

TRACKING RANSOMWARE : JAN 2026

Published On : 2026-02-12

Share : [f](#) [t](#) [in](#)



EXECUTIVE SUMMARY

The January 2026 Ransomware Threat Report highlights a ransomware ecosystem that has matured into a highly adaptive, service-oriented criminal economy defined less by technical exploitation and more by psychological, operational, and supply-chain leverage. Ransomware activity remained elevated entering 2026, with sharp fluctuations across groups, rapid operational rebounds, and continued concentration on high-value sectors, such as professional services, manufacturing, and information technology. The threat landscape shows a clear shift toward browser-centric,

user-mediated access, brokered initial access models, and long-lived loaders that preserve optionality rather than immediately deploying encryption. Extortion strategies increasingly prioritize human and regulatory pressure over technical disruption, while silent data theft and delayed extortion models complicate detection, attribution, and response. Geographically, ransomware remains dominated by the United States and Western Europe, but with sustained expansion across Asia-Pacific and emerging markets, reflecting a truly global and opportunistic threat. Overall, ransomware in January 2026 is best understood as a persistent business risk driven by modular ecosystems, psychological coercion, and stealth-first operations rather than isolated malware incidents.

INTRODUCTION

Welcome to the Jan 2026 Ransomware Threat Report. This report delivers a detailed analysis of the ransomware landscape, highlighting the emergence of new ransomware groups, evolving attack techniques, and notable shifts in targeted industries. By examining key trends, tactics, and significant incidents, this report aims to support organizations and security teams in understanding the current threat environment. As ransomware campaigns continue to grow in complexity, this report serves as a vital resource for anticipating future threats and strengthening proactive cybersecurity strategies.

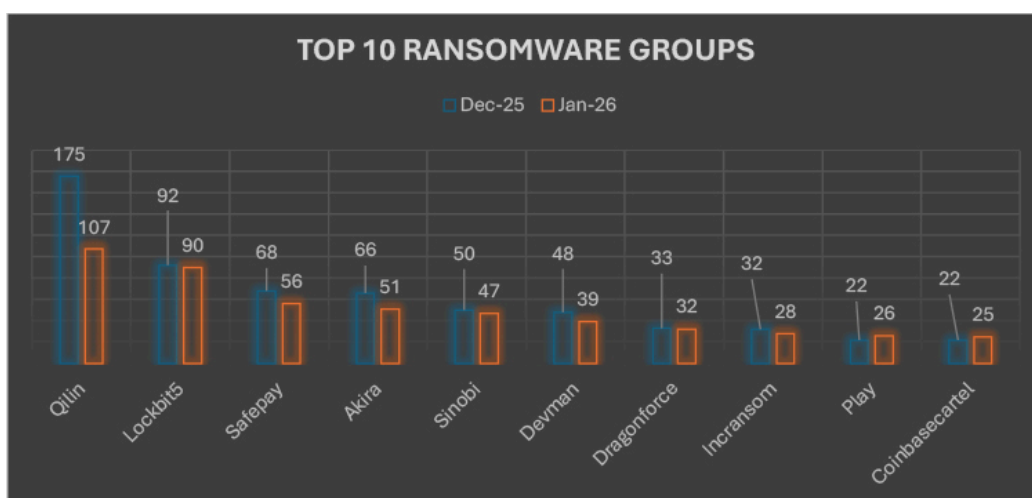
KEY POINTS

- Ransomware has shifted from exploit-driven intrusion to user-mediated access via trusted applications, especially web browsers.
- Initial access is increasingly brokered and traded, with encryption and extortion executed by separate downstream actors.
- Psychological coercion now outweighs encryption as the primary monetization lever, targeting executives and legal exposure.

- Loaders have evolved into persistent access infrastructure, prioritizing longevity and optionality over immediate payload delivery.
- Delivery artifacts are engineered to fail in security tooling but succeed on real endpoints, undermining sandbox reliability.
- Silent data theft and delayed extortion models are expanding, reducing noise and complicating attribution and response.
- Ransomware campaigns increasingly exploit subsidiaries and supply-chain trust relationships rather than core infrastructure.
- Tradecraft convergence with espionage has led to longer dwell times and stealth-first operations.
- Large-scale affiliate models introduce operational fragility, creating exploitable seams in backend infrastructure and coordination.
- Leadership exposure and rebranding cycles continue to destabilize ransomware ecosystems despite decentralization.

TREND COMPARISON: THE TOP 10 RANSOMWARE GROUPS

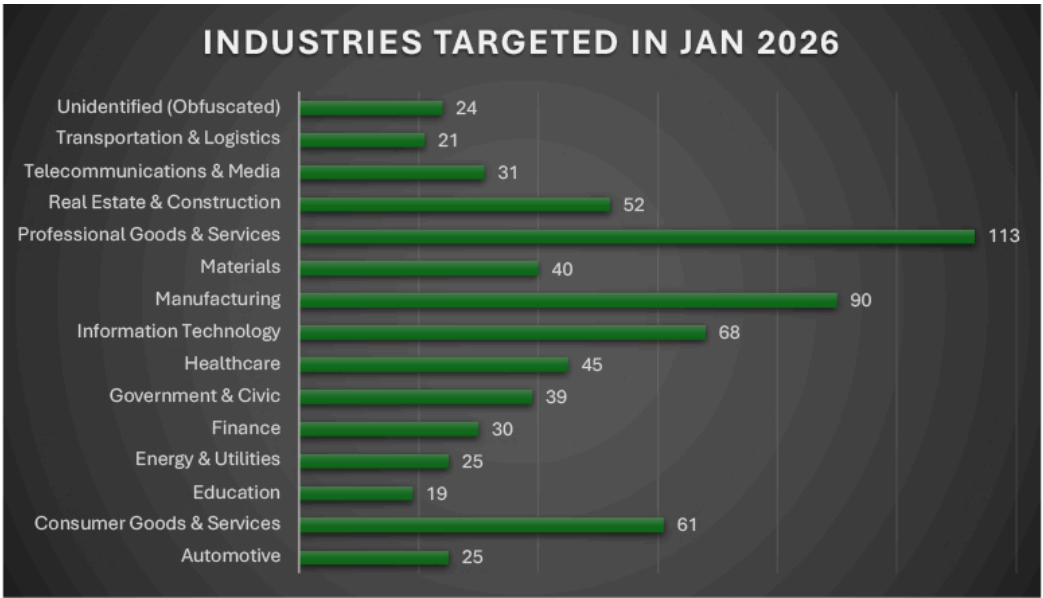
Throughout Jan 2026, there was notable activity from several ransomware groups. Here are the trends regarding the top 10:



The December 2025–January 2026 comparison reflects a broadly cooling yet still dynamic ransomware landscape, with most major actors showing moderated activity rather than expansion. Qilin

remained the most active group despite a sharp decline from 175 to 107 victims, indicating a pullback following elevated December operations, while Lockbit5 demonstrated relative stability with only a marginal decrease from 92 to 90, sustaining consistent campaign output. Safepay and Akira both recorded notable contractions, dropping from 68 to 56 and 66 to 51 respectively, and Sinobi and Devman similarly declined from 50 to 47 and 48 to 39, suggesting reduced operational tempo. Mid-tier actors largely held steady or trended slightly downward, with Dragonforce decreasing marginally from 33 to 32 and Incransom from 32 to 28, whereas Play and Coinbasecartel showed limited upward movement, rising from 22 to 26 and 22 to 25 respectively. Overall, January reflects a phase of consolidation and selective adjustment across the ecosystem, marked more by stabilization and tactical recalibration than by widespread surge activity.

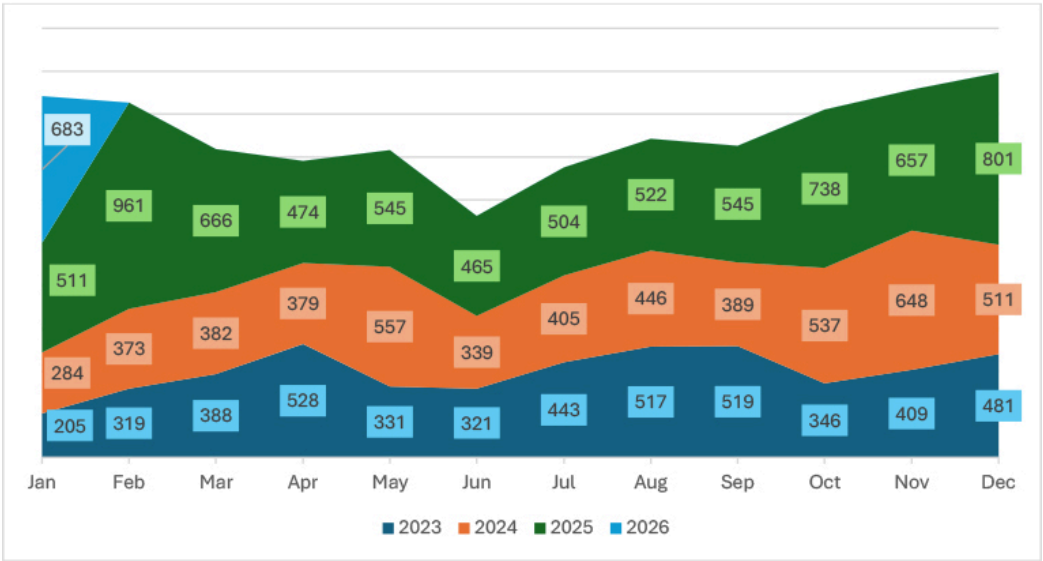
INDUSTRIES TARGETED IN JAN 2026



In January 2026, ransomware targeting continued to concentrate on high-impact and data-rich sectors, with Professional Goods & Services further solidifying its position as the most affected industry at 142 victims, reinforcing adversary preference for organizations with strong extortion leverage. Manufacturing followed with 109 incidents, reflecting sustained pressure on industrial and production

environments, while Information Technology rose to 78, underscoring the strategic value of digital service providers and downstream access opportunities. Consumer Goods & Services (73) and Real Estate & Construction (62) remained heavily targeted, indicating continued focus on sectors with operational disruption potential. Healthcare (55) and Materials (49) experienced notable activity, while Government & Civic entities recorded 44 incidents, highlighting ongoing public-sector exposure. Lower but meaningful levels of targeting were observed in Finance (34), Telecommunications & Media (36), Energy & Utilities (27), Automotive (26), Transportation & Logistics (28), and Education (23), alongside 28 obfuscated or unidentified victims. Overall, January’s distribution reflects a deliberate and sustained emphasis on professional services, manufacturing, and technology-driven sectors, consistent with ransomware operators’ prioritization of victims with high operational criticality and monetization potential.

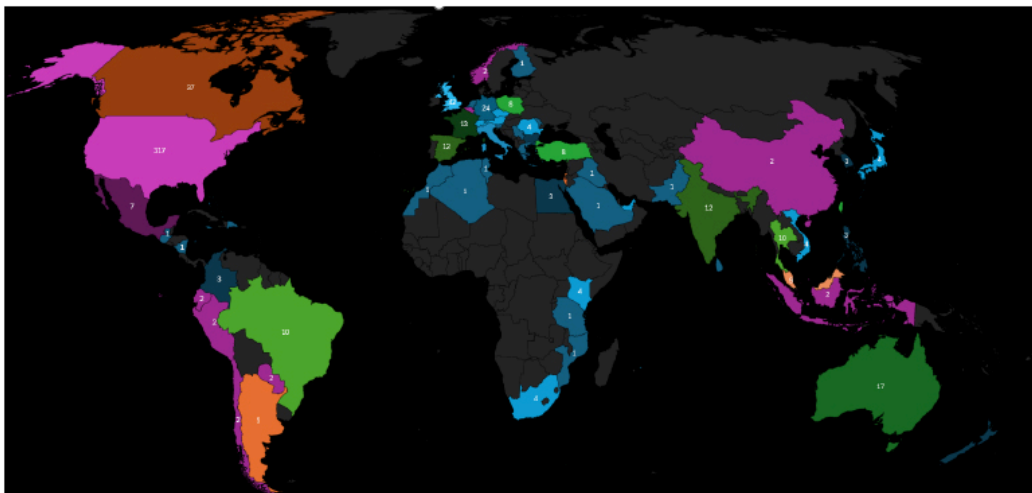
TRENDS COMPARISON OF RANSOMWARE ATTACKS



Ransomware activity demonstrated sustained year-on-year escalation, with December 2025 reaching 801 incidents the highest monthly total across the entire four-year dataset (2023–2026). This marks a substantial increase from December 2024 (511) and December 2023 (481), underscoring a structurally expanding threat

landscape rather than a short-term fluctuation. The broader 2025 trend shows consistently elevated volumes throughout the year, with multiple months exceeding 500 incidents and a pronounced surge in Q4, culminating in the December peak. Notably, January 2026 further accelerated to 683 incidents compared to 511 in January 2025 and 284 in January 2024, reinforcing the momentum carried over into the new year. Overall, the data indicates sustained operational scaling, growing affiliate ecosystems, and improved campaign throughput among ransomware actors, highlighting the ecosystem's resilience and continued expansion entering 2026.

GEOGRAPHICAL TARGETS: TOP COUNTRIES



In January 2026, ransomware activity was predominantly concentrated in the United States (317 victims), maintaining a significant lead over all other countries. The United Kingdom (42) and Canada (37) followed at a considerable distance, with Germany (24) and Italy (20) forming the next most impacted tier. Moderate activity levels were observed in Australia (17), France (13), India (12), and Spain (12), indicating continued targeting of highly digitized economies. Across Asia-Pacific and other regions, activity was more distributed and remained in single-digit to low double-digit ranges, including Malaysia (9), Taiwan (8), Turkey (8), Poland (8), Hong Kong (7), and Mexico (7). The remaining countries reported limited single-digit

incidents, reflecting geographically dispersed and opportunistic ransomware operations rather than concentrated regional surges.

Evolutions in Ransomware Threat Landscape In Jan 2026:

Browser-Centric Access Monetization Models

Ransomware operations increasingly treat the web browser as a primary access mediation layer rather than a mere delivery vector. This shift is not rooted in browser vulnerability exploitation but in the abuse of browser trust semantics extensions, security prompts, crash recovery dialogs, update workflows, CAPTCHA validation, and enterprise SSO flows. These mechanisms are implicitly trusted by users and often fall outside traditional exploit detection models. By inducing user-initiated execution within a trusted browser context, ransomware actors bypass multiple defensive layers simultaneously: exploit prevention, application allowlisting, attachment sandboxing, and network-based malware inspection.

The browser effectively becomes a psychological execution environment, where voluntary user actions replace technical exploitation, enabling ransomware operators to validate human presence, confirm enterprise relevance, fingerprint organizational identity, and ensure domain membership before committing high-risk payloads. From an economic perspective, this aligns closely with initial access brokerage models, where quality of access not speed is prioritized. The browser acts as a pre-qualification mechanism, ensuring that ransomware payloads are only deployed into environments with high monetization potential.

ETLM Assessment:

Browser-centric access models will continue to mature as endpoint and perimeter defenses harden. Future ransomware campaigns will treat browsers as programmable engagement layers, combining delayed activation, interaction gating, and environmental profiling. Rather than delivering payloads immediately, attackers will use

browsers to condition victims, escalate frustration or urgency, and trigger execution at moments of maximum trust or distraction. This evolution significantly degrades exploit-centric detection and elevates user interaction telemetry to a first-class security signal.

Delivery Artifact Engineering as Strategic Evasion

Ransomware delivery mechanisms have evolved beyond simple obfuscation into structural evasion engineering. Archives, installers, scripts, and container formats are now deliberately malformed or behaviorally ambiguous to exploit discrepancies between security tooling parsers and native OS execution logic. The objective is not stealth alone, but selective failure delivery artifacts that reliably break in sandboxes, email scanners, and automated pipelines while executing cleanly on real endpoints.

This approach reflects an understanding that modern ransomware defense relies heavily on predictable parsing, hashing, and extraction behaviors. By destabilizing these assumptions, ransomware operators ensure that delivery artifacts act as anti-analysis filters, screening out security tooling while preserving execution reliability in production environments. As a result, loaders and droppers are no longer disposable; they are engineered assets within the ransomware supply chain.

ETLM Assessment:

Future ransomware delivery will increasingly rely on client-side reconstruction, malformed standard-compliant formats, and execution paths that only fully resolve within live user environments. Artifacts will be dynamically generated per target to defeat correlation and signature-based defenses. This forces defenders to move away from artifact-centric inspection toward execution context analysis, behavioral lineage tracking, and end-to-end delivery provenance.

Loaders as Long-Lived Ransomware Infrastructure

Loaders have transitioned from short-lived payload carriers into long-lived access infrastructure within ransomware ecosystems. Modern loaders emphasize environmental awareness, defensive evasion, and persistence over immediate payload deployment. Their role is to maintain optionality holding access until conditions favor monetization. These loaders function as access validators, continuously assessing endpoint posture, security controls, business context, and user behavior before triggering ransomware, data theft, or resale. This reflects a strategic prioritization of access reliability over payload sophistication. Loaders now act as orchestration points, allowing operators to pause, redirect, or repurpose access without reinfection.

ETLM Assessment:

Ransomware loaders will evolve into multi-purpose access frameworks capable of supporting encryption, extortion-only operations, data exfiltration, or resale to third parties. Decision logic will increasingly factor in victim readiness, regulatory exposure, and operational disruption thresholds. The distinction between ransomware tooling and advanced access implants will continue to erode.

Structural Separation of Access and Extortion

Ransomware ecosystems have undergone a clear division of labor, separating access acquisition from extortion execution. Specialized actors now focus exclusively on intrusion, persistence, and validation, treating access as a tradable commodity rather than a precursor to encryption. This decoupling reduces operational risk, accelerates monetization, and limits early-stage attribution.

Access is brokered, refined, and resold within an ecosystem that resembles a distributed supply chain rather than a unified criminal group. This modularity allows ransomware operators to scale rapidly

while insulating core extortion teams from initial compromise or exposure.

ETLM Assessment:

This separation will deepen, with ransomware operations increasingly resembling service-oriented ecosystems. Access, data theft, encryption, negotiation, and laundering will function as interchangeable components. Defensive efforts focused on disrupting single stages will face diminishing returns, as pressure is re-applied through alternative suppliers within the ecosystem.

Psychological Coercion as the Dominant Ransomware Lever

Modern ransomware has shifted decisively toward human-centered coercion. Encryption is often secondary, serving as proof-of-capability rather than the primary leverage mechanism. Extortion strategies now emphasize fear, urgency, regulatory exposure, reputational damage, and executive liability. Ransomware communications are carefully structured to influence decision-makers, fragment internal response coordination, and reframe payment as a rational business decision. This reflects adaptation to improved backup hygiene, incident response maturity, and public awareness.

ETLM Assessment:

Future campaigns will increasingly integrate behavioral science and negotiation psychology into extortion workflows. Pressure tactics will be tailored to organizational structure, jurisdictional regulation, and public exposure risk. Effective ransomware defense will require governance, decision authority clarity, and executive preparedness, not just technical controls.

Operational Fragility in Scaled Ransomware Campaigns

As ransomware operations scale across affiliates, regions, and victim classes, operational complexity introduces fragility. Infrastructure reuse, tooling overlap, credential persistence, and human

coordination dependencies create systemic weaknesses. Backend operations, data storage, negotiation portals, and access management are now critical failure points. This exposes a paradox: increased scale amplifies revenue potential while simultaneously expanding the attack surface for defenders and investigators.

ETLM Assessment:

Ransomware groups will attempt to mitigate fragility through compartmentalization, automation, and ephemeral infrastructure. However, complexity will continue to generate exploitable seams, creating sustained defensive opportunities beyond endpoint containment, particularly in disrupting backend operations and coordination workflows.

Silent Extortion and Delayed Attribution Models

Ransomware increasingly manifests as covert data theft followed by delayed or conditional extortion, with no immediate encryption or public disclosure. This approach minimizes operational noise, preserves anonymity, and applies pressure through regulatory, contractual, or reputational channels. Victims are forced to operate under prolonged uncertainty, often without clear indicators of compromise or attribution clarity, complicating response and disclosure decisions.

ETLM Assessment:

Silent extortion models will expand, redefining ransomware response as long-term risk management rather than incident containment. Attribution ambiguity itself will become a coercive mechanism, increasing pressure while limiting defensive escalation options.

Subsidiary and Supply-Chain Leverage Strategies

Ransomware operators increasingly target subsidiaries, contractors, and service providers where data sensitivity exceeds operational criticality. These entities occupy trust intersections within ecosystems, making them effective leverage points even when core infrastructure

is hardened. This reflects a strategic shift from infrastructure disruption to business relationship exploitation.

ETLM Assessment:

Future campaigns will prioritize indirect targets, propagating pressure across supply chains. Third-party exposure will become a dominant ransomware risk factor, forcing organizations to reassess trust boundaries beyond their immediate networks.

Espionage-Grade Tradecraft Convergence

Ransomware operations now routinely employ tradecraft associated with espionage: long dwell times, memory-resident execution, encrypted communications, and stealthy persistence. Successful extortion increasingly depends on remaining undetected until leverage is maximized.

ETLM Assessment:

This convergence will continue, making early detection increasingly difficult. Defensive strategies must prioritize exposure visibility, behavioral anomalies, and access governance rather than malware-centric indicators.

KEY RANSOMWARE EVENTS IN JAN 2025

Leadership Exposure and Ecosystem Instability

Despite decentralized branding and affiliate structures, ransomware ecosystems remain dependent on human leadership, trust, and coordination. Exposure of key individuals undermines affiliate confidence, disrupts revenue flows, and destabilizes operations.

ETLM Assessment:

Ransomware groups will accelerate rebranding and leadership obfuscation, but coordination costs will rise. The tension between

secrecy and scale will continue to destabilize ecosystems, creating recurring opportunities for disruption.

BUSINESS IMPACT ANALYSIS

Based on available public reports, approximately 31% of enterprises are compelled to halt their operations, either temporarily or permanently, in the aftermath of a ransomware onslaught. The ripple effects extend beyond operational disruptions, as detailed by additional metrics:

- A significant 40% of affected organizations are forced into downsizing their workforce due to the financial strain caused by the attack.
- The aftermath sees 35% of businesses experiencing turnover at the executive level, with C-suite members stepping down in the wake of the security breach.
- The financial toll of cyber incidents is staggering, with the average cost burden to companies, irrespective of their size, estimated at around \$200,000. This figure underscores the substantial economic impact of cyber threats.
- Alarming, 75% of small to medium-sized enterprises (SMEs) face existential threats, admitting the likelihood of closure should cybercriminals extort them for ransom to avoid malware infection.
- The long-term viability of these entities is also in jeopardy, with 60% of small businesses shutting down within six months post-attack, highlighting the enduring impact of such security breaches.
- Even in instances where ransoms are not conceded to, organizations bear significant financial weight in their recovery and remediation endeavors to restore normality and secure their systems.

EXTERNAL THREAT LANDSCAPE MANAGEMENT (ETLM)

OVERVIEW

Impact Assessment

Ransomware remains a major threat to both organizations and individuals, locking critical data and demanding payment for its release. The consequences extend well beyond the ransom, often leading to costly recovery efforts, extended downtime, reputational harm, and potential regulatory fines. Such disruptions can destabilize operations and erode stakeholder trust. Addressing this growing risk demands a proactive cybersecurity posture and stronger collaboration between public and private sectors to build resilience against future attacks.

Victimology

Cybercriminals are increasingly targeting industries that manage vast amounts of sensitive data, ranging from personal and financial information to proprietary assets. Sectors such as manufacturing, real estate, healthcare, FMCG, e-commerce, finance, and technology remain high on the threat radar due to their complex and extensive digital infrastructures. Adversaries strategically exploit vulnerabilities in economically advanced regions, launching well-planned attacks designed to encrypt critical systems and extract significant ransom payments. These operations are calculated to yield maximum financial returns.

CONCLUSION

Ransomware entering 2026 is no longer a discrete cyber incident but an enduring, multi-stage business threat that blends elements of cybercrime, espionage tradecraft, and economic coercion. The continued separation of access, execution, and extortion, combined with browser-based trust abuse, engineered delivery artifacts, and long-lived access infrastructure, has significantly eroded the effectiveness of exploit-centric and signature-driven defenses. At the same time, the scale and complexity of affiliate-driven operations

introduce inherent fragility, creating opportunities for disruption beyond traditional endpoint containment, particularly at the levels of access brokerage, backend infrastructure, and coordination workflows. For organizations, resilience in this environment will depend less on preventing individual intrusions and more on governance readiness, third-party risk management, user interaction telemetry, and executive decision preparedness. As ransomware groups continue to evolve toward stealth, optionality, and psychological leverage, proactive external threat landscape management and cross-functional response planning will be critical to reducing both operational impact and long-term business risk.

RECOMMENDATIONS

STRATEGIC RECOMMENDATIONS:

1. **Strengthen cybersecurity measures:** Invest in robust cybersecurity solutions, including advanced threat detection and prevention tools, to proactively defend against evolving ransomware threats.
2. **Employee training and awareness:** Conduct regular cybersecurity training for employees to educate them about phishing, social engineering, and safe online practices to minimize the risk of ransomware infections.
3. **Incident response planning:** Develop and regularly update a comprehensive incident response plan to ensure a swift and effective response in case of a ransomware attack, reducing the potential impact and downtime.

MANAGEMENT RECOMMENDATIONS:

1. **Cyber Insurance:** Evaluate and consider cyber insurance policies that cover ransomware incidents to mitigate financial losses and protect the organization against potential extortion demands.
2. **Security audits:** Conduct periodic security audits and assessments to identify and address potential weaknesses in the organization's infrastructure and processes.

3. **Security governance:** Establish a strong security governance framework that ensures accountability and clear responsibilities for cybersecurity across the organization.

TACTICAL RECOMMENDATIONS:

1. **Patch management:** Regularly update software and systems with the latest security patches to mitigate vulnerabilities that threat actors may exploit.
2. **Network segmentation:** Implement network segmentation to limit the lateral movement of ransomware within the network, isolating critical assets from potential infections.
3. **Multi-Factor authentication (MFA):** Enable MFA for all privileged accounts and critical systems to add an extra layer of security against unauthorized access.



Company

Takedown Services

Products

Partners

Resources

Careers

Privacy Policy



Singapore

Hong Leong Building, 16
Raffles Quay, Floor #09-01 &
#10-01, Singapore 048581



India

2nd Floor, Workhub by Novel
Office, Doddanakundi
Industrial Area, Graphite India
Main Rd, Whitefield, KEB
Colony, Industrial Area,
Mahadevapura, Bengaluru,
Karnataka 560048



Japan

Otemachi One Tower, 6th
Floor, 1-2-1 Otemachi,
Chiyoda-ku, Tokyo, 100-0004
Tokyo, Japan



USA

501 Fifth Avenue Suite 805,
New York, NY 10017

Germany

South Korea

in

f

X



Opernplatz 14, 60313 Frankfurt
am Main



10F, 373 Gangnam-daero,
Seocho-gu, Seoul, Korea
06621



Australia

Unit 20 270 Blackburn Road,
Glen Waverley, VIC, 3150



Taiwan

9F, Second Building, No.96,
Sec. 2, Zhongshan N. Rd.,
Taipei, Taiwan



Vietnam

14th Floor, HM Town building,
412 Nguyen Thi Minh Khai,
Ward 5, District 3, Ho Chi Minh
City



Dubai

Unit JLT-PH2-RET-5, Cluster R,
Jumeirah Lakes Towers,
Dubai, UAE

Copyright CYFIRMA. All rights reserved.

