragmented, allowing groups such as CL0P, Qilin, Kill Security, and RansomHub to rise quickly. This phase is characterized by the integration of AI-augmented techniques, enabling faster reconnaissance, improved victim profiling, more convincing phishing content, and accelerated lateral movement. The sharp increase in victim counts in 2025 reflects not only more actors but also significantly enhanced scalability. Attacks are increasingly concentrated on high-value economies such as the United Arab Emirates, Saudi Arabia, and Egypt, with Financial Services joining Commercial Facilities and Critical Manufacturing as priority targets.

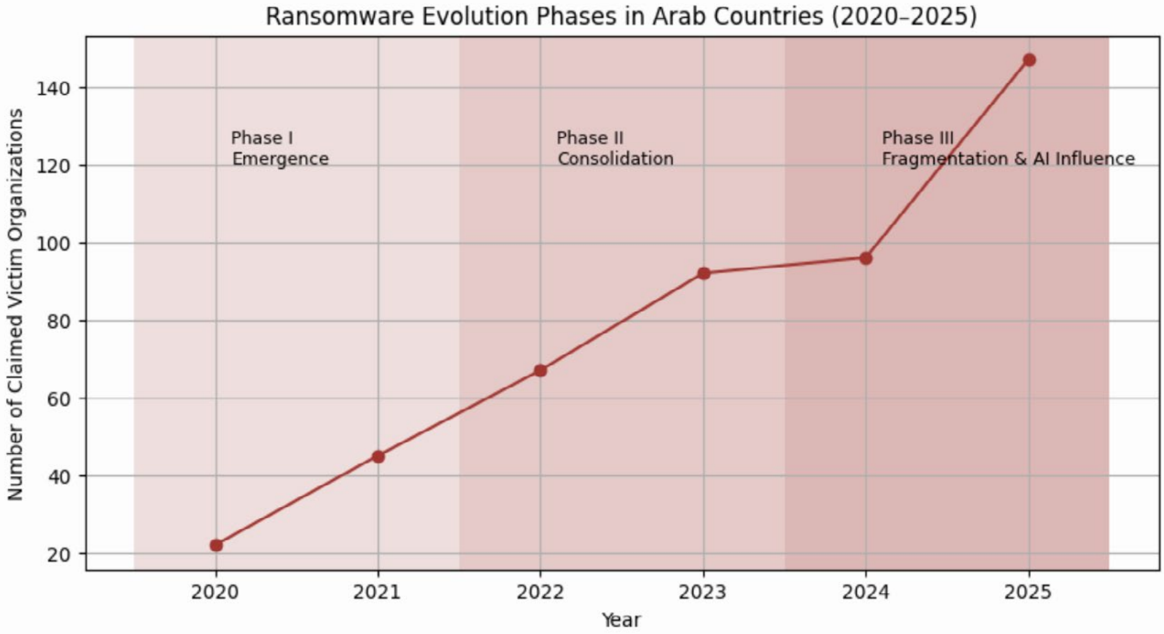


Figure 13. Ransomware Evolution Phase in Arab Countries (2020-2025)

AI-Driven Policy and Regulatory Implications

This evolution has direct implications for national cybersecurity policy and regional governance. Europol’s threat assessments highlight that cybercriminals are increasingly leveraging AI to improve the speed, scale, and effectiveness of digital crime, including more effective social engineering and greater exploitation of exposed data and the identity ecosystem [1]. The concentration of ransomware activity in economically critical sectors supports the introduction of sector-specific cybersecurity mandates and minimum baseline controls, particularly for commercial, financial, and manufacturing entities that may fall outside traditional critical infrastructure protections. Accordingly, this report recommends strengthening regulatory and governance measures to reduce AI-related risk and limit downstream exploitation. For the most targeted sectors, especially Commercial Facilities, priorities should include stronger controls on sensitive data exposure, improved identity assurance, and tighter access governance for high-risk systems.

The Use of Artificial Intelligence in Ransomware Attacks

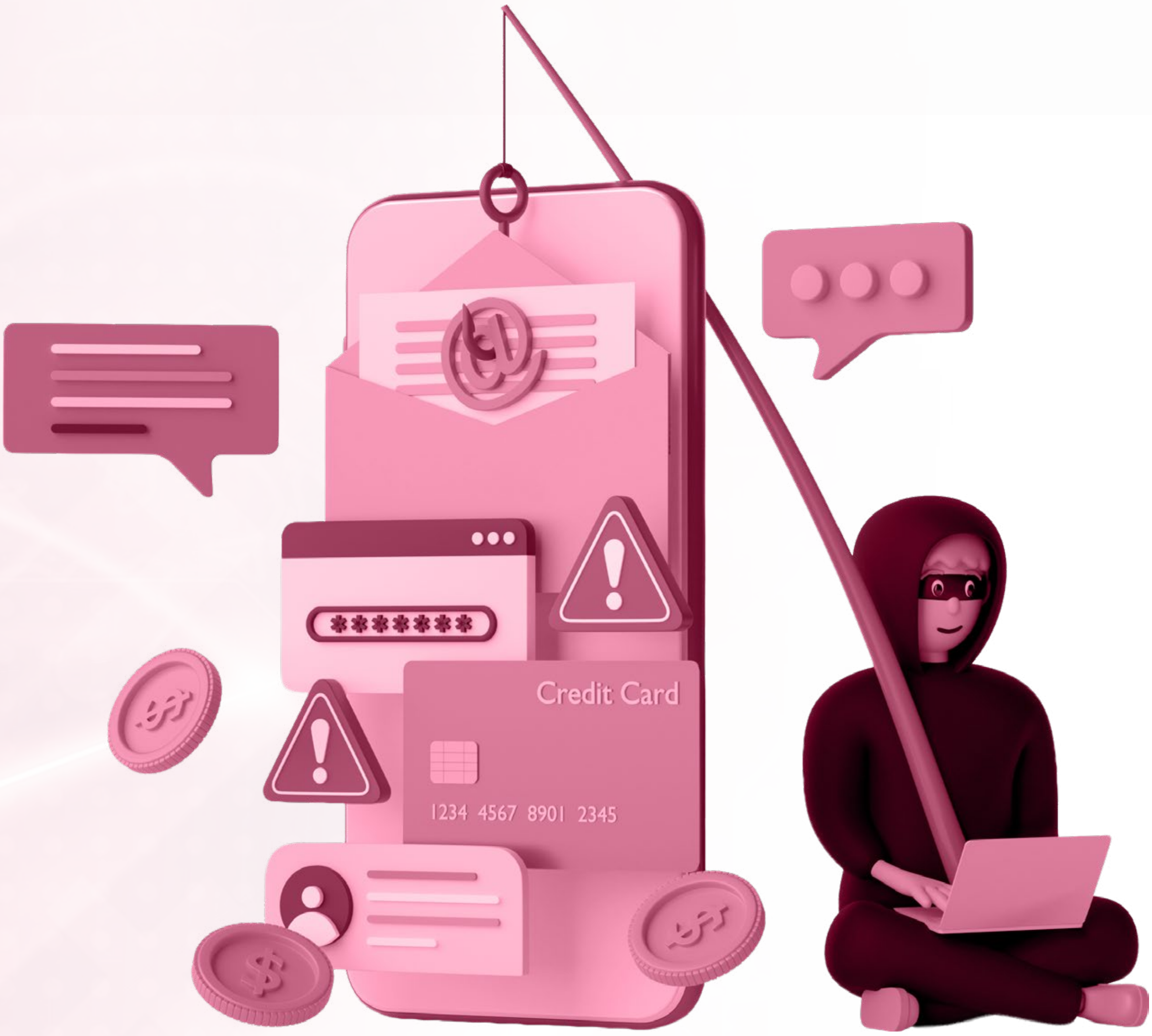
Recent threat intelligence assessments indicate that AI, and particularly generative AI (GenAI), is increasingly shaping how cybercrime operations are prepared and scaled. However, public reporting and open-source data rarely allow confident attribution of specific GenAI tooling to individual ransomware intrusions. As a result, AI is best treated as an ecosystem-level enabler that improves attacker efficiency rather than as a replacement for core ransomware techniques [2].

The impact of GenAI is most evident in social engineering and phishing. GenAI can increase the speed, linguistic quality, and localization of malicious email content, lowering the effort required to produce credible lures at scale. Verizon’s 2025 DBIR reports that synthetically generated text in malicious emails has doubled over the past two years, reinforcing the assessment that GenAI is already contributing to measurable changes in malicious email operations [3].

This aligns with the findings of this report, where phishing remains a dominant initial access pathway across the 2020–2025 period. Within this broader environment, the most active ransomware actors observed in 2025, including CL0P, Qilin, INC Ransom, and Kill Security, continue to rely on well-established intrusion chains where improved social engineering directly increases operational effectiveness. Consistent with the MITRE ATT&CK mappings in this report, phishing (T1566) and related user execution (T1204) behaviors remain recurring components of ransomware tradecraft. Accordingly, GenAI should be treated here as a force multiplier that strengthens existing pathways used by active ransomware actors, even when group-level attribution of GenAI usage is not directly observable from public data.

In addition, available evidence indicates that AI has not fundamentally changed the core structure of ransomware attacks. Instead, it optimizes execution by improving scale, speed, and adaptability across the attack lifecycle [4].

Overall, AI in ransomware operations should be understood as an accelerator of established criminal models rather than a paradigm shift. This reinforces the need for policy frameworks addressing AI misuse, stronger sector-specific cyber resilience, and enhanced regional intelligence sharing to counter increasingly automated and data-informed ransomware threats.



Observed ATT&CK Tactics and Techniques

In previous reporting periods, ransomware operations in the Arab region followed a relatively consistent tactical pattern, with strong emphasis on Initial Access, Execution, Lateral Movement, and Impact, reflecting attackers' focus on gaining entry, expanding access, and maximizing disruption through encryption. Earlier years showed particularly high reliance on Initial Access techniques, driven by phishing and exposed services, while Credential Access and Privilege Escalation played supporting roles in enabling broader network compromise.

In 2025, this pattern remains largely intact but becomes more balanced and mature, as illustrated in Figure 14. Initial Access continues to dominate, accounting for the largest share of observed tactics at 18%, underscoring the persistent exploitation of human and perimeter weaknesses. Impact follows at 11%, highlighting the continued centrality of encryption and disruption in ransomware operations. Other tactics, such as Execution, Defense Evasion, Discovery, Lateral Movement, Persistence, Credential Access, and Privilege Escalation, each account for a similar proportion, roughly 8–9%, indicating that ransomware groups in 2025 are executing more complete and methodical attack chains rather than relying on isolated techniques. This shift reflects increasing operational maturity, where attackers systematically progress through the full intrusion lifecycle, reinforcing the need for equally comprehensive, defense-in-depth security strategies.

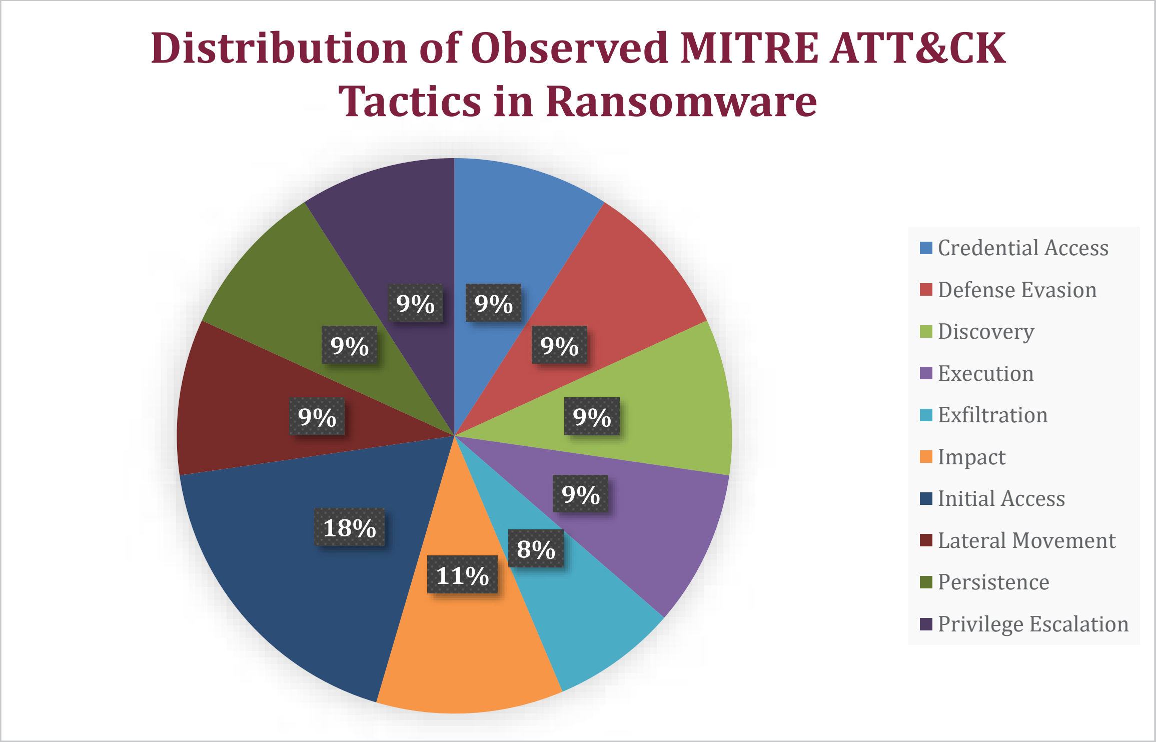


Figure 14. Distribution of Observed MITRE ATT&CK Tactics in Ransomware Operations

Table 1 and Figure 15 show the frequency of various techniques used by ransomware gangs. The data provides insight into the techniques most favored by attackers and can inform defensive strategies for organizations.

Table 1. Frequency of Observed MITRE ATT&CK Techniques

TECHNIQUE	Count of Techniques
T1566 – Phishing	5
T1204 – User Execution	5
T1053 – Scheduled Task/Job	5
T1055 – Process Injection	5
T1027 – Obfuscated Files or Information	5
T1003 – OS Credential Dumping	5
T1018 – Remote System Discovery	5
T1021 – Remote Services	5
T1133 – External Remote Services	4
T1048 – Exfiltration Over Alternative Protocol	4
T1486 – Data Encrypted for Impact	4
T1190 – Exploit Public-Facing Application	1

By focusing on these high-frequency techniques, we can significantly reduce the risk of a successful ransomware attack and minimize the potential damage. We must remember that a layered security approach that combines preventative measures, detection capabilities, and incident response procedures is essential for comprehensive protection.

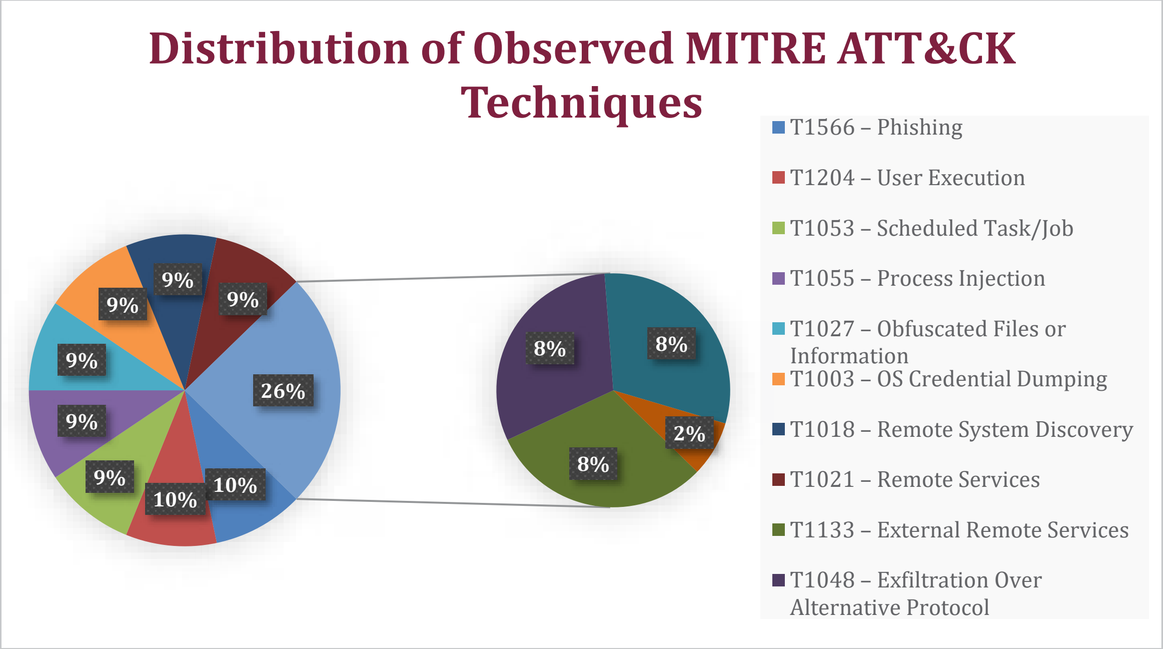


Figure 15. Distribution of Observed MITRE ATT&CK Techniques

Conclusion and Summary of Findings for 2025

The 2025 ransomware landscape in Arab countries confirms ransomware as a persistent and highly adaptive cyber threat, marked by increased operational maturity, broader sectoral targeting, and a more fragmented ecosystem of threat actors. Analysis of incidents throughout the year shows that ransomware activity remains strategically concentrated rather than opportunistic, with attackers prioritizing countries and sectors that offer maximum financial leverage, operational disruption, and reputational impact.

In 2025, ransomware attacks affected 14 Arab countries, with the United Arab Emirates, Saudi Arabia, and Egypt accounting for the majority of incidents. This concentration reflects the high digital adoption, economic scale, and regional influence of these states. From an industry perspective, Commercial Facilities and Critical Manufacturing remained the most targeted sectors, followed closely by Financial Services, Healthcare and Public Health, Government Facilities, and Transportation Systems, indicating a continued focus on sectors where downtime and data exposure are especially costly.

The ransomware ecosystem in 2025 was characterized by a shift in dominant threat actors. While previously dominant groups such as LockBit showed reduced activity, CL0P, Qilin, and Kill Security emerged as the most active ransomware gangs targeting the region. These groups demonstrated consistent use of double-extortion models, structured attack lifecycles, and well-established MITRE ATT&CK techniques, favoring reliability and scalability over novel exploits. Their sustained activity highlights how quickly the threat landscape evolves as new or existing groups adapt to law-enforcement pressure and operational disruption.

From a tactical standpoint, ransomware operations in 2025 exhibited balanced and methodical use of the full attack lifecycle. Initial access techniques, particularly phishing and exploitation of exposed services, remained dominant, while credential access, lateral movement, and data exfiltration were systematically employed to maximize impact. The increased visibility of AI in an offensive context further shaped the threat environment, enabling more efficient reconnaissance and social engineering on the attacker's side.

Overall, the 2025 findings underscore the need for sector-specific cybersecurity strategies, strengthened credential and access controls, continuous threat intelligence sharing, and regionally coordinated response frameworks. As ransomware groups continue to adapt and diversify, resilience in the Arab region will increasingly depend on proactive, intelligence-driven defense measures aligned with evolving attacker behavior rather than reactive incident response alone.

Appendices

Ransomware Group Analysis - CL0P

CL0P is a well-established ransomware group that has remained highly active and operationally relevant through 2025, demonstrating resilience despite increased law enforcement pressure on major ransomware ecosystems. Unlike groups that emerged after the disruption of LockBit and ALPHV, CL0P has leveraged its long-standing expertise in exploiting public-facing applications, allowing it to sustain large-scale campaigns and remain one of the most prolific ransomware actors targeting Arab countries in 2025. In contrast to the previous reports, where CL0P activity was more episodic, the 2025 data show a clear intensification of its regional focus, positioning CL0P among the top ransomware gangs alongside Qilin and Kill Security.

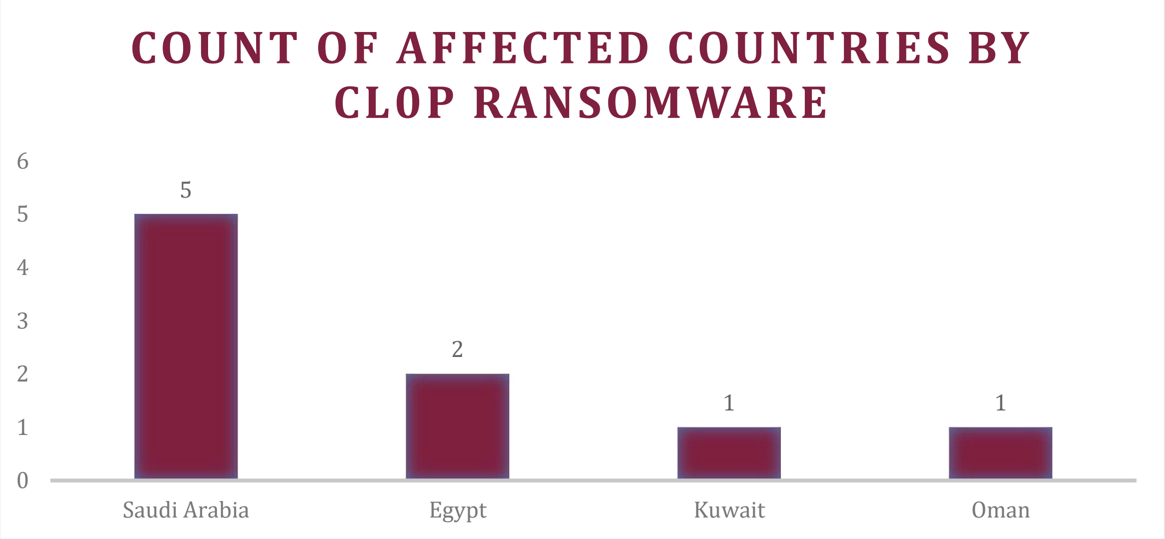
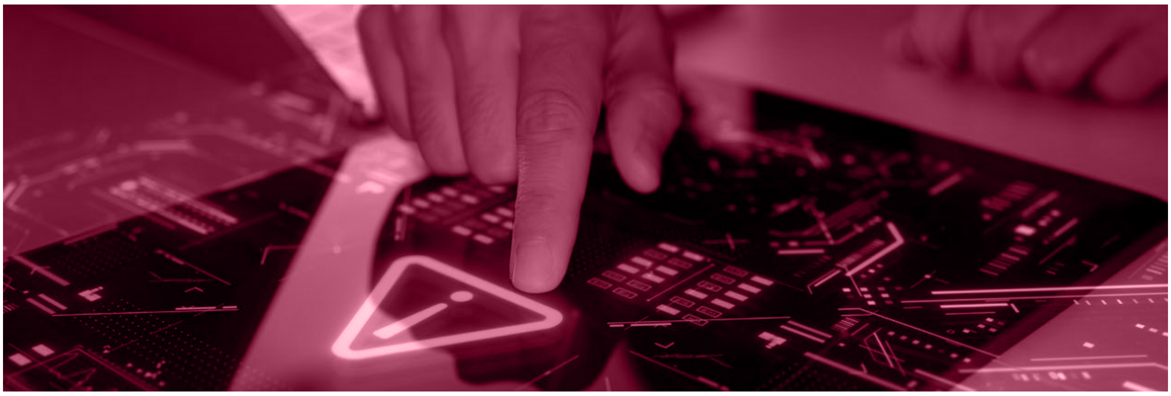


Figure 16. Count of Affected Countries by CL0P Ransomware

CL0P is particularly known for its mass exploitation strategy, targeting vulnerabilities in file-transfer platforms, web applications, and externally exposed services to compromise multiple victims simultaneously. Its operations rely heavily on double extortion, where sensitive data is exfiltrated and publicly leaked if ransom demands are not met, often without immediate encryption in early stages. The pie chart below presents the distribution of CL0P attacks in the Arab region in 2025, which were mainly concentrated on Commercial Facilities, Critical Manufacturing, Financial Services, Information Technology, Energy, and Transportation Systems, reflecting a deliberate focus on organizations with high operational and reputational impact.



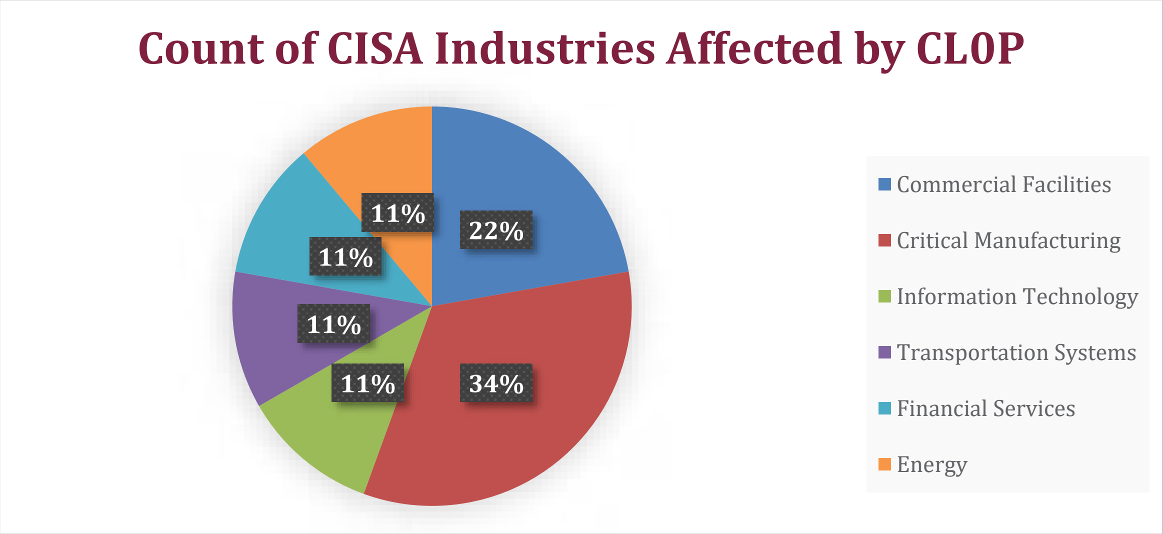


Figure 17. Count of Affected Industries by CL0P Ransomware

From a tactics, techniques, and procedures (TTPs) perspective, CL0P continues to follow a structured and repeatable intrusion lifecycle. Initial access is primarily achieved through exploitation of public-facing applications (T1190), complemented by phishing campaigns (T1566) in select cases. Execution commonly depends on user execution (T1204) once access is established. To maintain persistence, CL0P deploys scheduled tasks (T1053), while process injection (T1055) is used for privilege escalation and to blend malicious activity into legitimate processes. Defense evasion relies heavily on obfuscated files or information (T1027) to bypass endpoint detection tools. Credential access is achieved through OS credential dumping (T1003), enabling lateral movement across the network via remote services (T1021). CL0P conducts internal reconnaissance using remote system discovery (T1018) to identify high-value assets prior to data theft. Exfiltration is carried out through alternative protocols (T1048) designed to evade network monitoring, followed by the primary impact phase, where data is encrypted for impact (T1486) to coerce ransom payment.

Table 2. MITRE ATT&CK Technique Mapping for CL0P Ransomware Operations

CL0P			
Tactic	Technique ID	Technique Name	Description
Initial Access	T1190	Exploit Public-Facing Application	Actively exploits vulnerabilities in file transfer and web applications to gain initial access at scale.
Initial Access	T1566.002	Phishing	Uses phishing emails with malicious links or attachments as a secondary access vector.
Execution	T1204.001	User Execution	Relies on user interaction to execute malicious payloads when phishing is successful.
Persistence	T1053.005	Scheduled Task/Job	Establishes scheduled tasks to maintain persistence across reboots.
Privilege Escalation	T1055.012	Process Injection	Injects malicious code into legitimate processes to elevate privileges.
Defense Evasion	T1027.002	Obfuscated Files or Information	Obfuscates payloads to evade endpoint detection solutions.
Credential Access	T1003.001	OS Credential Dumping	Extracts credentials from memory to enable lateral movement.
Discovery	T1018	Remote System Discovery	Scans internal networks to identify additional systems.
Lateral Movement	T1021.001	Remote Services	Uses legitimate remote services such as SMB and RDP to move laterally.
Exfiltration	T1048.002	Exfiltration Over Alternative Protocol	Exfiltrates sensitive data prior to encryption to enable double extortion.
Impact	T1486	Data Encrypted for Impact	Encrypts victim data to disrupt operations and force ransom payment.

Ransomware Group Analysis - QILIN

Qilin is an increasingly prominent ransomware-as-a-service (RaaS) group that solidified its position as one of the most active ransomware actors targeting Arab countries in 2025. While Qilin was already visible in earlier reporting periods, its operational footprint expanded significantly in 2025, placing it alongside CL0P and Kill Security as a leading threat group in the region. This growth reflects Qilin's ability to rapidly scale operations, recruit affiliates, and adapt proven ransomware tradecraft to a wide range of targets.

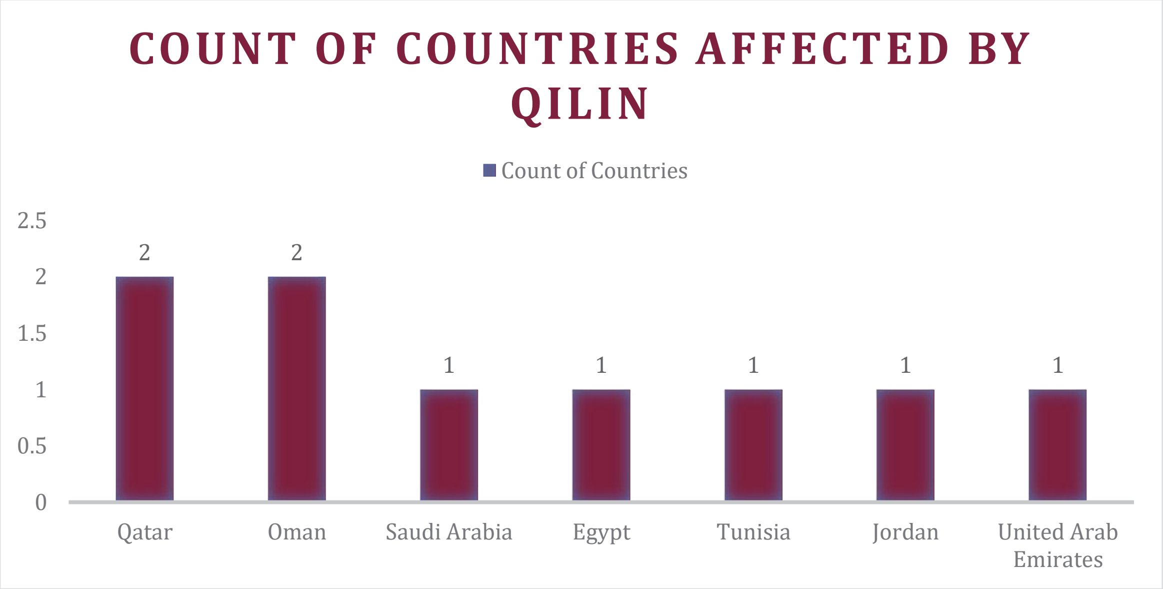


Figure 18. Count of Affected Countries by QILIN Ransomware

Qilin's activity in 2025 shows a deliberate focus on Commercial Facilities, Critical Manufacturing, Government Facilities, Financial Services, Healthcare and Public Health, Food and Agriculture, and Transportation Systems. This sectoral spread indicates a strategy aimed at maximizing both operational disruption and extortion leverage, particularly against organizations with time-sensitive services and regulatory exposure. Unlike exploit-driven groups such as CL0P, Qilin relies heavily on credential-based intrusion methods, enabling persistent access to poorly secured enterprise environments.

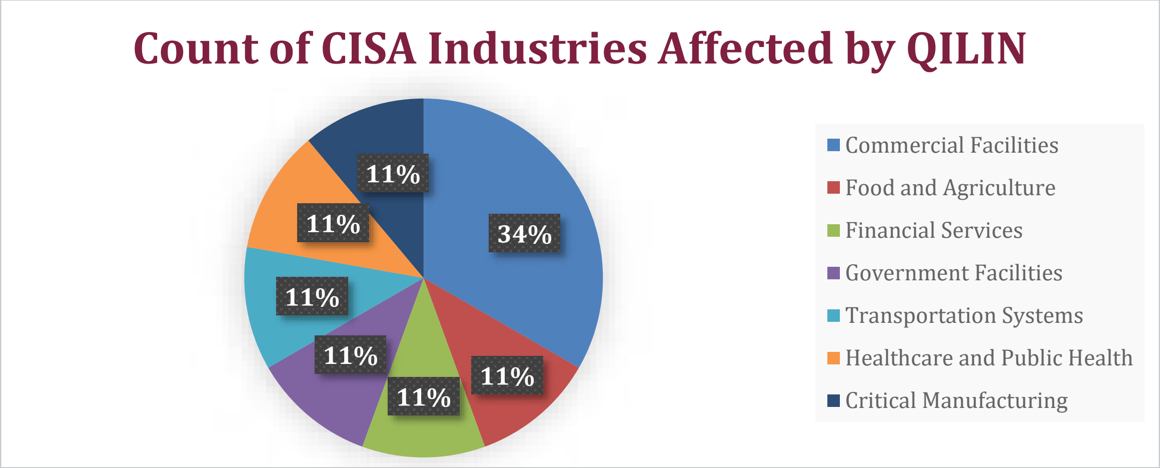


Figure 19. Count of Affected Industries by QILIN Ransomware

From a tactics, techniques, and procedures (TTPs) perspective, Qilin demonstrates a structured attack lifecycle consistent with mature ransomware operations. Initial access is primarily achieved through phishing (T1566) and abuse of external remote services (T1133), including exposed RDP and VPN endpoints. Execution depends on user execution (T1204), often following successful social engineering. Persistence is maintained through scheduled tasks (T1053), while process injection (T1055) is used to escalate privileges and conceal malicious activity within legitimate system processes. To evade detection, Qilin makes extensive use of obfuscated files or information (T1027), allowing payloads and scripts to bypass security controls. Credential harvesting via OS credential dumping (T1003) enables deeper network penetration and supports lateral movement through remote services (T1021). Internal reconnaissance is conducted using remote system discovery (T1018) to identify critical systems and high-value targets. Prior to encryption, Qilin frequently performs data theft using exfiltration over alternative protocols (T1048), reinforcing its double-extortion model. The attack culminates in data encryption for impact (T1486), designed to maximize operational disruption and ransom pressure.

Table 3. MITRE ATT&CK Technique Mapping for QILIN Ransomware Operations

QILIN			
Tactic	Technique ID	Technique Name	Description
Initial Access	T1566.001	Phishing	Uses targeted phishing campaigns to gain footholds in victim environments.
Initial Access	T1133	External Remote Services	Abuses exposed RDP and VPN services for initial access.
Execution	T1204.001	User Execution	Requires user interaction to execute malicious files.
Persistence	T1053.005	Scheduled Task/Job	Maintains access through scheduled tasks.
Privilege Escalation	T1055.012	Process Injection	Injects code into trusted processes to escalate privileges.
Defense Evasion	T1027.002	Obfuscated Files or Information	Obfuscates ransomware binaries and scripts.
Credential Access	T1003.001	OS Credential Dumping	Harvests credentials for privilege escalation and movement.
Discovery	T1018	Remote System Discovery	Enumerates network assets to identify high-value targets.
Lateral Movement	T1021.001	Remote Services	Moves laterally using standard administrative tools.
Exfiltration	T1048.002	Exfiltration Over Alternative Protocol	Steal sensitive data before encryption.
Impact	T1486	Data Encrypted for Impact	Encrypt systems to disrupt business operations.

Ransomware Group Analysis - Kill Security

Kill Security emerged once again in 2025 as a significant ransomware-as-a-service (RaaS) actor, reinforcing the trend of ransomware ecosystem diversification previously identified in earlier reports. In 2025, Kill Security demonstrated sustained operational maturity, positioning itself among the most active groups targeting organizations in Arab countries. Its campaigns reflect a shift away from opportunistic attacks toward more structured, financially motivated operations that deliberately focus on high-impact sectors. Its attacks have primarily focused on Windows and Linux environments, including cloud infrastructures and enterprise networks, marking a shift toward more coordinated, financially driven operations in the Arab region. Kill Security's rapid adoption of custom malware payloads and social engineering techniques demonstrates how new players are evolving quickly to fill the vacuum left by disrupted legacy gangs.

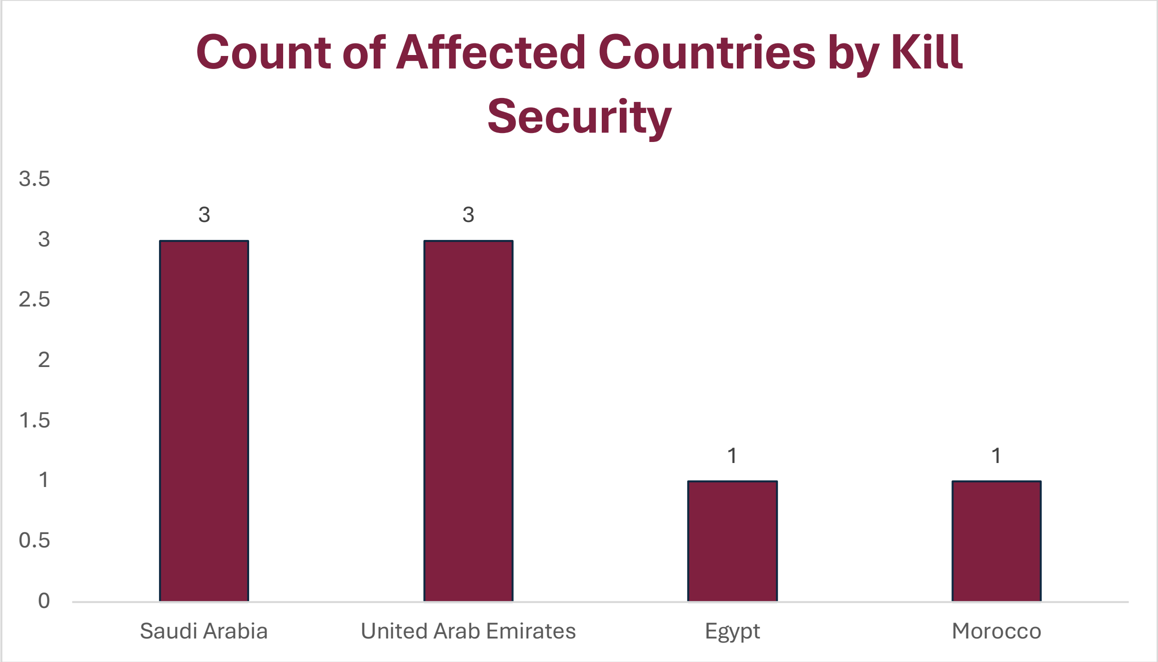


Figure 20. Count of Affected Countries by Kill Security Ransomware

This pie chart illustrates the distribution of CISA industry sectors affected by Kill Security in 2025. Commercial Facilities were the most heavily targeted sector, accounting for 50% of the recorded incidents. This was followed by the Healthcare and Public Health Sector, which represented 25% of the attacks. The Information Technology sector accounted for 13%, while the Defense Industrial Base comprised the remaining 12% of the affected industries.

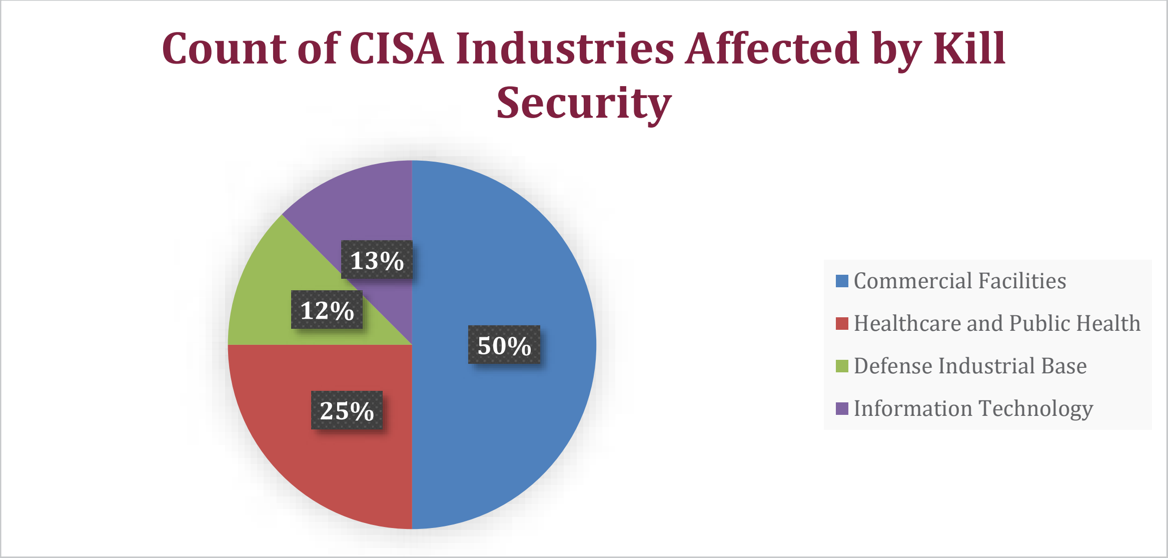


Figure 21. Count of Affected Industries by Kill Security Ransomware

From a TTPs perspective, Kill Security employs a conventional but effective ransomware attack chain focused on reliability and speed. Initial access is mainly achieved through phishing (T1566) and abuse of external remote services (T1133), followed by user execution (T1204) to launch malicious payloads. Persistence is maintained using scheduled tasks (T1053), while process injection (T1055) is used for privilege escalation and stealth. To evade detection, the group relies on obfuscated files or information (T1027) and harvests credentials via OS credential dumping (T1003). Internal reconnaissance is conducted using remote system discovery (T1018), with remote services (T1021) enabling lateral movement across networks. Attacks typically conclude with data encryption for impact (T1486), supporting Kill Security's pressure-driven extortion model. Overall, its TTPs reflect a mature use of well-known techniques rather than novel exploits.

Table 4. MITRE ATT&CK Technique Mapping for Kill Security Ransomware Operations

Kill Security			
Tactic	Technique ID	Technique Name	Description
Initial Access	T1566.001	Phishing	Primary access vectors use socially engineered emails.
Initial Access	T1133	External Remote Services	Exploits weak or exposed remote access services.
Execution	T1204.001	User Execution	Relies on user interaction to trigger malicious payloads.
Persistence	T1053.005	Scheduled Task/Job	Creates scheduled tasks to retain access.
Privilege Escalation	T1055.012	Process Injection	Injects code into trusted processes for privilege escalation.
Defense Evasion	T1027.002	Obfuscated Files or Information	Obfuscates malware to bypass security controls.
Credential Access	T1003.001	OS Credential Dumping	Dumps credentials to expand access across the environment.
Discovery	T1018	Remote System Discovery	Identifies additional hosts and assets for expansion.
Lateral Movement	T1021.001	Remote Services	Use RDP and SMB for lateral movement.
Impact	T1486	Data Encrypted for Impact	Encrypt victim systems to disrupt operations.

Tactics, Techniques, and Procedures (TTPs)

Drawing on recent industry threat intelligence analyses, this table consolidates commonly observed MITRE ATT&CK tactics, techniques, and sub-techniques reported across contemporary ransomware campaigns, with a focus on the three most active ransomware groups [5–7].

Initial Access

- ✓ T1190 Exploit Public-Facing Application
- ✓ T1133 External Remote Services
- ✓ T1566.001 Phishing (Spearphishing Attachment)
- ✓ T1566.002 Phishing (Spearphishing Link)

Execution

- ✓ T1204.001 User Execution: Malicious File
- ✓ T1059 Command and Scripting Interpreter

Persistence

- ✓ T1053.005 Scheduled Task/Job
- ✓ T1547.001 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder

Privilege escalation

- ✓ T1055.012 Process Injection: Process Hollowing
- ✓ T1548.002 Abuse Elevation Control Mechanism: Bypass User Account Control
- ✓ T1134 Access Token Manipulation

Defense evasion

- ✓ T1027.002 Obfuscated Files or Information: Software Packing
- ✓ T1218 Signed Binary Proxy Execution
- ✓ T1562.001 Impair Defenses: Disable or Modify Tools
- ✓ T1036 Masquerading
- ✓ T1070.001 Indicator Removal on Host: Clear Windows Event Logs
- ✓ T1070.004 Indicator Removal on Host: File Deletion

Credential Access

- ✓ T1003.001 OS Credential Dumping: LSASS Memory

Discovery

- ✓ T1049 System Network Connections Discovery
- ✓ T1018 Remote System Discovery
- ✓ T1087 Account Discovery

Lateral Movement

- ✓ T1021.001 Remote Services: Remote Desktop Protocol
- ✓ T1021.002 Remote Services: SMB / Windows Admin Shares

Exfiltration

- ✓ T1041 Exfiltration Over C2 Channel
- ✓ T1567.002 Exfiltration Over Web Service: Cloud Storage

Impact

- ✓ T1486 Data Encrypted for Impact
- ✓ T1490 Inhibit System Recovery
- ✓ T1489 Service Stop

Glossary of Terms

Term	Definition
Artificial Intelligence (AI)	A field of computer science focused on creating systems that can perform tasks normally requiring human intelligence, such as decision-making, problem-solving, and pattern recognition.
Credential Theft	The act of stealing login credentials to gain unauthorized access to a system.
Cyber Threat Intelligence (CTI)	Threat intelligence is data that is collected, processed, and analyzed to understand a threat actor's motives, targets, and attack behaviors. Threat intelligence enables us to make faster, more informed, data-backed security decisions and change their our behavior from reactive to proactive in the fight against threat actors
Dark Web	A portion of the internet that cannot be accessed by normal search engines and requires special software or authorization to access. Notorious for hosting websites with criminal content such as drug marketplaces and child sexual exploitation material.
Data Breach	The unauthorized movement or disclosure of sensitive information to a party, usually outside the organization, that is not authorized to have or see the information (Department of Homeland Security). See also Exfiltration
Data Exfiltration	The unauthorized transfer of information from an information system.
Decryption	Decryption is the process of transforming data that has been rendered unreadable through encryption back to its unencrypted form
Defense Evasion	The adversary is trying to avoid being detected.
Encryption	Data encryption is a way of translating data from plaintext (unencrypted) to ciphertext (encrypted). Users can access encrypted data with an encryption key and decrypted data with a decryption key.
Exploit Public-Facing Application	Adversaries may attempt to exploit a weakness in an Internet-facing host or system to initially access a network. The weakness in the system can be a software bug, a temporary glitch, or a misconfiguration.
Incident Response	The approach and processes used by an organization to handle a cyber-attack or data breach.
Initial Access	The adversary is trying to get into your network.
Lateral Movement	The adversary is trying to move through your environment.
Malware	Hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose.
Obfuscated Files	Files that have been made difficult to understand.
Open-Source Intelligence (OSINT)	Open-Source Intelligence (OSINT) is defined as intelligence produced by collecting, evaluating, and analyzing publicly available information with the purpose of answering a specific intelligence question.
Phishing	A technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a web sitewebsite, in which the perpetrator masquerades as a legitimate business or reputable person.
Privilege Escalation	An attacker to gain elevated access to resources that are normally protected from an application or user

Term	Definition
Ransomware	Ransomware is a type of malicious software, or malware, that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return.
Ransomware-as-a-Service (RaaS)	A subscription-based business model for ransomware, where operators provide malware and infrastructure to affiliates who execute attacks.
Rust programming language	systems programming language that aims to provide memory safety without sacrificing performance
Supply Chain Attack	Attacks that allow the adversary to utilize implants or other vulnerabilities inserted prior to installation to infiltrate data, or manipulate information technology hardware, software, operating systems, peripherals (information technology products), or services at any point during the life cycle.
Tactics, Techniques, and Procedures (TTPs)	The behavior of cyber adversaries, including their methods of attack, tools, and processes.
Zero-Day Vulnerability	A previously unknown vulnerability in software that attackers can exploit.

Note: This glossary of terms was written with reference to the cybercrime dictionary published by the Centre for Cybercrime and Economic Crime.

References

1. Europol. (2024). Internet organised crime threat assessment (IOCTA) 2024.

https://www.europol.europa.eu/cms/sites/default/files/documents/Internet%20Organised%20Crime%20Threat%20Assessment%20IOCTA%202024.pdf

2. European Union Agency for Cybersecurity (ENISA). (2025). ENISA threat landscape 2025.

https://www.enisa.europa.eu/sites/default/files/2025-11/ENISA%20Threat%20Landscape%202025.pdf

3. Verizon. (2025). 2025 data breach investigations report (DBIR): SMB snapshots.

https://www.verizon.com/business/resources/infographics/2025-dbir-smb-snapshot.pdf

4. Microsoft. (2025). Cyber Signals issue 9: AI-powered deception.

https://www.microsoft.com/en-us/security/blog/2025/04/16/cyber-signals-issue-9-ai-powered-deception-emerging-fraud-threats-and-countermeasures/

5. CyberProof Threat Researchers. (2025). 2025 mid-year threat landscape report: Top ransomware trends, TTPs, and defense strategies. CyberProof.

https://www.cyberproof.com/blog/mid-year-threat-landscape-report-top-ransomware-trends-ttps-and-defense-strategies-for-2025/

6. Picus Labs. (2025). Picus Red Report 2025: Top MITRE ATT&CK techniques. Picus Security.

https://www.picussecurity.com/resource/report/red-report-2025

7. Arctic Wolf. (2025, November 10). The top 10 ransomware TTPs [Blog post]. Arctic Wolf Networks.

https://arcticwolf.com/resources/blog/the-top-10-ransomware-ttps/

This report provides a comprehensive overview of the ransomware attack landscape in the Arab countries during 2025, highlighting the key ransomware actors, targeted sectors, and the growing role of artificial intelligence in ransomware operations.

It serves as an analytical reference for decision-makers and security specialists seeking intelligence-driven insights that contribute to building genuine cyber resilience at the regional level.

9 786039 383642

Naif University Press
2026