IT ISAC

CELEBRATING 25 YEARS OF THREAT INTELLIGENCE SHARING

EXPLORING THE DEPTHS

ANALYSIS OF THE 2025 RANSOMWARE LANDSCAPE AND INSIGHTS FOR 2026

FEBRUARY 2026

IT ISAC

CELEBRATING 25 YEARS OF THREAT INTELLIGENCE SHARING

ABOUT IT-ISAC

Founded in 2000, the Information Technology - Information Sharing and Analysis Center (IT-ISAC) is a non-profit organization that provides a trusted forum for IT companies and those that leverage IT for core business functions to share information, manage risks, and collaborate on cyber incident response and strategy.

Our mission is to grow a diverse community of companies that leverage information technology and have in common a commitment to cybersecurity, to serve as a force-multiplier that enables collaboration and sharing of relevant, actionable cyber threat information, effective security policies and practices for the benefit of all.

Our membership is comprised of security leaders from leading technology companies across the globe. We have built a network of relationships with trusted partners across the critical-infrastructure community and through this multidirectional sharing, we help companies manage risks to their enterprises and to the critical infrastructure community.

TABLE OF CONTENTS

Introduction 1

Attacks on Critical Infrastructure 2

Attacks by Country | IT Sector 2

2024 VS 2025 Ransomware Groups Activity | IT Sector 3

Top 5 Ransomware Strains 4

Vulnerabilities 5

2026 Predictions 6

INTRODUCTION

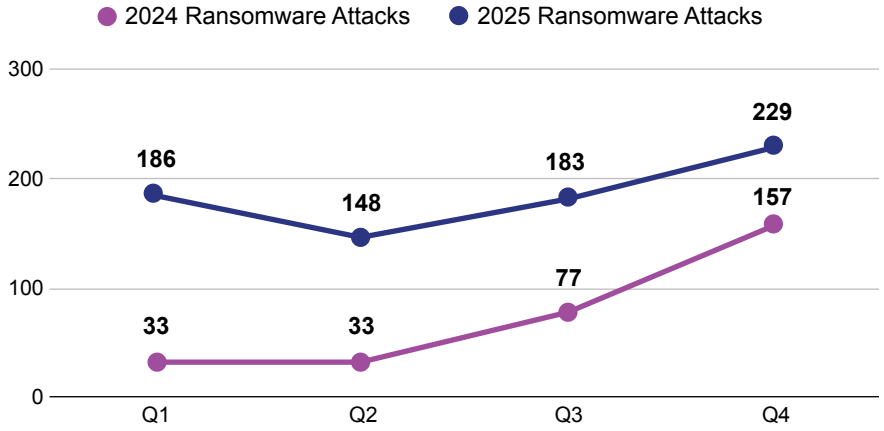
The Information Technology - Information Sharing and Analysis Center (IT-ISAC) tracks ransomware attacks to better understand patterns and threat actor behavior. To date, we have recorded over 15,265 ransomware incidents through proprietary automation tools that aggregate data from public breach reports, RSS feeds, dark web leak sites, and internal threat intelligence.

The IT-ISAC team researches the ransomware groups involved, their operational methods, and the context surrounding each incident. This process includes cross-referencing data with open-source intelligence (OSINT), industry reports, and internal member contributions to address gaps in the affected sector, geographic location, attack timeline, and possible entry points used by attackers.

The IT-ISAC ransomware tracker database is a queryable resource accessible to IT-ISAC members and acts as a central hub for monitoring ransomware incidents. This joint effort allows members to analyze trends collaboratively and improves the capacity of all participants to remain informed, while bolstering the overall resilience of the IT-ISAC community against ransomware attacks. When the IT-ISAC team and its member companies identify significant and emerging ransomware groups and incidents, comprehensive Adversary Attack Playbooks are built for them. These playbooks provide in-depth analysis of the groups' tactics, techniques, and procedures (TTPs), equipping members with valuable intelligence to enhance their cybersecurity defenses.

The IT-ISAC tracked approximately 6,351 total attacks in 2025, including 746 ransomware incidents within the information technology (IT) sector, a significant increase from the 300 incidents recorded in 2024. The 148% surge in ransomware attacks during 2025 was driven by a strategic pivot toward the IT sector, where ransomware operators deployed "one-to-many" exploitation techniques to reach broader supply chains. While defensive capabilities may have improved, attackers countered with record-breaking speed, weaponizing critical zero-day vulnerabilities in platforms within hours of disclosure. Last year also saw a rise in "living-off-the-land" (LOTL) tactics, where groups abused legitimate administrative tools and forensic platforms to blend into network traffic and evade detection. Furthermore, sophisticated social engineering and "vishing" campaigns targeted staff to bypass multi-factor authentication (MFA) by stealing OAuth tokens. While the use of generative AI may have been attributed to its increased efficiency and convincing nature, the overall spike reflects a more aggressive and professionalized criminal ecosystem.

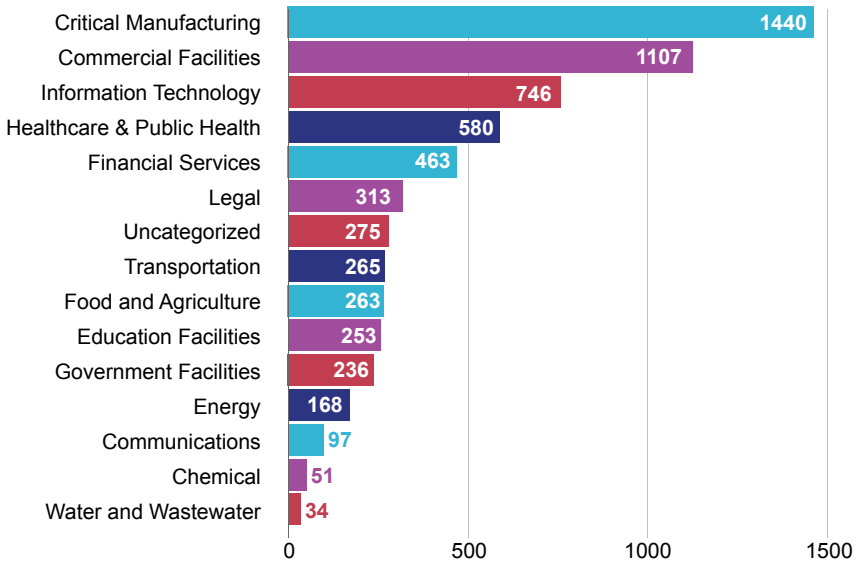
RANSOMWARE ATTACKS ON THE IT SECTOR 2024 VS. 2025



ATTACKS ON CRITICAL INFRASTRUCTURE

- The **critical manufacturing sector** saw the highest number of attacks we tracked, experiencing 1440 attacks (22.7%).
- Following closely, the **commercial facilities sector** saw 1107 attacks (17.5%).
- The **information technology sector** accounted for 746 attacks (11.8%).
- The **healthcare and public health sector** saw 580 attacks (9.2%).
- Additionally, the **financial services sector** experienced 463 attacks (7.3%).
- Finally, although not a critical infrastructure sector, it is worth noting that the **legal sector** accounted for 313 attacks (4.9%).

NUMBER OF ATTACKS ON CRITICAL INFRASTRUCTURE

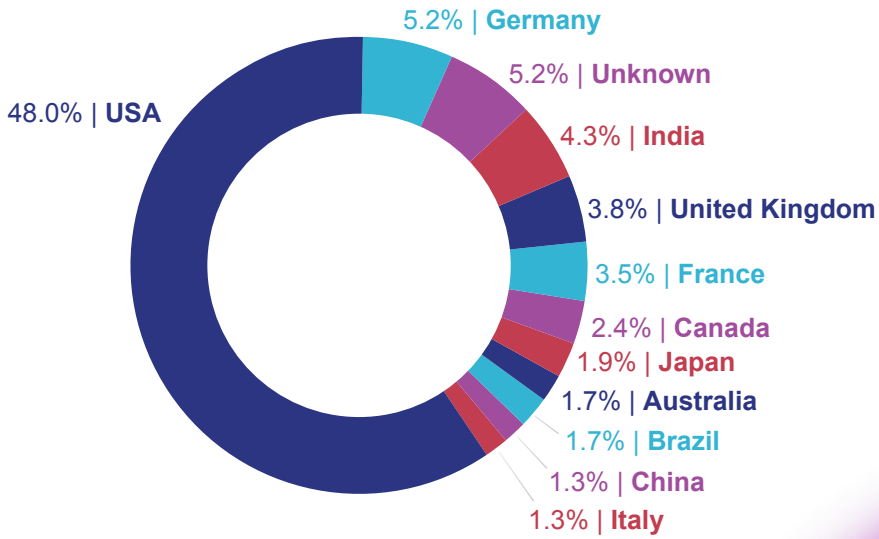


ATTACKS BY COUNTRY IT SECTOR

Geographically, the 2025 data suggests that ransomware attacks are highly concentrated against companies located in the United States. The U.S. accounts for the majority of incidents within the IT sector, with 357 attacks (48.0%), reflecting its position as a significant economic and technological hub. In all other countries, fewer than 300 attacks were recorded against IT companies (under 6%).

The U.S. is also the world's largest economy, housing many high-value corporations and critical infrastructure components. Thus, it is a prime target for ransomware operators who seek to enrich themselves and create chaos.

NUMBER OF ATTACKS BY COUNTRY IT SECTOR | 2025

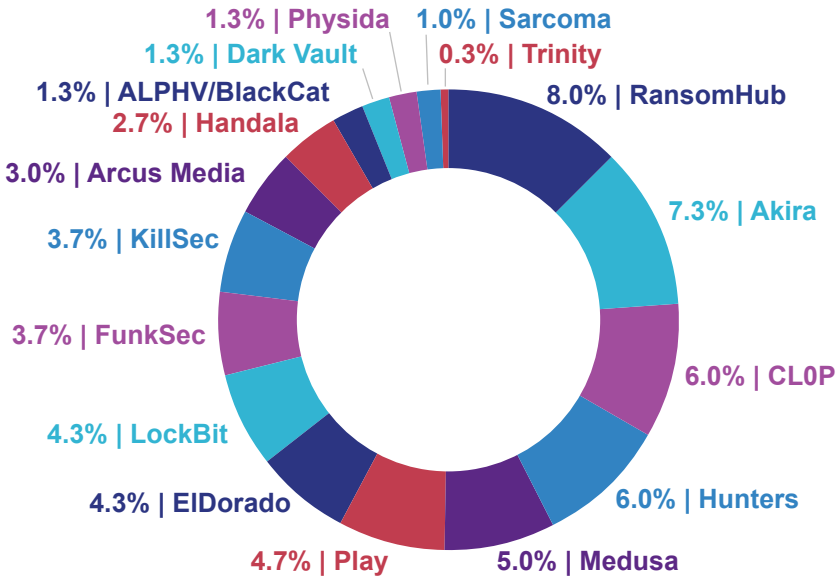


This graph represents the top 12 countries attacked by ransomware groups in 2025.

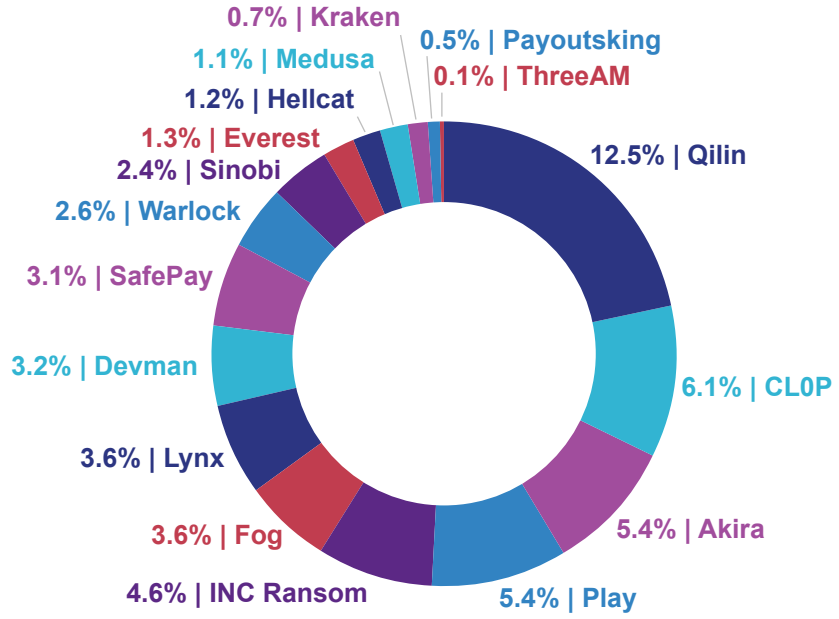
RANSOMWARE GROUP ACTIVITY IT SECTOR

The ransomware landscape shifted dramatically between 2024 and 2025, most notably with the disappearance of the 2024 leader, RansomHub, and the meteoric rise of Qilin to a dominant 12.5% market share. While the 2024 market was more evenly distributed, 2025 shows a dangerous consolidation of power, as Qilin's share is now more than double that of the next largest group. Despite this volatility at the very top, established actors like CL0P, Akira, and Play remained remarkably consistent threats across both years. The data also highlights rapid turnover in the lower tiers, where previous heavy hitters like Hunters and Medusa have been replaced by emerging groups such as INC Ransom and Fog.

RANSOMWARE GROUP ACTIVITY IT SECTOR | 2024



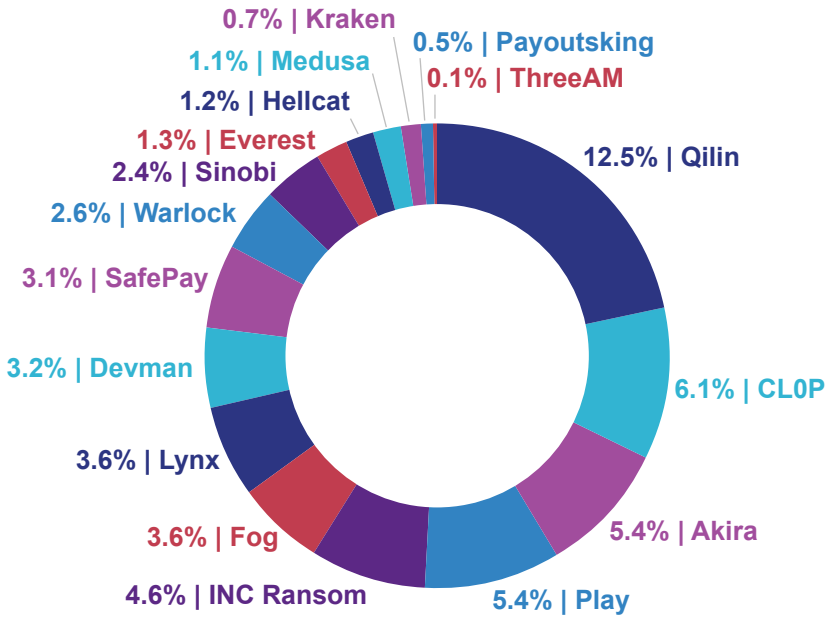
RANSOMWARE GROUP ACTIVITY IT SECTOR | 2025



TOP 5 RANSOMWARE STRAINS | IT SECTOR

The top five ransomware strains in 2025 were Qilin, CL0P, Akira, Play, and INC Ransom. Together, these five groups accounted for approximately 34% of ransomware attacks targeting the IT sector recorded by the IT-ISAC, highlighting their significant impact on the ransomware landscape.

RANSOMWARE GROUP ACTIVITY IT SECTOR | 2025



QILIN

Attacks Targeting the IT Sector: 93
Attacks Overall: 912

Operational Profile: Qilin (also known as Agenda) was the most active threat group in our dataset. Operating as a ransomware-as-a-service (RaaS), the group has recently pivoted to a Rust-based encryptor, allowing them to target Windows, Linux, and ESXi environments with high efficiency.

CL0P

ATTACKS TARGETING THE IT SECTOR: 45
ATTACKS OVERALL: 280

Operational Profile: CL0P remains a top-tier threat due to its strategy of “hunting big”. Unlike groups that rely on phishing, CL0P focuses on mass-exploitation of Zero-Day vulnerabilities in enterprise software, specifically Managed File Transfer (MFT) platforms.

AKIRA

ATTACKS TARGETING THE IT SECTOR: 40
ATTACKS OVERALL: 594

Operational Profile: Akira has aggressively targeted small-to-medium businesses (SMBs) and the managed service providers (MSPs) that support them. Their rapid ascent is attributed to their willingness to target the “infrastructure” of IT service delivery.

PLAY

ATTACKS TARGETING THE IT SECTOR: 40
ATTACKS OVERALL: 315

Operational Profile: Unlike the other groups on this list, Play is not a public ransomware-as-a-service (RaaS). They operate as a secretive, “closed” cell of developers and operators. This tight operational control allows them to maintain high security and evade law enforcement infiltration more effectively than larger groups.

INC RANSOM

ATTACKS TARGETING THE IT SECTOR: 34
ATTACKS OVERALL: 348

Operational Profile: While previously considered a newer entrant in 2023, INC Ransom is now a fully established, high-tier threat actor. In 2025, they drastically intensified their operations, with activity peaking in July. They have gained a reputation for ruthlessness, targeting “life-safety” sectors and IT service providers alike.

VULNERABILITIES

Ransomware activity observed in 2025 demonstrated a broad range of vulnerabilities that threat actors exploited to infiltrate organizations, exfiltrate sensitive data, and engage in extortion. Below are some of the most prominent vulnerabilities leveraged by ransomware groups during the year:

EXPLOITATION OF VULNERABILITIES

CVE-2025-10035 – GoAnywhere Managed File Transfer (MFT)

CVE-2025-61882 – Oracle E-Business Suite

CVE-2025-55182 – React Server Components (React2Shell)

2026 PREDICTIONS

In 2025, ransomware actors refined their strategies, targeting high-value data and leveraging new vulnerabilities. In 2026, these evolving tactics are expected to further influence how ransomware campaigns are conducted across industries:

1. **Supply Chain and SaaS Ecosystem Targeting**
   The breach involving Mobility Software Solutions highlights how attackers can take advantage of trusted vendor relationships and shared infrastructure to extend their reach well beyond the initial victim. Heading into 2026, we expect ransomware groups to expand their focus to third-party vendors and SaaS providers, where a single compromise can expose many downstream organizations.

2. **Encryptionless Extortion**
   Encryptionless extortion is expected to continue into 2026, as actors favor lower-risk, high-impact operations focused on data theft and public-leak pressure. In 2025, ransomware actors prioritized data theft over endpoint encryption. Groups such as CL0P demonstrated the effectiveness of this model, exploiting enterprise software vulnerabilities to exfiltrate sensitive data at scale and extort dozens of victims worldwide. The emergence of Scattered LAPSUS$ Hunters, particularly its Salesforce-focused campaigns last year, further reinforced this shift.

3. **Cloud Infrastructure Attacks**
   We expect ransomware actors to shift towards targeting cloud infrastructure, where misconfigurations and cloud-native features are abused rather than deploying traditional malware. Actors will increasingly leverage excessive IAM permissions, exposed management interfaces, and weak identity controls to operate directly through cloud control planes. By using legitimate APIs, backup deletion features, and native encryption or key-management functions, attackers can encrypt or destroy data while blending in with normal administrative activity and bypassing many endpoint detection tools.

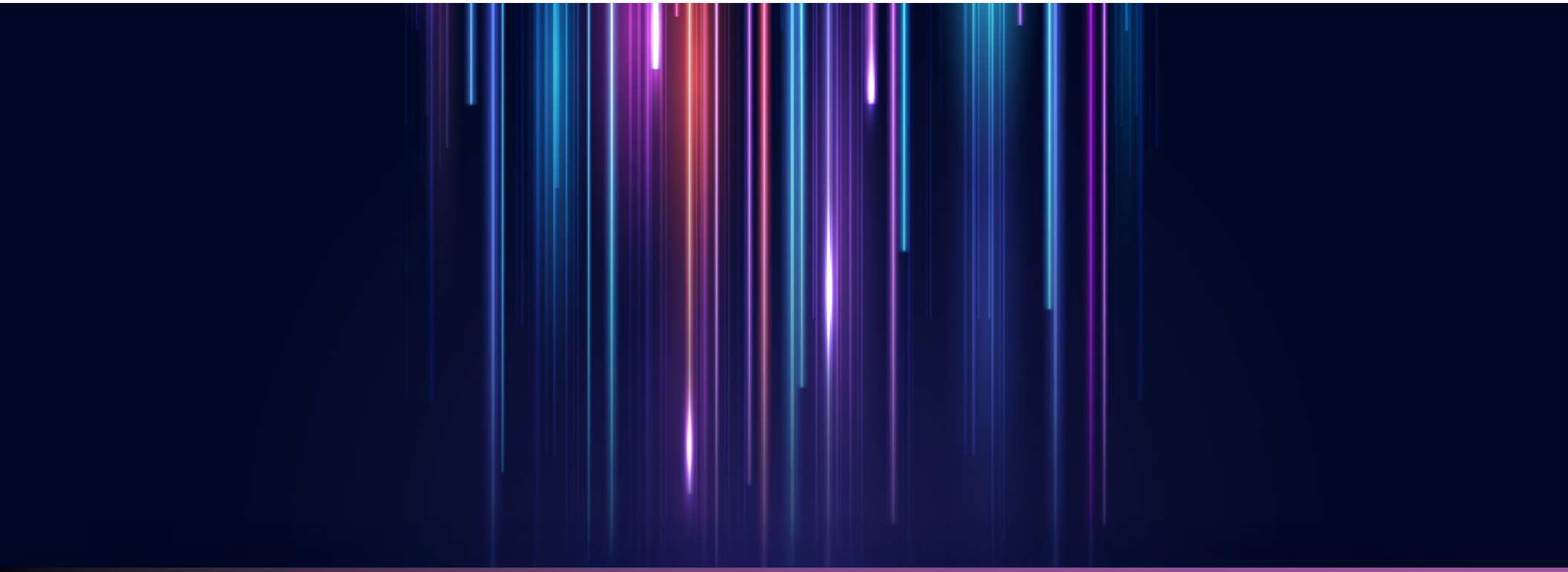
4. **Zero-Day Exploitation**
   Zero-day exploitation will remain a key enabler of ransomware operations in 2026, as demonstrated by the widespread abuse of vulnerabilities such as CVE-2025-61882 (Oracle E-Business Suite) in 2025. High-impact flaws in enterprise software provide attackers with immediate, unauthenticated access to sensitive systems and allow them to bypass traditional perimeter defenses. Once exploit details or proof-of-concept code become public, ransomware actors are often quick to weaponize them, rapidly scanning for exposed endpoints and automating exploitation at scale. This trend is expected to continue as actors seek fast and reliable initial access vectors that offer broad victim reach and minimal user interaction.

5. **Legitimate Tool Abuse**
   We expect ransomware actors to continue to abuse legitimate administrative and security tools to conduct intrusions while minimizing their malware footprint. By abusing trusted platforms such as remote management, monitoring, and incident response tools, actors can blend malicious activity into normal enterprise operations and evade traditional endpoint-based detections. These living-off-the-land techniques enable attackers to maintain persistence, perform reconnaissance, and facilitate data exfiltration without deploying custom binaries.

2026 PREDICTIONS

The ransomware threat landscape in 2026 will be characterized by increased sophistication, strategic patience, and a fundamental shift in attacker methodology. As adversaries move away from encryption-based attacks toward stealthier data theft operations, cloud infrastructure exploitation, and the abuse of trusted vendor relationships, traditional defense strategies centered on endpoint protection and perimeter security won't be sufficient.

The groups driving these trends have demonstrated both technical capability and operational discipline. Their success in 2025 will only encourage further refinement of these tactics in the year ahead. Organizations that invest now in detection capabilities, incident response readiness, and a robust defense-in-depth strategy aligned with emerging threats will be significantly better positioned to prevent, detect, and respond to ransomware campaigns in 2026.



The attackers share with each other.
The defenders share with us.

IT-ISAC.org
Membership@IT-ISAC.org