BRANDEFENSE

RANSOMWARE TRENDS REPORT Q4 | 2025

with comparison 2025

Executive Summary

The Q4/2025 Ransomware Trends Report (RTR) presents a comprehensive analysis of the evolving global ransomware landscape, based on 1,422 confirmed incidents and activity from 125 ransomware groups across 134 countries and 27 industry verticals. Powered by Brandefense Cyber Threat Intelligence Team, the report offers in-depth visibility into operational patterns, group behaviors, targeted sectors, exploited vulnerabilities, and significant attack news from the quarter.

KEY INSIGHTS INCLUDE

- **Operational Fragmentation:** Nearly half (46.3%) of ransomware activity now stems from small to mid-sized groups operating under flexible RaaS models, signaling the decline of monolithic threat actors and the rise of a more fragmented, resilient cybercrime ecosystem.

- **Top Threat Actors:** Groups like Qilin, Akira, and INC Ransom displayed sustained growth and infrastructure maturity, while Clop focused on high-impact, vulnerability-driven campaigns, demonstrating the coexistence of both scale-based and precision exploitation models.

- **Strategic Sector Targeting:** Manufacturing, technology, and healthcare remained the most targeted sectors due to their high operational sensitivity and financial leverage. Attackers increasingly map business impact to select high-pressure environments for maximum extortion value.

- **Geographic Concentration:** North America continued to dominate as the primary target region, with the U.S. accounting for nearly half of all global incidents. Meanwhile, activity across EMEA, APAC, and LATAM reflected ransomware's expanding operational theater.

- **Tactical Exploitation:** Q4 / 2025 was marked by aggressive exploitation of high impact vulnerabilities affecting managed file transfer solutions, enterprise application platforms, and internet facing infrastructure. CVEs such as CVE-2025-10035 in Fortra GoAnywhere MFT, CVE-2025-55182 in React Server Components, CVE-2025-61882 and CVE-2025-61884 in Oracle E Business Suite, along with continued abuse of CVE-2024-21762 in Fortinet FortiOS SSL VPN, were actively weaponized by multiple ransomware groups to achieve unauthenticated access, escalate privileges, and rapidly expand control within compromised environments.

- **Notable Incidents:** High-profile attacks on Askul (Japan), Pierce County Library (U.S.), and Romania's National Water Agency underscored ransomware's growing reach into public infrastructure, e-commerce, and national utilities.

This report is designed to inform security leaders, threat analysts, and risk professionals by providing tactical and strategic foresight into ransomware evolution. It offers a foundation for targeted defense planning and underscores the importance of intelligence-driven vulnerability management and cross-sector readiness.

Sincerely,
Brandefense CTI

2373
VICTIMS

134
COUNTRY

27
INDUSTRIES

51
RANSOMWARE GROUP

Methodology

To develop this report, Brandefense CTI analysts systematically monitored ransomware activity across deep and dark web ecosystems throughout the fourth quarter of 2025. The team gathered detailed intelligence on targeted organizations, impacted geographies, stolen data types, ransom demands, and attacker tactics. This data was thoroughly validated and consolidated into a comprehensive retrospective analysis that captures the evolving dynamics of global ransomware operations.

The analysis primarily focused on activity observed between **October and December 2025**, with special attention given to attacker trends, group behavior, victimology patterns, and sectoral targeting. Key variables included the industries affected, ransom size, initial access vectors, and the financial profile of victim organizations. Where relevant, **comparative insights from Q3/2025** were integrated to highlight evolving strategies and shifting threat landscapes.

In addition to quantitative metrics, the report includes a curated selection of notable ransomware incidents from the quarter. These narratives offer critical context and illustrate the real-world consequences of ransomware operations across public services, critical infrastructure, and commercial sectors. By combining tactical data with incident-level storytelling, the report aims to support security leaders with actionable intelligence and strategic foresight.

Key Insights

- Ransomware Activity Reached Record Levels: Q4/2025 witnessed the highest volume of ransomware attacks of the year, with 2,373 confirmed incidents across 134 countries and 27 sectors.

- Qilin Emerged as the Top Threat Actor: With 481 known attacks in Q4 alone, Qilin solidified its status as the most active and scalable ransomware group of the year.

- Mid-Sized and Emerging Groups Gained Ground: “Others” category accounted for 46.3% of all attacks, indicating increasing decentralization and commoditization of ransomware operations.

- Manufacturing Sector Remained the Prime Target: 24.1% of attacks targeted manufacturing, underscoring attackers’ focus on operationally critical industries vulnerable to downtime.

- North America Was Disproportionately Affected: Over half of all ransomware activity (53.5%) occurred in North America, driven by digital maturity and high ransom-paying capacity.

- Exploitation of Perimeter Vulnerabilities Continued: Groups like Qilin, Akira, and Clop heavily leveraged VPN, firewall, and ERP platform vulnerabilities to gain initial access.

- Shift Toward Sustained Criminal Operations: Data shows that ransomware groups now operate as long-term, structured businesses with predictable growth cycles and reinvestment in infrastructure.

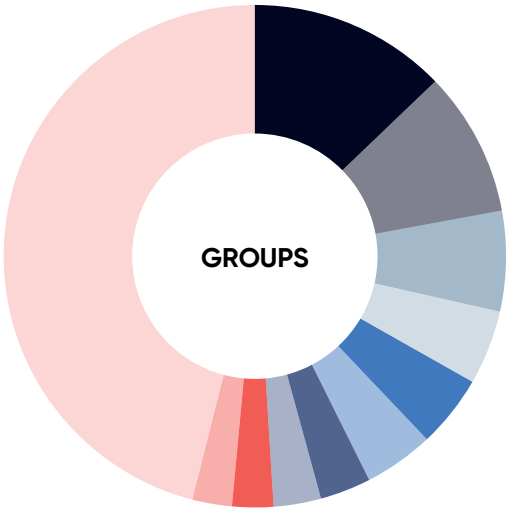
Table of Contents

Statistics on Ransomware Attacks

A visual breakdown of the targeted countries, sectors, and regions, along with the attack counts of top ransomware groups.

01

Ransomware Attack Distributions by Group: 2025



12.9	Qilin	3.3	Lynx
9.3	Akira	2.9	Ransomhub
6.4	Cl0p	2.7	Dragonforce
4.8	Play	2.3	Sinobi
4.7	Incransom	46.3	Others
4.4	Safepay		

The dominance of the “Others” category, accounting for 46.3% of all ransomware activity in 2025, clearly demonstrates that ransomware power is no longer concentrated within a small number of elite groups. Instead, the ecosystem is increasingly shaped by a large population of small, mid-sized, and rapidly rotating crews operating with comparable tooling, playbooks, and access to commoditized Ransomware-as-a-Service infrastructure. This diffusion of capability reflects a structural shift in the ransomware economy, where operational power is fragmenting and barriers to entry continue to fall.

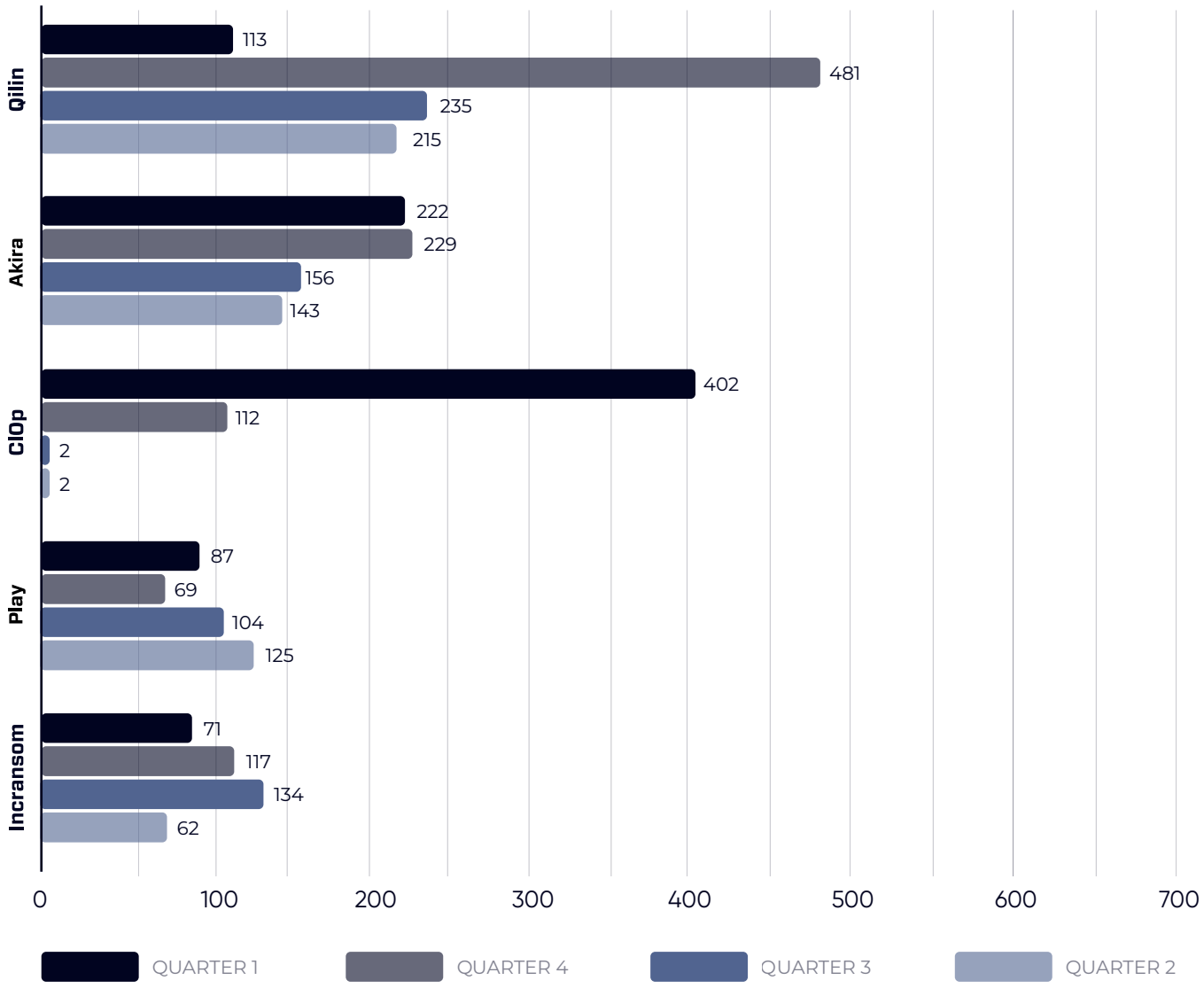
At the same time, the sustained presence of top-tier groups such as Qilin, Akira, and Clop shows that while ransomware influence is dispersing, it is not weakening. Rather, the threat is becoming more distributed, more resilient, and more difficult to suppress through law enforcement disruption alone. As ransomware capabilities spread across a broader range of actors, defenders are no longer facing a handful of dominant adversaries, but an industrialized criminal ecosystem capable of regenerating itself at scale.

Top of the list

Qilin, Akira and ClOp

02

Ransomware Attacks Comparison Across Group: Q1/2025 - Q4/2025



The quarterly comparison highlights how ransomware operations have shifted from intermittent, opportunistic campaigns into sustained, high-tempo criminal enterprises. Qilin's trajectory is particularly striking. After a relatively contained first quarter, its activity accelerates sharply through the year, peaking in Q4 with 481 recorded attacks. This growth reflects a highly efficient affiliate model and a mature operational structure capable of scaling rapidly. By the end of 2025, Qilin had clearly positioned itself as one of the most active and commercially successful ransomware platforms in the ecosystem.

At the same time, the data shows that not all groups operate on the same rhythm. Clop's activity is heavily concentrated in Q1, driven by large-scale exploitation campaigns linked to major software vulnerabilities, followed by a steep decline in later quarters. Akira, Play, and Incransom follow a more consistent and steady growth pattern, indicating long-term investment in infrastructure and repeatable attack workflows. Together, these trends illustrate a ransomware landscape that is no longer defined by isolated waves of attacks, but by continuously operating criminal businesses with predictable growth cycles and increasing operational maturity.

03

Ransomware Attack Distributions by Sector: 2025

24.1	Manufacturing
16.7	Technologies
10	Health
9.3	Hospitality
8	Consulting
7.1	Finance
5.5	Education
5.4	Logistics
5	Goverment & Administrations
3.8	Agriculture & Agribusiness
5.1	Others

The sectoral distribution of ransomware attacks in 2025 reveals a clear prioritization of operationally critical and economically sensitive industries. Manufacturing emerges as the most targeted sector, accounting for 24.1% of all observed incidents. This reflects attackers' continued focus on environments where operational downtime directly translates into financial loss, production delays, and supply chain disruption. Technology (16.7%) and healthcare (10%) follow closely, highlighting how digital dependency and sensitive data remain powerful leverage points in modern extortion campaigns.

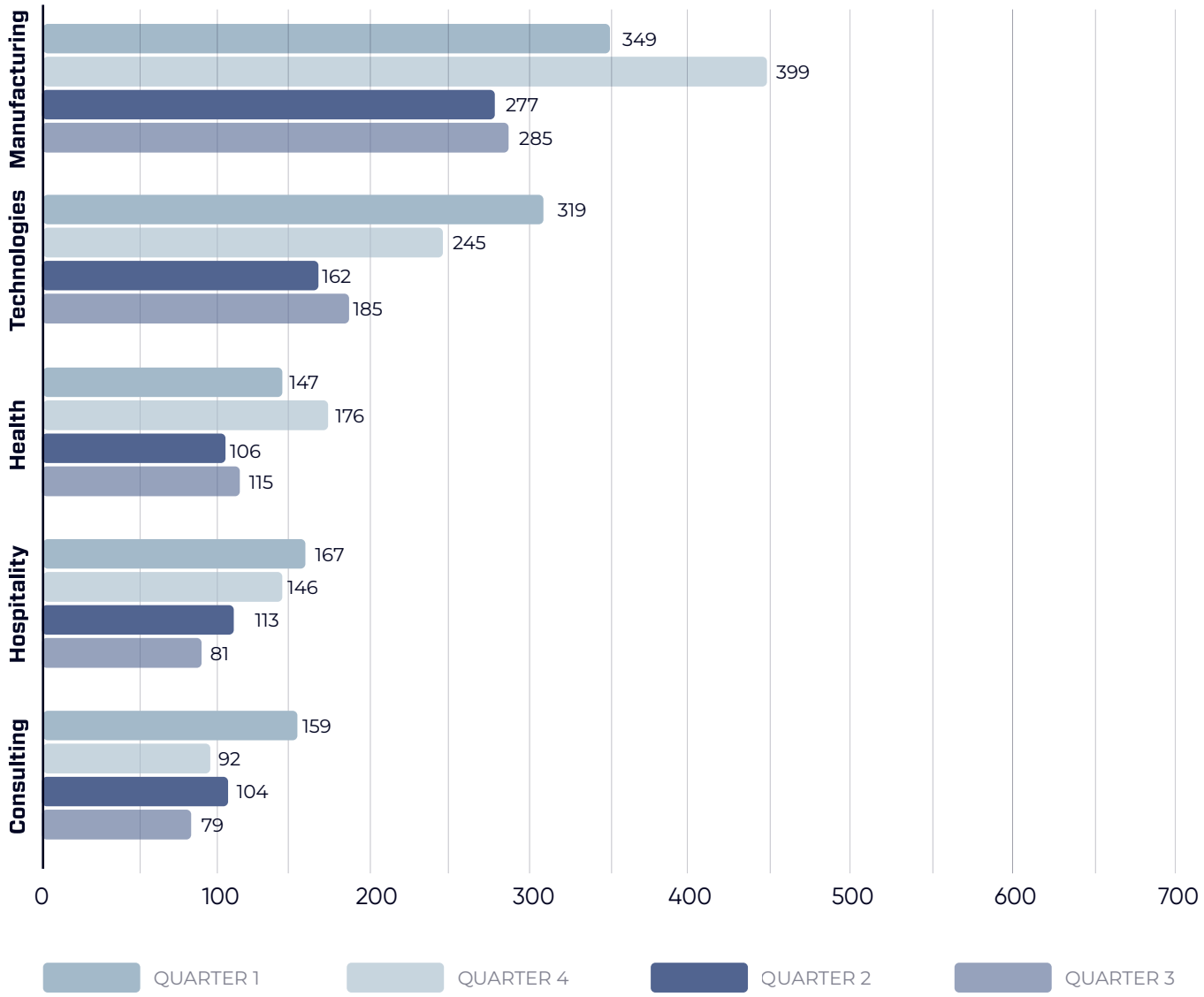
Beyond the top-tier targets, the data shows a broad and deliberate expansion across service-driven and public-facing sectors. Hospitality, consulting, finance, education, logistics, and government institutions together represent a substantial portion of total activity, reinforcing that ransomware groups are pursuing diversification rather than concentration. This wide distribution illustrates a mature threat economy that systematically maps business dependency, regulatory pressure, and reputational risk to identify high-impact targets. In 2025, ransomware is no longer confined to a handful of vulnerable sectors — it has become a universal business risk embedded across the global economy.

Top of the list

Manufacturing, Technologies and Health

04

Ransomware Attacks Comparison Across Sector: Q1/2025 - Q4/2025

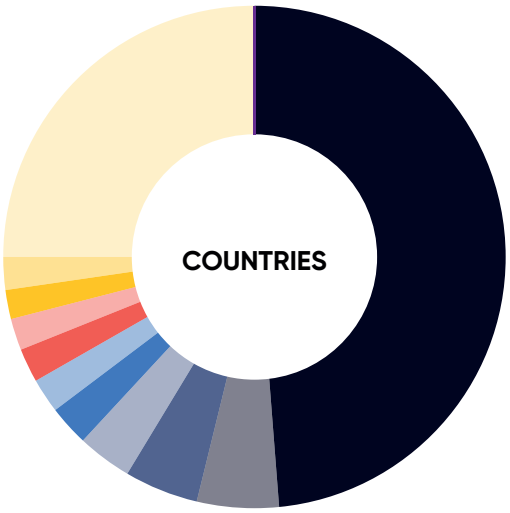


The quarterly sector comparison reinforces that ransomware activity in 2025 followed a clear pattern of strategic targeting rather than random victimization. Manufacturing stands out as the most persistently targeted sector throughout the year, peaking in Q4 with 399 recorded attacks after already elevated activity in Q1 and Q3. This reflects the sector's high operational sensitivity, where even short periods of downtime translate into immediate financial loss, production delays, and contractual penalties. For ransomware groups, manufacturing environments continue to represent one of the highest-return targets in the global economy.

Technology and healthcare follow a similar trajectory, with both sectors experiencing sustained pressure and a noticeable escalation toward the end of the year. Technology firms remain attractive due to their central role in digital ecosystems and their access to downstream customer and partner networks, while healthcare organizations continue to be targeted for their critical service dependency and highly sensitive data. Hospitality and consulting show more moderate but consistent exposure, reflecting attackers' growing focus on service-driven businesses where reputational damage and operational disruption can quickly translate into ransom leverage. Taken together, the data illustrates that ransomware operators are no longer opportunistic. They are executing sector-aware campaigns built around business impact, recovery timelines, and financial pressure points. The steady growth across nearly all industries from Q1 to Q4 confirms that ransomware has evolved into a long-term, industrialized threat model — one that systematically maps the global economy and prioritizes sectors where disruption delivers the greatest commercial return.

05

Ransomware Attack Distributions by Country: 2025



48.4	USA	3.6	Spain
5.1	Canada	3.5	Brazil
4.7	Germany	1.9	India
3.6	UK	1.8	Australia
4.5	France	25.3	Others
3.9	Italy		

The country-level distribution of ransomware attacks in 2025 reveals a clear geographic concentration of activity, with the United States accounting for nearly half of all observed incidents (48.4%). This reflects the country's large digital footprint, high concentration of enterprise infrastructure, and the financial capacity of organizations to meet high-value ransom demands. For ransomware operators, the U.S. continues to represent the most lucrative and operationally efficient hunting ground, offering both scale and monetization potential.

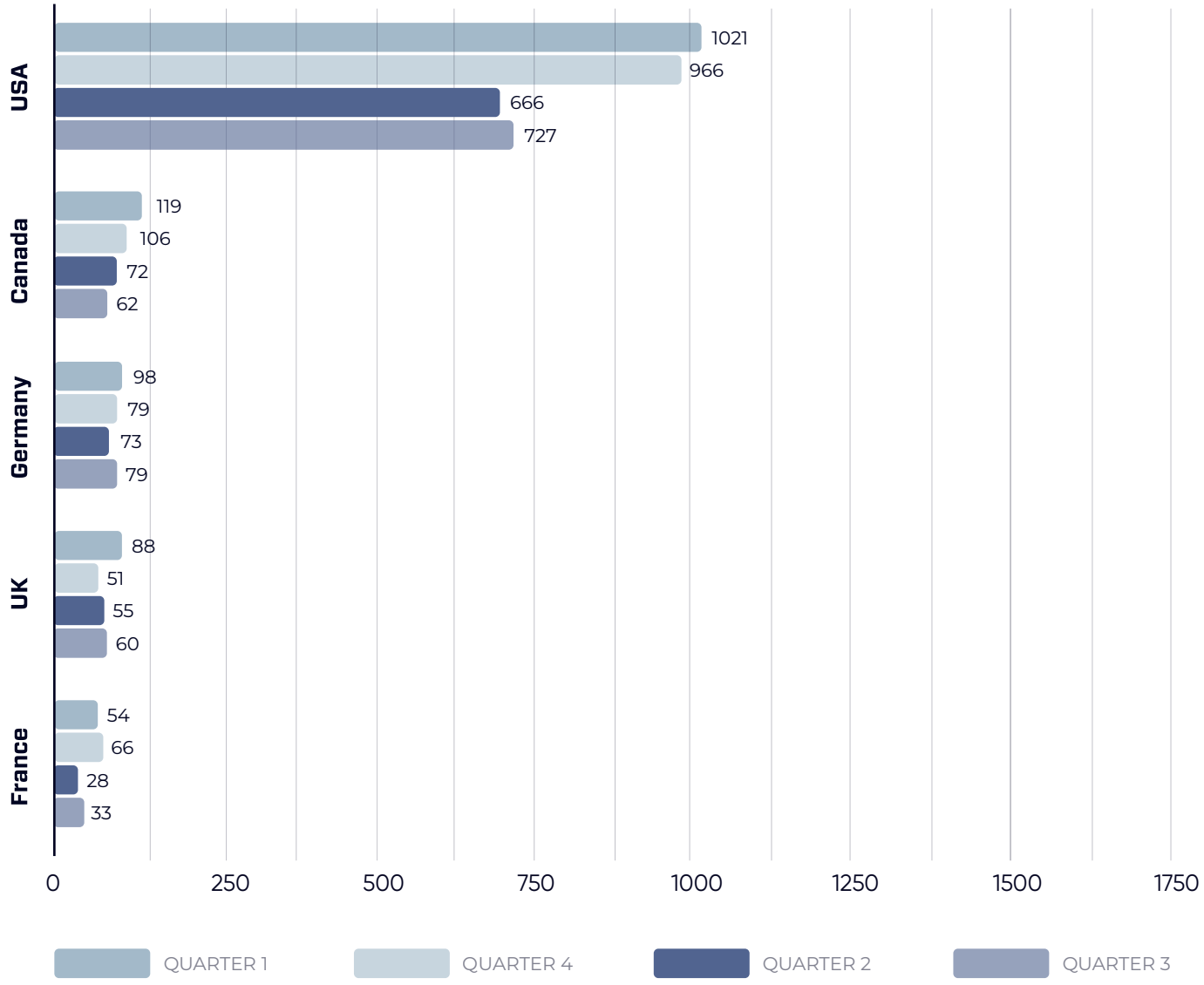
Canada, Germany, and the United Kingdom form the second tier of heavily targeted countries, together representing a significant share of global activity. These markets combine strong digital adoption with mature regulatory environments, making them attractive for double-extortion campaigns where reputational and legal pressure amplifies ransom leverage. The sizable "Others" category (25.3%) further illustrates that ransomware is no longer confined to a small set of high-income economies. Instead, attackers are systematically expanding into emerging and mid-sized markets, mapping global business dependency and pursuing victims wherever digital operations and economic value intersect.

Top of the list

USA, Canada and Germany

06

Ransomware Attacks Comparison Across Country: Q1/2025 - Q4/2025

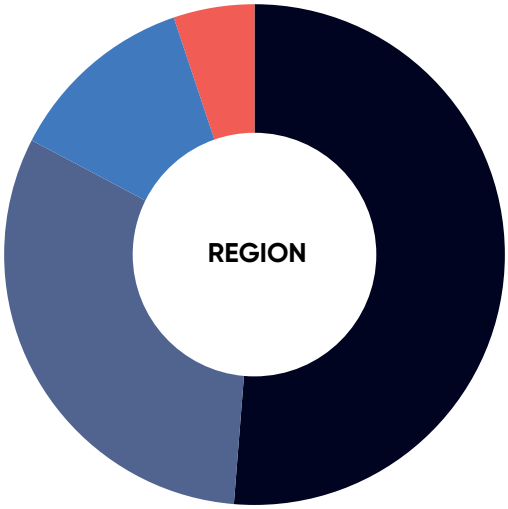


The quarterly comparison by country highlights a consistent and overwhelming concentration of ransomware activity in the United States throughout 2025. With more than 1,000 recorded attacks in Q1 alone and sustained high volumes across all subsequent quarters, the U.S. remains the primary operational and financial center of the global ransomware economy. Its combination of enterprise scale, digital dependency, and high ransom-paying capacity continues to make it the most attractive and reliable market for ransomware operators seeking predictable monetization.

Canada and Germany form a second tier of persistently targeted countries, showing steady activity across all four quarters. Their mature digital infrastructure and strong business ecosystems provide ransomware groups with a broad attack surface and a consistent pool of high-value victims. The United Kingdom and France follow similar patterns at a smaller scale, reflecting how ransomware activity is not episodic but deeply embedded into the economic fabric of developed digital economies. Together, these trends confirm that ransomware campaigns are now geographically optimized, with threat actors prioritizing regions where operational disruption, regulatory pressure, and financial leverage converge to maximize return on investment.

07

Ransomware Attack Distributions by Region: 2025



53.5	NA	12.6	APAC
27.4	EMEA	6.5	LATAM

The regional distribution of ransomware attacks in 2025 highlights a strong concentration of activity in North America, which accounts for more than half of all observed incidents (53.5%). This dominance reflects the region's dense enterprise landscape, high level of digitalization, and the strong monetization potential offered by large, well-insured organizations. For ransomware operators, North America remains the most reliable and profitable operational theater, where attacks can be executed at scale and converted into high-value ransom payments.

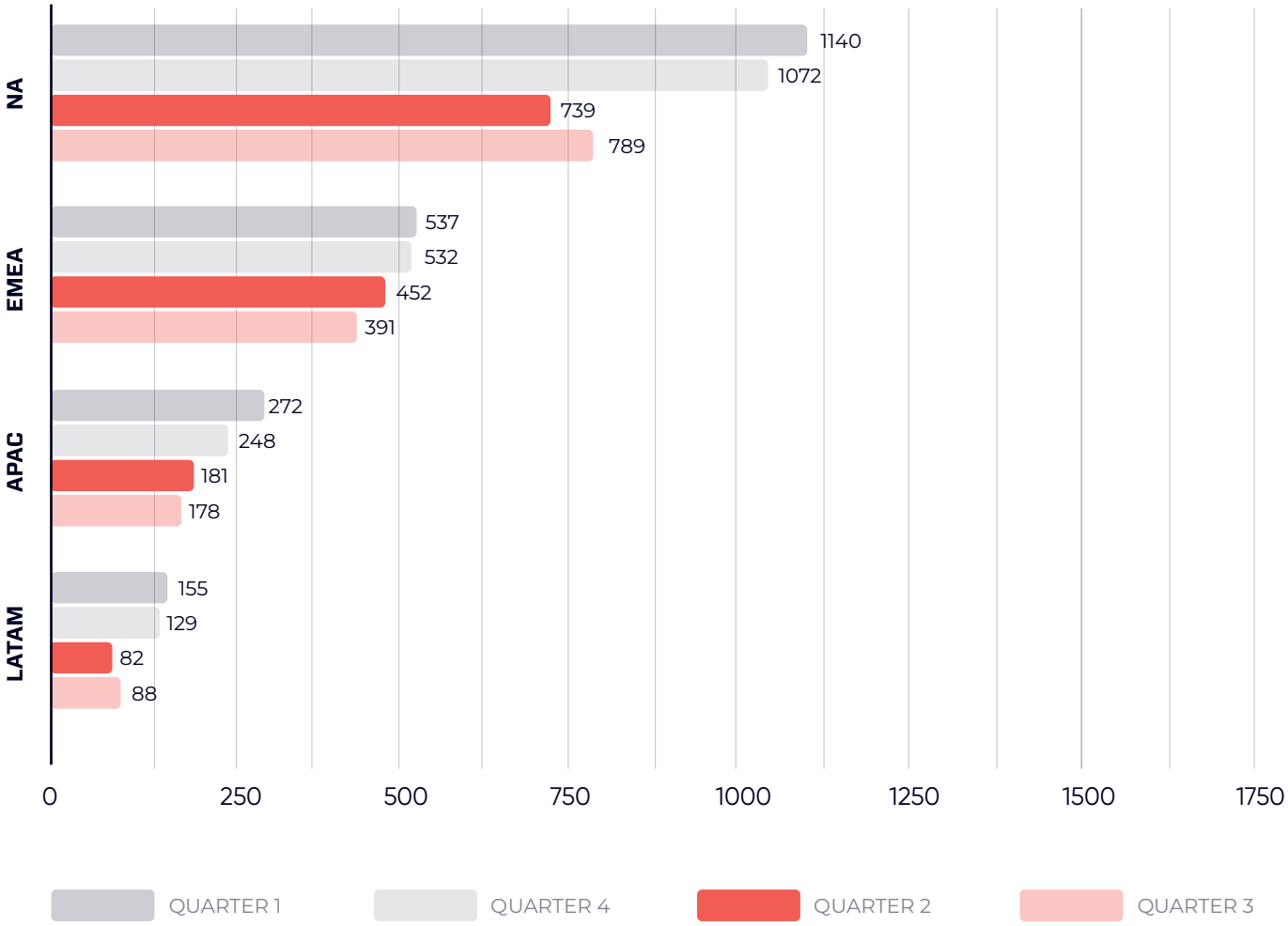
EMEA follows as the second most targeted region with 27.4% of total activity, driven by a large concentration of industrial, financial, and public sector organizations with strict regulatory environments. These conditions amplify extortion pressure and increase attackers leverage. APAC, representing 12.6% of activity, continues to emerge as a growing target zone as digital transformation accelerates across manufacturing, logistics, and technology sectors. LATAM, while currently smaller in volume at 6.5%, shows steady exposure as ransomware groups expand into developing digital economies. Together, these trends confirm that ransomware operations are now globally optimized, with threat actors prioritizing regions where economic value, operational dependency, and disruption potential intersect.

Top of the list

NA, EMEA, and APAC

08

Ransomware Attacks Comparison Across Region: Q1/2025 - Q4/2025



The quarterly regional comparison confirms that ransomware activity in 2025 remained heavily concentrated in North America, with consistently high attack volumes across all four quarters. After peaking at 1,140 incidents in Q1, activity remained elevated through Q4 with more than 1,000 recorded attacks, demonstrating that North America continues to serve as the primary operational and financial hub of the global ransomware economy. The region's dense enterprise footprint, extensive digital infrastructure, and strong monetization potential make it the most attractive environment for sustained ransomware campaigns.

EMEA follows a similar but more moderate trajectory, showing steady growth from Q3 through Q1 and maintaining a consistently high baseline of activity. This reflects the region's mix of industrial, financial, and public sector targets, where regulatory exposure and operational dependency increase extortion leverage. APAC and LATAM, while smaller in absolute volume, display a clear upward trend, particularly toward the end of the year. This signals an ongoing geographic expansion strategy, with ransomware groups increasingly diversifying beyond their traditional strongholds and building long-term operational presence across emerging digital economies.

Ransomware Groups: Q4/2025 Analysis

Emerging ransomware groups like RansomHub, Lynx, and Arcus Media have reshaped the threat landscape with innovative tactics and growing influence, emphasizing the need for organizations to strengthen their cybersecurity defenses.

09

Qilin

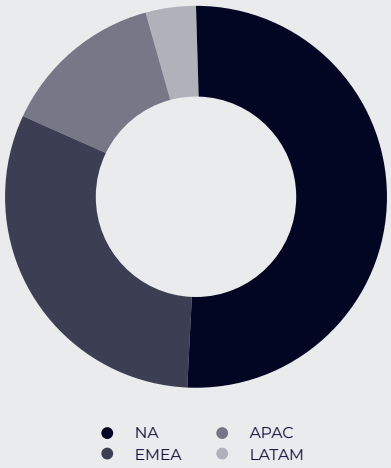
Who is Qilin?

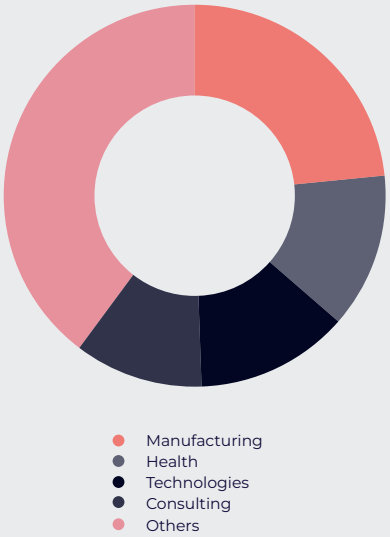
Qilin ransomware, also known as Agenda, has been a prominent and evolving threat across multiple sectors including healthcare, education, manufacturing, logistics, and real estate since July 2022. Operating as a Ransomware-as-a-Service (RaaS) platform, it enables affiliates to deploy the ransomware in exchange for a share of the profits. Technically, Qilin stands out for its use of modern programming languages such as Rust and Go, significantly enhancing its ability to evade traditional detection mechanisms.

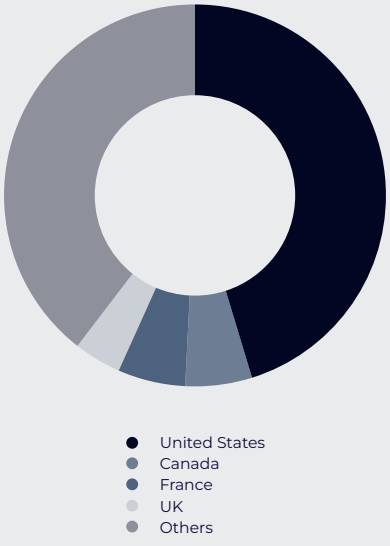
For encryption, Qilin employs AES-256 combined with RSA-2048 for key protection, generating a unique and randomly assigned file extension for encrypted data. Recent variants have introduced improved lateral movement modules, enhanced privilege escalation techniques, and advanced defense evasion capabilities. This sophisticated architecture underlines the group's technical expertise and continuous development cycle.

The financial structure of Qilin is particularly notable. It operates on a high-profit sharing model, offering affiliates up to 85% of ransom payments, especially for ransom demands exceeding $3 million. This lucrative model incentivizes participation and accelerates the expansion of its affiliate ecosystem. Additionally, Qilin's selective targeting strategy, deliberately avoiding CIS countries, highlights a calculated geopolitical and operational focus.

Qilin ransomware, targeting high-value and operationally critical organizations, represents a growing and evolving cyber threat. Its focus on large enterprises, combined with efficient coordination through an affiliate management panel, demonstrates a highly scalable criminal business model. The group's continuous recruitment of new affiliates and rapid malware evolution further reinforce its expanding global footprint and long-term threat potential.







10

Akira

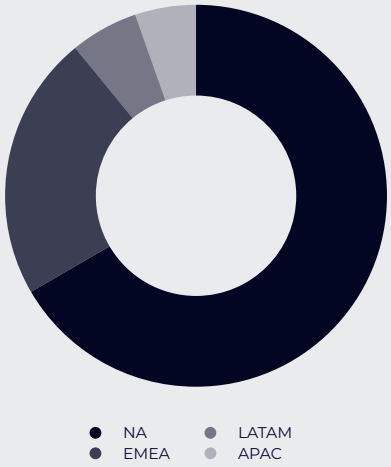
Who is Akira?

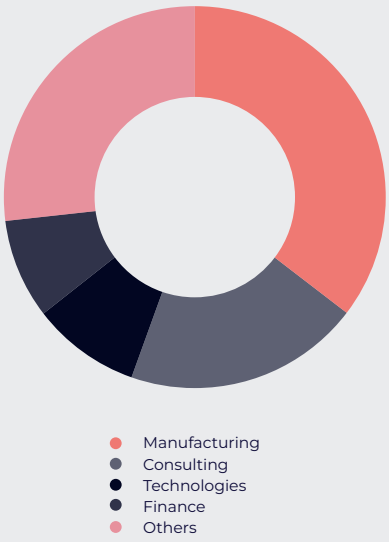
Akira ransomware emerged in early 2023 and rapidly established itself as one of the most active ransomware operations worldwide. The group primarily targets manufacturing, professional services, healthcare, finance, and critical infrastructure sectors. Operating under a Ransomware-as-a-Service (RaaS) model, Akira provides affiliates with a full attack framework including encryption tools, negotiation portals, and data leak infrastructure.

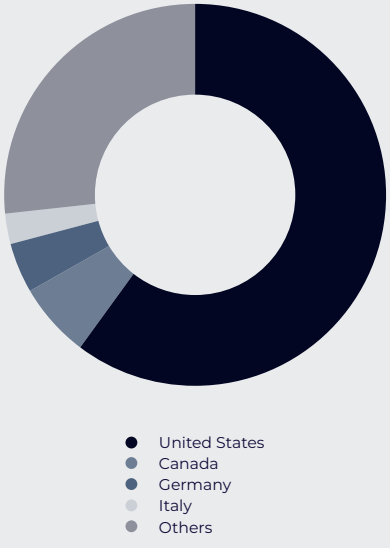
Technically, Akira is developed in C++ and supports both Windows and Linux environments, including VMware ESXi systems, making it highly effective in enterprise and virtualized networks. The ransomware utilizes AES encryption with RSA-based key protection and appends a distinctive ".akira" extension to encrypted files. Affiliates commonly gain initial access through VPN vulnerabilities, stolen credentials, and misconfigured remote access services.

Akira maintains a highly professionalized criminal ecosystem, offering detailed operational documentation and negotiation support for its affiliates. The group actively applies double-extortion tactics, threatening public data leaks to increase ransom pressure. Its aggressive monetization strategy and high victim turnover rate indicate a mature and well-coordinated ransomware enterprise.

Akira ransomware represents a significant operational threat due to its speed of deployment and wide global targeting footprint. Its ability to compromise both traditional enterprise environments and virtual infrastructure platforms makes it particularly dangerous for large organizations. The group's continued expansion and aggressive victimization strategy underline its role as a dominant player in the ransomware ecosystem.







11

Sinobi

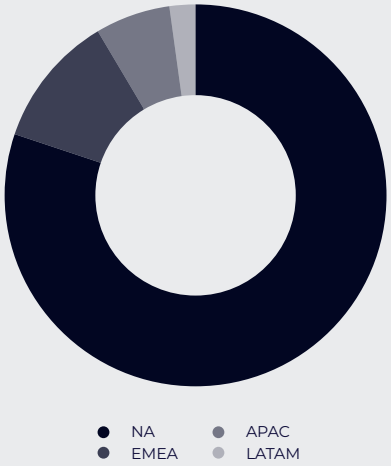
Who is Sinobi?

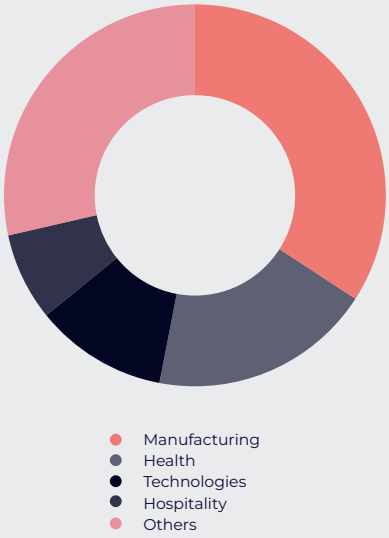
Sinobi ransomware is an emerging ransomware operation that has gained traction through targeted campaigns against small and mid-sized enterprises across manufacturing, logistics, retail, and regional service sectors. While not as globally dominant as major RaaS platforms, Sinobi operates with a focused, financially motivated business model emphasizing rapid compromise and fast monetization.

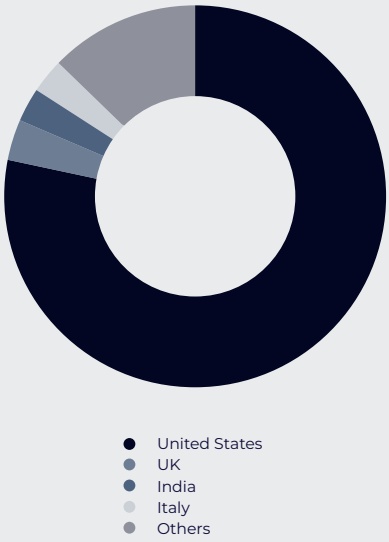
The malware is believed to be written in C++ and employs AES-256 encryption combined with RSA-2048 key protection. Encrypted files are marked with a custom extension and victims are directed to Tor-based negotiation portals. Sinobi campaigns frequently leverage phishing emails, brute-force RDP attacks, and exploitation of unpatched perimeter services for initial access.

Sinobi's operational approach prioritizes volume over individual ransom size, focusing on organizations with limited cybersecurity maturity and weak incident response capabilities. The group systematically applies double-extortion tactics by exfiltrating sensitive data prior to encryption and using public leak threats as negotiation leverage.

Sinobi ransomware represents a growing threat within the mid-market segment. Its increasing campaign frequency suggests an expanding affiliate network and rising automation across its attack lifecycle. As the group continues to refine its delivery mechanisms and extortion strategies, its impact on regional and sector-focused organizations is expected to increase.







12

Inc Ransom

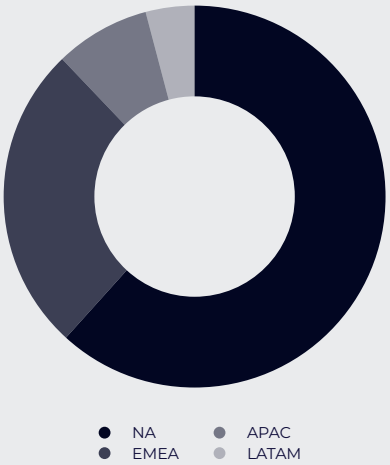
Who is Inc Ransom?

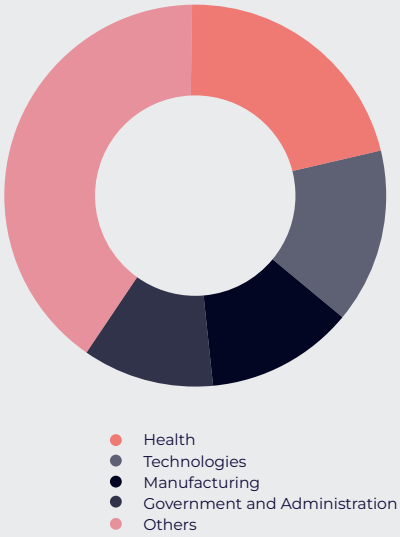
Incransom is a relatively new ransomware operation that surfaced through targeted attacks against manufacturing, construction, engineering, and professional services organizations. The group operates as a financially motivated extortion campaign, combining data theft with file encryption to maximize pressure on victim organizations.

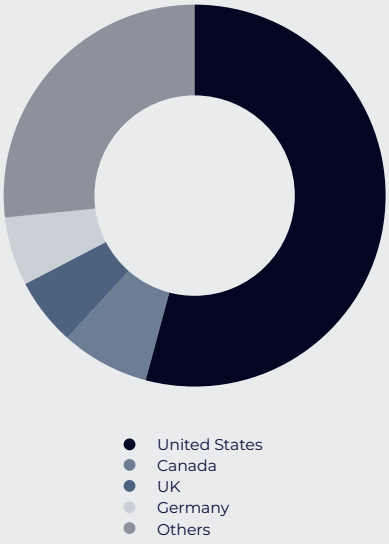
Technically, Incransom is based on a modern ransomware framework utilizing AES encryption with RSA-based key exchange mechanisms. Encrypted files are renamed with a custom extension and ransom notes are deployed across compromised systems. Initial access is commonly achieved through exposed RDP services, compromised VPN accounts, and exploitation of unpatched edge devices.

Incransom actively applies double-extortion techniques, exfiltrating sensitive corporate data prior to encryption and threatening public disclosure through dedicated leak platforms. The group maintains a centralized negotiation infrastructure hosted on Tor, allowing direct communication with victims and facilitating ransom negotiations.

Incransom ransomware represents a growing operational risk, particularly for industrial and engineering-focused organizations with complex IT and OT environments. Its focus on financially viable targets and rapid execution model demonstrates a commercially driven threat actor seeking to scale its operations through repeatable and efficient attack workflows.







13

Cl0p

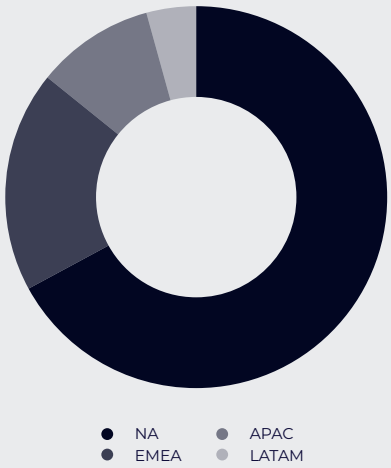
Who is Cl0p?

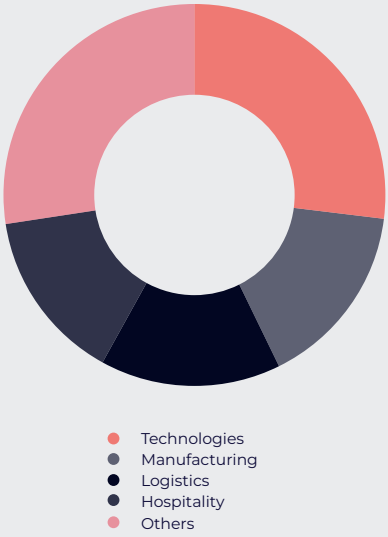
Cl0p ransomware is one of the most well-established and financially successful ransomware operations in the cybercrime ecosystem. Active since 2019, the group is best known for conducting large-scale mass exploitation campaigns against enterprise software vulnerabilities, targeting sectors such as finance, logistics, manufacturing, telecommunications, and government services.

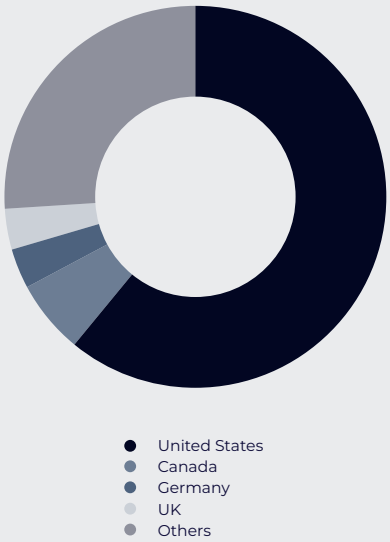
Unlike traditional RaaS groups, Cl0p operates under a closed and highly centralized model. The group is particularly associated with zero-day exploitation campaigns, most notably against file transfer platforms such as MOVEit, GoAnywhere, and Accellion. Instead of deploying widespread encryption, Cl0p often prioritizes data theft and extortion-only operations.

Cl0p employs advanced data exfiltration frameworks and maintains a dedicated leak platform where stolen data is published if ransom demands are not met. The group is known for targeting large enterprises with high regulatory exposure, maximizing reputational and legal pressure during negotiations.

Cl0p represents one of the most strategically dangerous ransomware groups due to its ability to weaponize zero-day vulnerabilities at scale. Its focus on supply-chain platforms enables mass victimization across thousands of organizations simultaneously. The group's operations demonstrate a high level of technical sophistication and long-term strategic planning, positioning Cl0p as a persistent and systemic threat actor.







Q4/2025 Spotlight Uncovering the Significant News Surrounding the Quarter's Top Threats

14

Ransomware Attack Disrupts Japan's E-Commerce Sector as Askul Confirms Massive Data Theft

In December 2025, Japan's e-commerce sector was hit by a major ransomware incident after online retailer Askul confirmed that attackers had stolen the personal data of approximately 740,000 customers. The attack was attributed to the RansomHouse ransomware group, which targeted Askul's internal systems and disrupted order processing and shipping operations across the company's digital commerce platform. The stolen data included business and individual customer details, partner information, and employee records, significantly impacting both commercial operations and customer trust.

The breach forced Askul to temporarily suspend parts of its logistics and order fulfilment processes, creating delays for customers and business partners during the peak year-end shopping period. The company stated that attackers had gained unauthorized access to internal infrastructure before exfiltrating sensitive data and launching their extortion campaign. RansomHouse is known for operating a data-extortion model, focusing on data theft and public exposure rather than only file encryption.

This incident highlights the growing exposure of digital commerce platforms to ransomware groups seeking to monetize both operational disruption and large-scale customer datasets. The Askul attack underscores how ransomware has evolved into a systemic business risk, capable of directly impacting national retail ecosystems and supply chains during critical commercial periods.

INC Ransomware Hits U.S. Public Sector as 340,000 Affected in Washington Library Attack

In mid-December 2025, a ransomware attack on the Pierce County Library System in Washington State exposed the personal data of more than 340,000 individuals, marking one of the most significant public-sector ransomware incidents of the quarter. The attack was claimed by the INC ransomware group, a financially motivated operation known for targeting government bodies and public services with high operational dependency on IT systems.

According to official disclosures, attackers accessed internal systems and exfiltrated sensitive data including names, birthdates, and confidential employee records. The breach disrupted library services across one of Washington's largest counties, affecting digital access platforms and forcing emergency response measures to protect remaining infrastructure. The exposed information placed both citizens and staff at increased risk of identity theft and fraud.

The incident demonstrates how ransomware groups continue to focus on public institutions with large citizen datasets and limited tolerance for service disruption. By targeting essential public services such as libraries, INC ransomware leveraged operational urgency and reputational pressure to increase extortion leverage. The Pierce County breach reinforces the growing need for ransomware readiness across local government and public infrastructure sectors.

Romanian National Water Agency Paralyzed by BitLocker Ransomware Attack

In late December 2025, Romania's national water agency suffered a widespread ransomware attack that disrupted nearly 1,000 IT systems across the organization. The incident, which involved the deployment of BitLocker ransomware, disabled workstations, servers, email services, and GIS platforms, forcing employees to rely on phone and radio communications to maintain operational coordination. While water distribution itself remained unaffected, the digital paralysis significantly impaired administrative and monitoring functions.

The attack caused immediate disruption to internal workflows and delayed reporting, asset management, and field coordination activities. Romanian authorities confirmed that the ransomware had spread across multiple internal networks, rendering critical digital infrastructure unusable. Although no specific threat actor group was publicly named, the scale and coordination of the attack indicate a highly organized ransomware operation.

This incident illustrates the growing vulnerability of national infrastructure operators to ransomware campaigns that aim to cripple operational technology through IT disruption. The Romania water agency attack serves as a stark reminder that ransomware no longer targets only commercial enterprises, but increasingly focuses on national utilities and critical public services where operational downtime carries severe societal impact.

DragonForce and Scattered Spider: The Rise of the "Cartel" Model in Ransomware

One of the most notable developments in the ransomware ecosystem in 2025 was DragonForce openly positioning itself as a "ransomware cartel." The group announced this new structure through underground cybercrime forums and Telegram channels, offering affiliates high profit shares, flexible operational models, and white-label ransomware capabilities. This shift signaled DragonForce's move away from a traditional Ransomware-as-a-Service (RaaS) model toward a more organized and scalable criminal enterprise.

During the same period, DragonForce's activities were increasingly assessed alongside overlapping attack chains attributed to Scattered Spider. Scattered Spider's strengths in social engineering, credential theft, and initial access operations complemented DragonForce's ransomware deployment infrastructure, creating the conditions for highly impactful attacks. Although no joint public announcement was made by the two groups, similarities in tools, timing, and target profiles led security researchers to link their operations.

Experts describe this structure as a cartel-like division of labor within the ransomware ecosystem. Assigning stages such as initial access, lateral movement, and data theft to different actors has made attacks both faster to execute and more difficult to detect. DragonForce's forum-announced model, combined with operations associated with Scattered Spider, clearly demonstrates that the ransomware threat is increasingly driven not by isolated groups, but by interconnected criminal networks operating in coordination.

ClOp Brings Supply Chain Attacks via Oracle and Cleo Back Into Focus in 2025

The year 2025 marked a renewed surge in supply chain–focused attacks by the Cl0p ransomware group, once again placing the threat actor at the center of the global cybersecurity agenda. Rather than targeting individual organizations directly, the group focused on critical vulnerabilities in widely used enterprise software to gain access to broad customer ecosystems relying on these platforms.

Among Cl0p's most notable activities during the year were attacks targeting file transfer solutions developed by Cleo and the Oracle E-Business Suite platform. In these campaigns, the group rapidly weaponized vulnerabilities assessed as zero-days, enabling swift access to the systems of numerous organizations.

In the early months of the year, critical flaws identified in Cleo's Harmony, VLTrader, and LexiCom products were exploited by Cl0p as part of large-scale data theft campaigns. As a result, the names of hundreds of organizations were published on the group's leak platforms, with the impact extending beyond directly targeted companies to include supply chain partners using the affected software.

Cl0p's activities in 2025 were not limited to file transfer software. In October, a critical vulnerability in Oracle E-Business Suite that enabled unauthorized remote access became the group's next focal point. Following the disclosure of the flaw, widespread exploitation attempts against internet-facing Oracle EBS systems were observed. During this period, attackers were reported to have gained unauthorized access to systems, exfiltrated sensitive corporate data, and used it for extortion purposes.

A key aspect of these campaigns was Cl0p's departure from traditional ransomware tactics. In many cases, the group avoided encrypting systems altogether, instead prioritizing data theft and applying pressure through the threat of public disclosure. This approach aimed to inflict damage through reputational harm and regulatory exposure rather than operational disruption.

Experts note that Cl0p's attack model throughout 2025 underscored the growing severity of supply chain risks within the ransomware ecosystem. In particular, vulnerabilities in widely deployed enterprise software were shown to have the potential to rapidly escalate into mass compromise events.

Security authorities emphasize that preventing similar incidents requires more than timely patching alone, highlighting the need for continuous monitoring of internet-exposed systems and proactive threat detection to identify signs of compromise at an early stage.

Most Used CVEs by Ransomware Groups Q4/2025 Analysis A Study of Prevalent Vulnerabilities

15

Critical Vulnerabilities Analysis Over Q4/2025

In the fourth quarter of 2025, ransomware activity remained elevated as threat actors continued to prioritize unauthenticated remote code execution (RCE) and post-compromise privilege escalation vulnerabilities to rapidly gain initial access and establish control over enterprise environments. During this period, CVE-2025-53770 affecting Microsoft SharePoint Server was actively exploited by the 4L4MD4R and Warlock ransomware groups, while CVE-2025-10035 in Fortra GoAnywhere MFT was leveraged by Medusa to compromise exposed file transfer systems and accelerate data-extortion operations.

Enterprise business applications were also heavily targeted in Q4 2025. The Cl0p ransomware group exploited CVE-2025-61882 in Oracle E-Business Suite to gain unauthenticated network access and compromise Oracle Concurrent Processing components. In parallel, CVE-2025-42999 in SAP NetWeaver Visual Composer was abused by RansomExx in post-authentication scenarios, allowing attackers to execute malicious payloads and fully compromise affected systems.

Perimeter and infrastructure technologies continued to present high-impact attack surfaces. The critical CVE-2024-21762 in Fortinet FortiOS SSL VPN remained a widely used initial access vector for the Qilin ransomware group, enabling remote code execution against exposed firewall appliances. Following initial compromise, attackers frequently relied on CVE-2025-29824 in the Windows Common Log File System (CLFS) driver, which was exploited by the Play ransomware group to escalate privileges to SYSTEM level and deploy ransomware across enterprise networks.

10 - Critical

Fortra GoAnywhere MFT

CVE-2025-10035

Group: Medusa

10 - Critical

React Server Components

CVE-2025-55182

Group: Weaxor ransomware

10 - Critical

SAP NetWeaver Visual Composer

CVE-2025-31324

Group: BianLian, RansomExx

9.8 - Critical

Oracle E-Business Suite

CVE-2025-61882

Group: Cl0p

9.8 - Critical

Fortinet FortiOS SSL VPN

CVE-2024-21762

Group: Qilin

9.8 - Critical

Microsoft SharePoint Server

CVE-2025-53770

Group: 4L4MD4R, Warlock Ransomware

9.1 Critical

SAP NetWeaver Visual Composer

CVE-2025-42999

Group: Ransomexx

7.8 High

Windows Common Log File System Driver

CVE-2025-29824

Group: Play

7.5 High

Oracle E-Business Suite

CVE-2025-61884

Group: Cl0p

16

Deep Dive in Tactics, Techniques, and Procedures

Ransomware operators continue to refine their attack strategies by aggressively exploiting remote code execution vulnerabilities in externally exposed enterprise systems. In 2025, flaws such as CVE-2025-10035 in Fortra GoAnywhere MFT, CVE-2025-55182 in React Server Components, CVE-2025-61882 in Oracle E-Business Suite, CVE-2024-21762 in Fortinet FortiOS, CVE-2025-53770 in Microsoft SharePoint Server, and CVE-2025-42999 in SAP NetWeaver enabled attackers to execute arbitrary code without authentication or with minimal privileges. By abusing deserialization flaws and improper request handling, ransomware groups rapidly transitioned from initial access to full system compromise, often within minutes, allowing them to deploy ransomware payloads and initiate data exfiltration.

Once initial access was achieved through remote code execution, attackers frequently relied on privilege escalation vulnerabilities to strengthen their foothold and expand control across compromised environments. CVE-2025-29824, a use-after-free flaw in the Windows Common Log File System (CLFS) driver, was leveraged in post-compromise scenarios to escalate privileges to SYSTEM level. This capability enabled ransomware operators to disable security controls, access protected credentials, and deploy ransomware across multiple hosts, significantly amplifying the impact of the attack.

In parallel, ransomware campaigns increasingly incorporated authentication bypass and pre-authentication vulnerabilities to facilitate reconnaissance and unauthorized data access prior to full exploitation. CVE-2025-61884 in the Oracle Configurator component of Oracle E-Business Suite allowed unauthenticated attackers to access sensitive application data over HTTP, supporting early-stage discovery and target validation. Combined, the exploitation of remote code execution, privilege escalation, and authentication bypass vulnerabilities demonstrates a clear shift toward streamlined, high-impact attack chains designed to achieve rapid compromise, maximize operational disruption, and increase extortion pressure on victim organizations.

1.TTP Exploiting Remote Code Execution Vulnerabilities

CVE-2025-10035: This vulnerability involves a deserialization flaw in the License Servlet of Fortra's GoAnywhere MFT, which can allow an attacker with a forged license response signature to deserialize attacker-controlled objects. Under specific conditions, this may lead to command injection and remote code execution on the affected system.

CVE-2025-55182: This vulnerability involves a pre-authentication remote code execution flaw in React Server Components, caused by unsafe deserialization of attacker-controlled HTTP payloads sent to Server Function endpoints. An unauthenticated attacker can exploit this issue to execute arbitrary code on the affected server.

CVE-2025-61882: This vulnerability involves an unauthenticated remote code execution flaw in the Oracle Concurrent Processing component of Oracle E-Business Suite, caused by improper handling of network-accessible HTTP requests.

CVE-2024-21762: This vulnerability involves an out-of-bounds write flaw in Fortinet FortiOS and FortiProxy, which can allow an unauthenticated remote attacker to execute arbitrary code or commands via specially crafted network requests. Successful exploitation can result in full compromise of the affected firewall or proxy device.

CVE-2025-53770: This vulnerability involves unsafe deserialization of untrusted data in on-premises Microsoft SharePoint Server, which can allow an unauthenticated remote attacker to execute arbitrary code over the network. Exploitation of this flaw may result in full compromise of the affected SharePoint server.

CVE-2025-42999: This vulnerability involves a deserialization flaw in the SAP NetWeaver Visual Composer Metadata Uploader, where a privileged user can upload malicious content that, when deserialized, may lead to remote code execution and compromise of the host system's confidentiality, integrity, and availability.

2.TTP Exploiting Privilege Escalation Vulnerabilities

CVE-2025-29824: This vulnerability involves a use-after-free flaw in the Windows Common Log File System (CLFS) driver, which allows a local authenticated attacker to elevate privileges on the affected system. Successful exploitation can result in SYSTEM-level access.

3.TTP Bypassing Authentication and Exploiting Pre-Authentication Vulnerabilities

CVE-2025-61884: This vulnerability involves an authentication bypass flaw in the Oracle Configurator component of Oracle E-Business Suite, which allows an unauthenticated remote attacker with network access to gain unauthorized access to sensitive application data over HTTP.

CVE-2025-31324: This vulnerability affects SAP NetWeaver Visual Composer. It is an unauthenticated file upload vulnerability with a CVSS score of 10.0, allowing remote threat actors to upload arbitrary executable binaries to the server.

Final Words

Strengthening Cybersecurity Against Ransomware Attacks:
To mitigate risks, adopt multi-layer security approaches and proactive and comprehensive solutions.

Conclusion

The year 2025 clearly demonstrated the scale and maturity of the global ransomware threat. Throughout the year, ransomware campaigns impacted **2,373 confirmed victims across 134 countries**, spanning **27 industries** and involving **125 distinct ransomware groups.**

This breadth highlights how ransomware has evolved into an industrialized ecosystem driven by shared techniques, reusable tooling, and rapid adaptation rather than isolated criminal operations.

A significant portion of ransomware activity in 2025 was enabled by the exploitation of critical vulnerabilities in internet facing enterprise technologies. Platforms such as **Fortinet FortiOS SSL VPN, Microsoft SharePoint Server, SAP NetWeaver, Oracle E Business Suite, and managed file transfer solutions** remained prime targets for initial access. These weaknesses were leveraged by prominent groups including **Qilin, Cl0p, Play,** and **Akira** to rapidly compromise environments, followed by privilege escalation and lateral movement to maximize operational impact.

Structurally, the ransomware ecosystem in 2025 was characterized by a dual dynamic. While a small number of well established groups maintained consistent operational output, a constantly shifting population of smaller or rebranded actors sustained high attack volumes and complicated attribution efforts. This fragmentation, combined with continued reliance on vulnerability exploitation, reinforces the need for organizations to prioritize continuous vulnerability management, rapid remediation of exposed systems, and intelligence driven security strategies to effectively reduce ransomware risk moving forward.

Key Observations

THE REPORT'S DATA DEMONSTRATES SEVERAL CRITICAL REALITIES

- **Ransomware groups are optimizing for impact.**

Attacks are increasingly shaped by industry vertical, geographic location, operational sensitivity, and regulatory exposure. Victim selection is now driven by business logic rather than technical exposure alone.

- **Perimeter exploitation has become the norm.**

The most exploited CVEs reveal persistent deficiencies in patch management and VPN infrastructure hardening. Critical flaws affecting technologies such as Fortinet, SonicWall, Citrix, and Oracle continue to provide reliable entry points for ransomware operators.

- **Targeted sectors and geographies are diversifying.**

While North America and manufacturing remain heavily affected, ransomware activity is expanding across APAC and LATAM regions, as well as into public services, logistics, and regional consulting, where operational disruption can still generate significant leverage.

- **The ransomware economy remains highly adaptive.**

Groups such as Qilin illustrate scalable affiliate driven operations, while Cl0p demonstrates the effectiveness of precision supply chain exploitation. Together, these models reflect an ecosystem with both operational depth and strategic flexibility.

Ultimately, defending against ransomware in 2026 and beyond will require more than reactive security controls. Organizations must adopt proactive threat intelligence, sector aware risk modeling, and continuous attack surface monitoring to keep pace with adversary evolution. Brandefense remains committed to supporting this effort by delivering timely insights and forward looking threat intelligence to help organizations strengthen resilience against ransomware threats.

18

Recommendation

As ransomware attacks continue to rise and evolve, it is critical for organizations and nations to develop proactive and comprehensive strategies to mitigate these threats.

Below are key steps that can be taken to minimize the impact of ransomware attacks:

Strengthening Cybersecurity Infrastructure

Given that ransomware groups frequently exploit zero-day vulnerabilities, organizations must ensure continuous monitoring and patch management processes to address these vulnerabilities promptly. System updates should be applied without delay, and vulnerability management processes must be enhanced to close potential gaps in security.

Enhancing Security in Critical Sectors

Sectors such as manufacturing, business services, and retail are primary targets for ransomware attacks. Companies in these industries should regularly update their cybersecurity training programs and educate employees about social engineering tactics. Additionally, strengthening backup processes and revising disaster recovery plans are crucial to preventing operational disruptions and minimizing financial losses.

Focusing on Small and Medium-Sized Enterprises (SMEs)

SMEs are perceived as more vulnerable by ransomware groups. These businesses need to increase their investments in cybersecurity, implement robust authentication systems, and consistently monitor security gaps. The use of multi-factor authentication (MFA) and other advanced security measures should be prioritized to protect against potential attacks.

Defending Against Ransomware Group Tactics

Ransomware groups such as RansomHub, LockBit3, and Play use double extortion tactics. To counter this, organizations should implement strong encryption and data protection methods, minimizing the impact of potential data leaks. Keeping track of the evolving tactics used by these groups and establishing threat intelligence and early warning systems will enable organizations to respond quickly and effectively to threats.

Developing Region-Specific Defense Strategies

Given that North America and EMEA regions face the highest number of attacks, it is essential to tailor security strategies to the specific threat models and risks of each region. Implementing cybersecurity measures aligned with local regulations and sector-specific requirements will create a more effective defense framework.

Raising Cybersecurity Awareness and Training

Employees often represent the weakest link in the defense chain. Regular awareness training and simulated attack scenarios can help increase awareness and preparedness against ransomware attacks. Specifically, organizations should focus on educating employees about social engineering threats and enforce strong password policies to reduce the risk of compromise.

Organizations can benefit from working with cybersecurity companies such as Brandefense, which provide up-to-date threat intelligence and analysis, helping businesses build robust defense strategies against evolving ransomware threats. Leveraging expert resources can better prepare organizations for both current and future cyber risks.

Why Digital Risk Protection is Important?

Digital risk protection, attack surface management and threat intelligence are critical to organizations; because these three elements form the basis of cybersecurity defense.

Why Brandefense?

In today's hyperconnected world, organizations face escalating digital risks across open, deep, and dark web ecosystems. From phishing and credential leaks to data exposure and third-party compromise, digital threats increasingly originate beyond the traditional network perimeter.

Digital Risk Protection (DRP) bridges this visibility gap — enabling companies to proactively detect, analyze, and mitigate emerging external threats before they cause operational or reputational damage.

A mature DRP strategy enhances resilience by:

- Identifying exposed data and impersonation attempts early.
- Eliminating fraudulent domains and phishing sites.
- Monitoring supplier vulnerabilities and digital footprints.
- Providing actionable, real-time threat intelligence.
- This proactive visibility empowers CISOs and SOC teams to prevent breaches instead of reacting to them.

About Brandefense

Brandefense is a leading Digital Risk Protection and Threat Intelligence Platform designed to help organizations detect, analyze, and mitigate external cyber threats before they impact business operations or reputation. Our unified platform combines multiple intelligence disciplines to provide complete external risk visibility:

01

Threat Intelligence (TI)

Real-time monitoring of threat actor discourse, malware activity, APT operations, and botnet infrastructures.

02

Digital Risk Protection (DRP)

Automated detection and takedown of phishing, credential leaks, and impersonation campaigns across the surface, deep, and dark web.

03

Third-Party Cyber Risk Management (TPCRM)

Continuous scoring and monitoring of suppliers and partners to identify exposures before they are exploited.

04

External Attack Surface Management (EASM):

Discovery of external assets and misconfigurations before attackers can leverage them.

Why Organizations Choose Brandefense

Brandefense combines automation, analyst expertise, and rich intelligence coverage to deliver measurable results in threat prevention, brand protection, and external risk management.

All-in-One Platform

Unified visibility across threat intelligence, attack surfaces, and digital risks.

Human + Machine Intelligence

Proprietary data enhanced by expert validation for unmatched accuracy.

Credit-Based Model

Flexible system allows clients to scale investigations and takedowns as needed.

Regulatory Alignment

GDPR-compliant, ISO-aligned processes and executive-ready reporting.

Awards

With its innovative solutions and technology-driven approach in the field of cybersecurity, Brandefense once again proved its industry leadership in 2025 by receiving prestigious awards. These awards are not only a testament to our technological excellence but also an international recognition of our end-to-end protection approach offered to our clients.

At Brandefense, we continue to raise the bar in threat intelligence, dark web monitoring, brand protection, and digital risk prevention — embracing each award as a responsibility to go even further.

Deloitte EMEA Technology Fast 500

500 Technology Fast 500 2024 EMEA WINNER Deloitte.

Deloitte Technology Fast 50 in Türkiye

50 Deloitte. Technology Fast 50 2023 TÜRKİYE

Global Infosec Awards

2025 WINNER CYBER SECURITY EXCELLENCE AWARDS

- Brand Protection & Dark Web Monitoring Provider of the Year
- Best Digital Risk Protection Solution (Cybersecurity Product/Service)
- Best Threat Intelligence Solution (Cybersecurity Product/Service)

Smarti Awards 2024

smartiawards WINNER 24

Cybersecurity Excellence Awards

GLOBAL INFOSEC AWARDS WINNER CYBER DEFENSE MAGAZINE 2025

- Hot Company
  Digital Risk Protection
- Publisher's Choice
  Third Party Cyber Risk Management
- Visionary
  Threat Intelligence

Gold Smarti Awards 2023

smartiawards WINNER 23

IT Harvest Cyber 150

IT-HARVEST CYBER 150 WINNER

Brandefense has earned a coveted spot on IT-Harvest's esteemed annual Cyber 150 list in the Threat Intelligence category!

PSM Awards

winner 2024 PSM AWARDS

Real Experiences Shared on Gartner Peer Insights »

Don't just rely on our claims; hear it straight from our satisfied customers. Delve into the authentic user reviews on Gartner Peer Insights, where our clients candidly share their experiences with our products and services. Discover how our solutions have made a real difference in their businesses, and learn why they trust and recommend us.

Gartner peerinsights™

Brandefense

★★★★★ 4.7 out of 5

Very Good CTI And Brand Monitoring Source

Brandefense acts as the backbone of our Cyber Threat Intelligence and brand monitoring activities.

- IT Security and Risk Management

25.04.2023

Intelligence Beyond The Borders

The product helped us to mitigate our brand risk with giving us very valuable intelligence. The most I liked about Brandefense are user friendly interface, low false positive ratio, proactive use cases.

- IT Security and Risk Management

05.04.2023

Like They Said, They Know What Hackers Know About Us

It is like I have glass that shows the whole dark web. Dark web monitoring and botnet intelligence services are working great.

- Engineering

19.10.2022

See in Action :
Request a Demo

BRANDEFENSE

United States · 300 Delaware Ave. Ste 210 #328 Wilmington, DE 19801 / USA
Turkey · Üniversiteler Mh. 1605 Cd. Cyberpark Vakıf Binası No: B25 Çankaya/Ankara

brandefense.io • info@brandefense.io