CYFIRMA
DECODING THREATS

CYFIRMA ANNUAL INDUSTRIES REPORT

2024

WWW.CYFIRMA.COM

EXECUTIVE SUMMARY

The CYFIRMA Industries Report provides cutting-edge cybersecurity insights and telemetry-driven statistics on global industries. Spanning the last 365 days and highlighting year-over-year changes between 2023 and 2024, this report covers 13 key industries and presents critical trends and data in a compelling infographic format.

INTRODUCTION

Welcome to the CYFIRMA Infographic Industry Report, where we examine the external threat landscape across 13 industries over the past year. Through clear, data-driven visuals and expert insights, we present concise analyses of attack campaigns, phishing telemetry, and ransomware incidents affecting organizations worldwide.

Leveraging our cutting-edge platform telemetry and the deep expertise of our analysts, this report highlights both cross-industry trends and year-over-year changes, along with detailed, industry-specific breakdowns. Our goal is to equip you with actionable intelligence that helps you stay ahead in the ever-evolving cybersecurity landscape.

CYFIRMA
DECODING THREATS

METHODOLOGY

CYFIRMA provides cyber threat intelligence and external threat landscape management platforms, DeCYFIR and DeTCT, which utilize artificial intelligence and machine learning to ingest and process relevant data, complemented by hands-on CTI research.

For the purpose of these reports, we leverage the following data from our platform. These are data processed by AI and ML automation based on both human research input and automated ingestions.

OBSERVED ATTACK CAMPAIGNS

Leveraging our Early Warning platform data set, we present known attack campaigns conducted by known advanced persistent threat actors. Both nation-state and financially motivated.

Each attack campaign may target multiple organizations across various countries.

Campaign durations can vary from weeks to months or even years. They are sorted by the "last seen" date of activity to include the most relevant ones. Note that this may result in campaigns stacking up on later dates, affecting time-based trends.

Attribution to specific threat actors can be murky due to increasingly overlapping TTPs and commodity tools used. While suspected threat actors in this report are attributed with high confidence, we acknowledge the potential for inaccuracy.

PHISHING

Our data focuses on phishing campaigns rather than individual phishing or spear-phishing emails, which may limit visibility into more advanced single-target attacks.

Our primary focus is on detecting brand impersonation over intended targets. Due to our collection methodology and automation, we may not present comprehensive victimology for phishing campaigns across all industries as some are simply not good phishing lures.

RANSOMWARE

Our data on victims in this report is directly collected from respective ransomware blogs, though some blogs may lack detailed victim information beyond names or domains, impacting victimology accuracy during bulk data processing.

In some cases, there are multiple companies that share the same name but are located in different countries, which may lead to discrepancies in geography and industry. Similar discrepancies occur with multinational organizations where we are not able to identify which branch in which country was actually compromised. In such a case, we count the country of the company's HQ.

During the training of our processing algorithms, we manually verified results for industry and geography statistics at an accuracy rate of 85% with a deviation of ±5%. We continuously fine-tune and update the process.

Data related to counts of victims per ransomware group and respective dates are 100% accurate at the time of ingestion, as per their publishing on the respective group's blog sites.

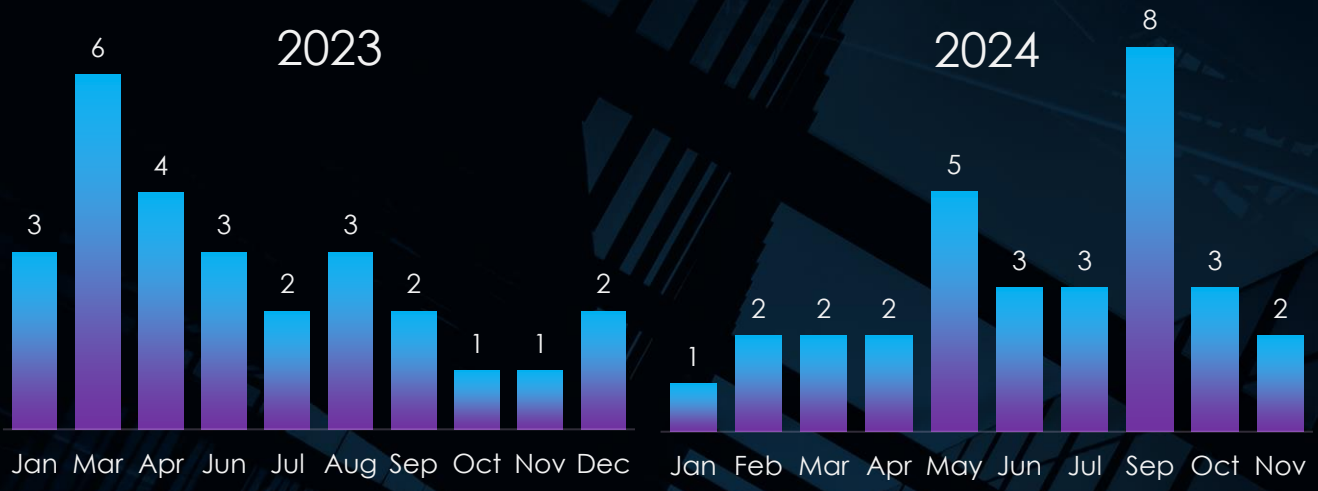
Finally, we acknowledge that many victims are never listed as they are able to make a deal with the attackers to avoid being published on their blogs.

While this report contains statistics and graphs generated primarily by automation, it undergoes thorough review and enhancement for additional context by CYFIRMA CTI analysts to ensure the highest quality and provide valuable insights.

ADVANCED PERSISTENT THREATS

YEAR-TO-YEAR ELEVATION

In 2023, the DeCYFIR platform recorded a total of 27 campaigns. Meanwhile, in 2024, it recorded 31, representing a 14.8% increase year-over-year.



The monthly chart shows a distribution of observed campaigns. We can see periods of relative calm as well as periods with significant spikes in activity.

The spikes are mostly linked to the discovery of new TTPs for specific threat actors or new exploitable vulnerabilities.

For example, the spike in September 2024 is linked to the activity below:

Lazarus Group (North Korea) intensified its VMConnect campaign against software developers, posing as Capital One employees, conducting fake interviews, and delivering malicious GitHub links via LinkedIn.

FIN7 (Russia), often collaborating with APT29 (Cozy Bear), hijacked .NET applications (Hijack Execution Flow: AppDomainManager) to inject malicious payloads. Cozy Bear also targeted Microsoft 365 accounts in NATO countries, disabling security features like Purview Audit.

Fancy Bear (APT28, Russia) continued with disinformation and large-scale phishing attacks against government, NGO, education, and transportation targets in Ukraine, Western Europe, and North America.

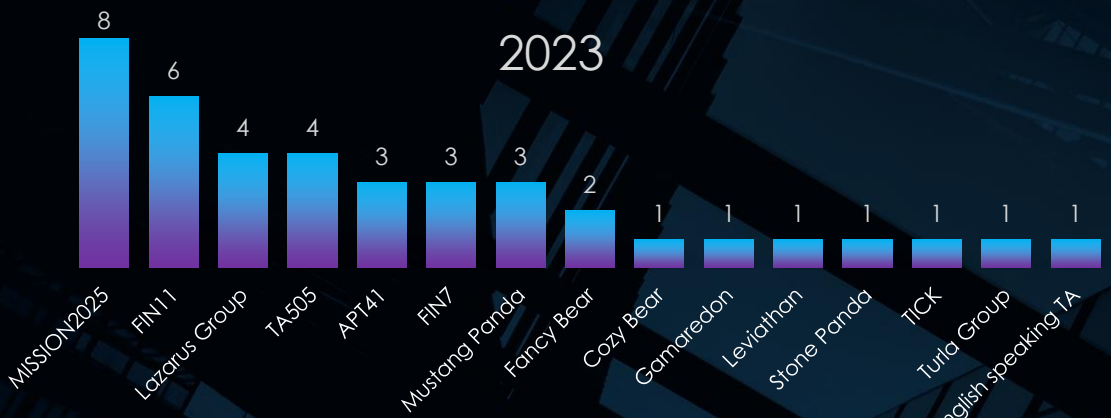
TA505 (Russia) continued large-scale phishing operations, focusing on financial data theft.

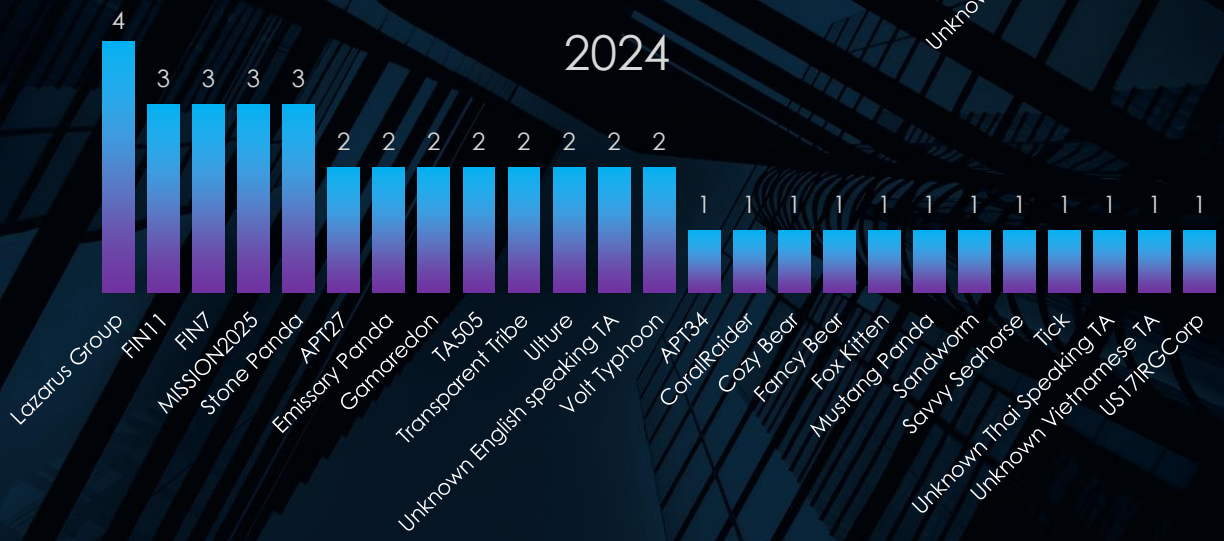
Stone Panda (APT10, China) conducted supply chain attacks by infiltrating software providers and embedding malware into legitimate updates.

Transparent Tribe (Pakistan) carried out espionage in South Asia, using custom malware to steal sensitive documents and monitor communications.

SUSPECTED THREAT ACTORS

Alongside the moderate increase in observed campaigns, we also noticed a disproportionately large increase in observed threat actors. In 2023, the detected APT campaigns were linked to 15 threat actors. However, in 2024, this number surged to 25 groups (+40%).

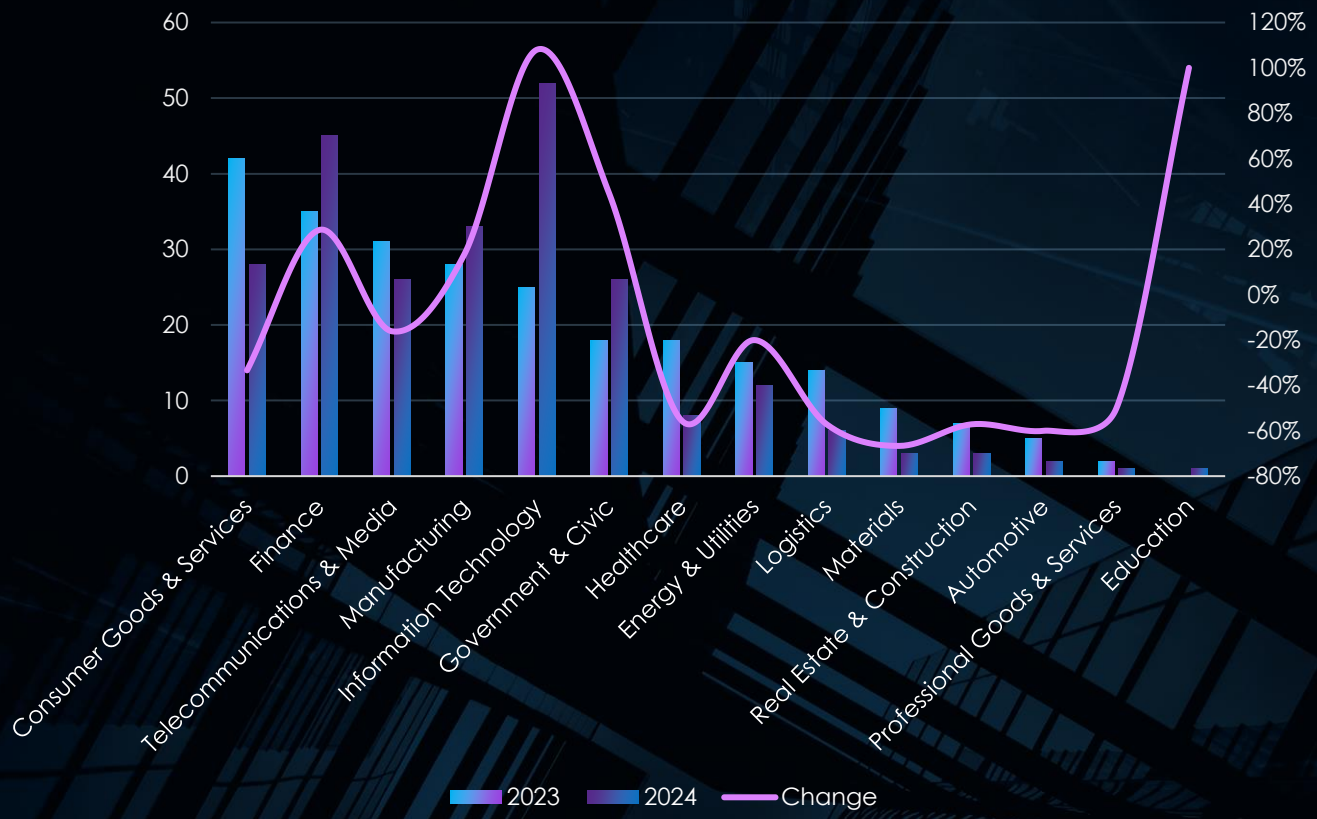




Furthermore, we can also observe changes in the activity of threat actors. While Lazarus Groups maintained four campaigns annually, the 2023 leader, MISSION2025 (APT 41 Nexus of activity), has experienced a significant decline from eight to three campaigns. We attribute this to the fragmentation of Chinese nation-state activity and a substantial shift in the Chinese government's focus.

Notably, there are also many threat actors from various countries. The traditional players like Russia and China are now joined by substantial activity from Vietnam, India, Thailand, Pakistan, and more.

MOST ATTACKED INDUSTRIES



The chart above shows industries sorted by the number of recorded attacks in 2023, from the most frequently targeted to the least. Each bar for the respective industry indicates how many campaigns included victims from that sector in a specific year. The trendline shows percentage changes compared to the previous year.

In 2023, the most targeted industries were Consumer Goods & Services, Finance, and Telecommunications & Media. By 2024, the threat landscape shifted significantly. Information Technology, Finance, and Manufacturing became the top three most targeted industries.

In 2024, the largest increases in attacks appeared in Information Technology (+108%), Government & Civic (+44.4%), and Finance (+28.6%). The Education sector increased from zero to one victim, which is effectively an infinite percentage rise.

At the same time, several industries saw significant decreases in attacks. Materials (-66.7%), Automotive (-60%), as well as Logistics and Real Estate & Construction (both -57.1%) were the most reduced.

In total, 9 out of the 13 industry categories experienced fewer observed APT attacks, even though the overall number of attacks rose by almost 15%. This suggests that the threat landscape is shifting. Major threat groups, mostly supported by nation-states, have realigned their focus, most likely in response to increasing global tensions and growing armed conflicts.

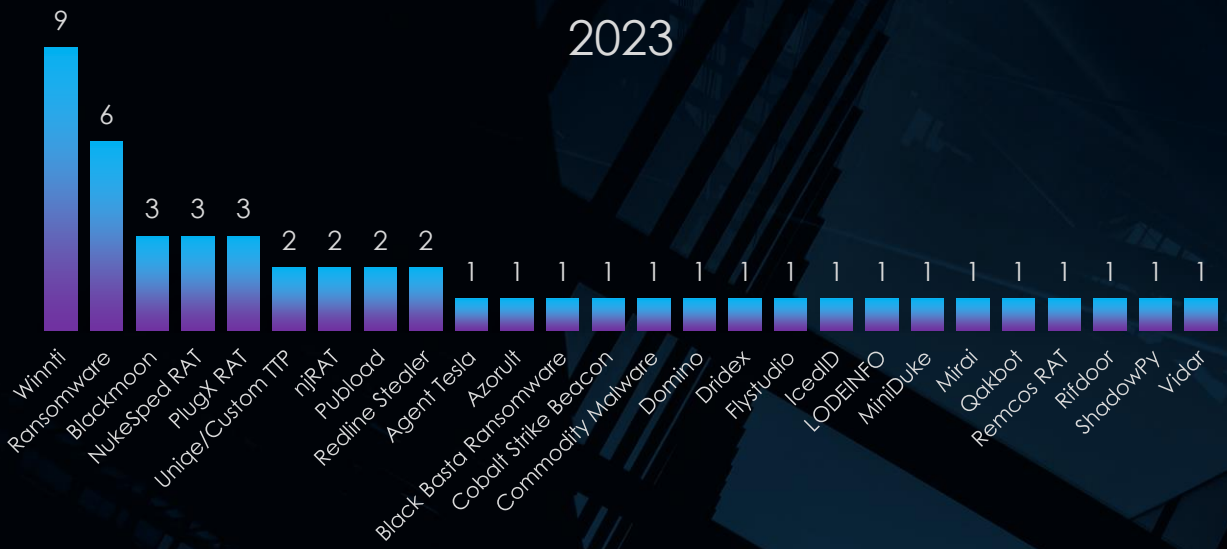
GEOGRAPHICAL DISTRIBUTION

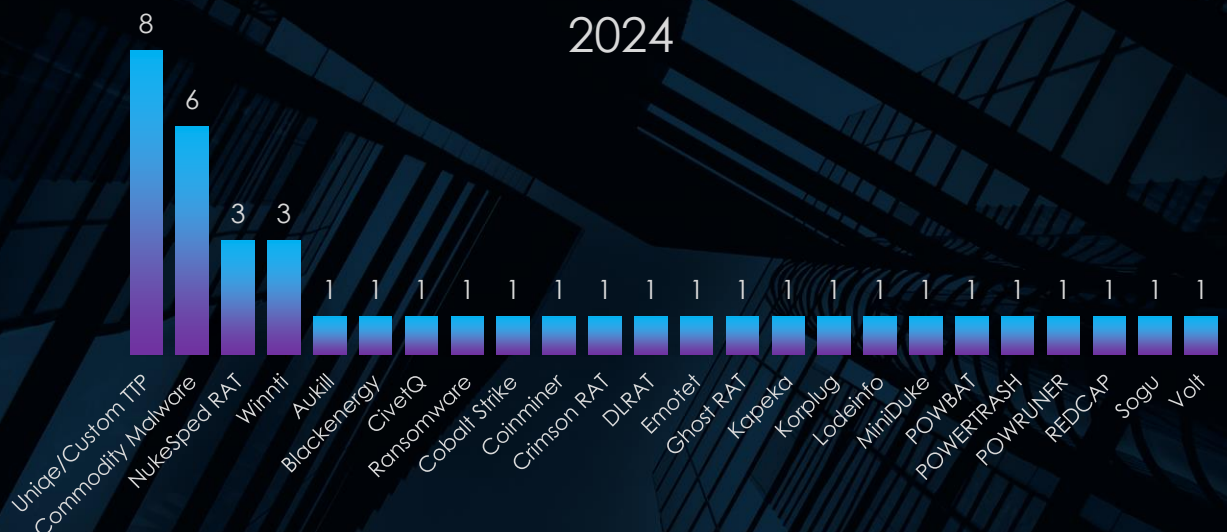
Data of geographical distribution reveals evolving global patterns, with the number of affected countries slightly decreasing from 32 to 31 in 2024. Despite this minimal change, the distribution and intensity of incidents shifted significantly, marked by notable turnover. Seven countries not targeted in 2023 experienced attacks in 2024, while eight previously affected countries saw no new campaigns in our telemetry.

Regions like East and Southeast Asia—including Taiwan, Thailand, Indonesia, Malaysia, Singapore, and Vietnam—experienced heightened activity, reflecting a growing regional focus potentially linked to expanding digital infrastructure and geopolitical factors. At the same time, traditionally high-profile targets such as Canada and New Zealand saw sharp declines in incidents, likely due to changes in adversary priorities or improved defensive measures.

The United Kingdom, Ukraine, Saudi Arabia, and Israel recorded significant increases in attack campaigns, in line with the evolving geopolitical landscape in the respective regions.

TOP MALWARE USED



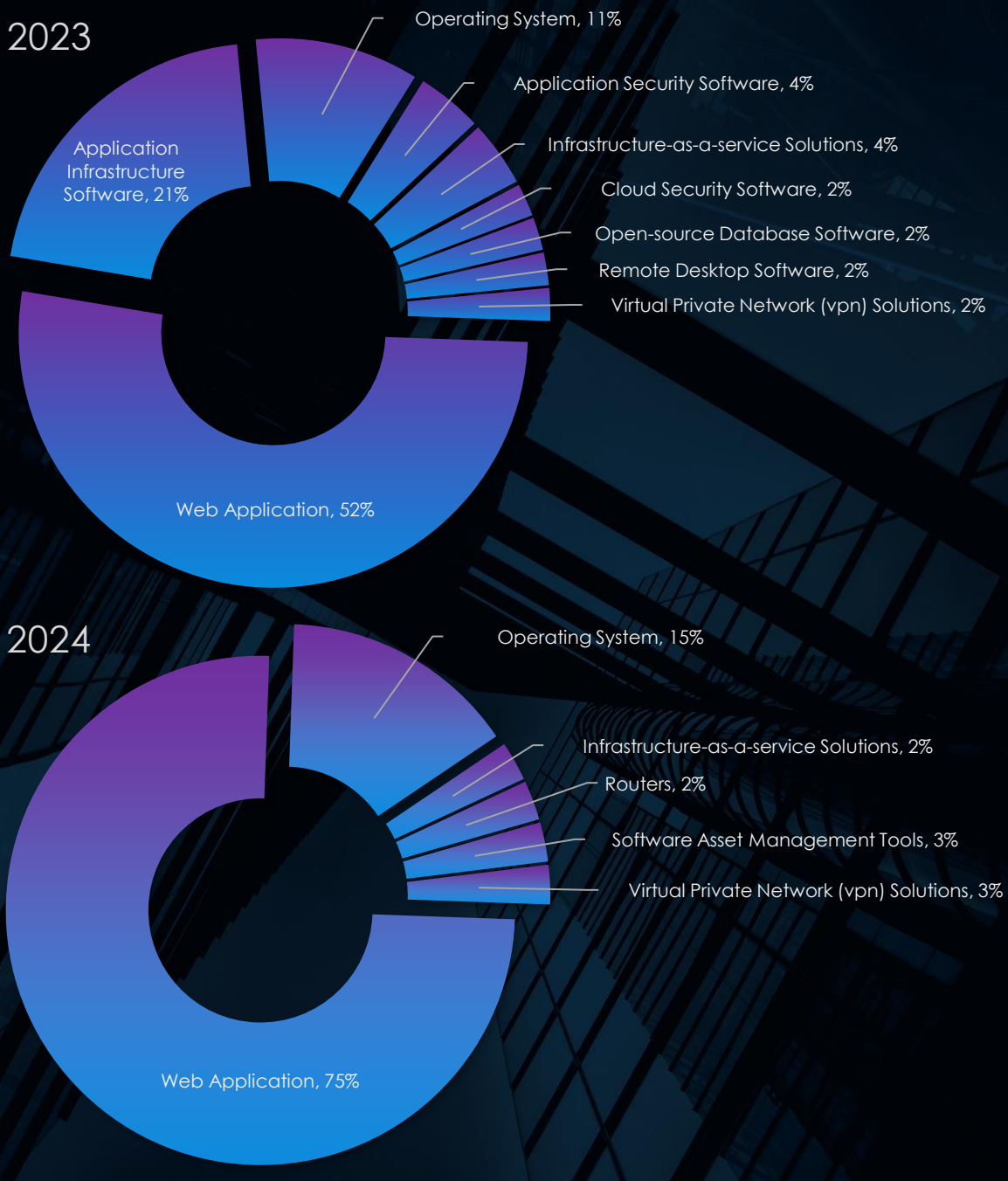


In both 2023 and 2024, the top observed malware strongly correlates with the activities of suspected threat actors. For example, Winnti and PlugX were predominantly linked to MISSION2025, while NukeSped RAT and Tofsee were associated with the Lazarus Group. Meanwhile, Emotet and various ransomware strains continued to be leveraged by Russian cybercrime syndicates. Notably, Cobalt Strike remained a ubiquitous tool across actor types, valued for its effectiveness and the plausible deniability it affords.

Focusing on 2024, there was a clear growth in the use of both custom TTPs and commodity malware. This trend aligns with the diversification of the threat landscape, characterized by increasing sophistication and widespread adoption of commodity tools. The shift reflects the dual emphasis on innovation and accessibility within adversary operations.

A comparison of 2023 and 2024 highlights a notable reduction in the variety of unique malware families, accompanied by a sharp increase in the volume of both custom TTPs and custom malware. The respective share of these categories grew significantly, rising from 7% in 2023 to 35% in 2024. This underscores a strategic pivot by threat actors toward more tailored and impactful attack methodologies.

TOP ATTACKED TECHNOLOGY



In 2024, the increased reliance on commodity tools and malware was accompanied by a noticeable trend toward more unified attack techniques targeting specific technologies.

Web applications remain the most frequently targeted technology, primarily due to their inherently internet-facing nature, which exposes them to a wider array of threats.

Additionally, remote access tools continued to serve as a common attack vector. However, attackers typically use stolen credentials to gain direct access, rather than exploiting vulnerabilities within the tools themselves.

APT CAMPAIGNS EXTERNAL THREAT LANDSCAPE MANAGEMENT (ETLM) OVERVIEW

Year-to-Year Elevation: Moderate

The year-to-year elevation in APT campaign activity from 2023 to 2024 was moderate but marked by significant shifts in focus and methodology. The total number of campaigns rose from 27 to 31, reflecting a 14.8% increase. This modest growth was accompanied by a 40% surge in the number of observed threat actors, rising from 15 to 25, signaling a broader diversification of adversarial players.

Geopolitical factors strongly influenced the external threat landscape. East and Southeast Asia—particularly Taiwan, Thailand, Indonesia, Malaysia, Singapore, and Vietnam—emerged as hotspots of heightened activity. Meanwhile, traditionally high-profile targets such as Canada and New Zealand experienced sharp declines, likely due to shifts in adversary priorities or strengthened defenses. Politically significant regions, including the United Kingdom, Ukraine, Saudi Arabia, and Israel, faced notable increases, underscoring their strategic importance amid rising global tensions.

Industrially, the threat landscape shifted. In 2024, Information Technology, Finance, and Manufacturing became the most targeted sectors, replacing Consumer Goods & Services and Telecommunications. Information Technology attacks saw a dramatic 108% rise, while Finance increased by 28.6%. Conversely, Materials, Automotive, Logistics, and Real Estate experienced significant declines in attack frequency, with nine out of 13 industry categories recording fewer campaigns overall. This suggests that threat actors are realigning their focus toward higher-value and geopolitically strategic targets.

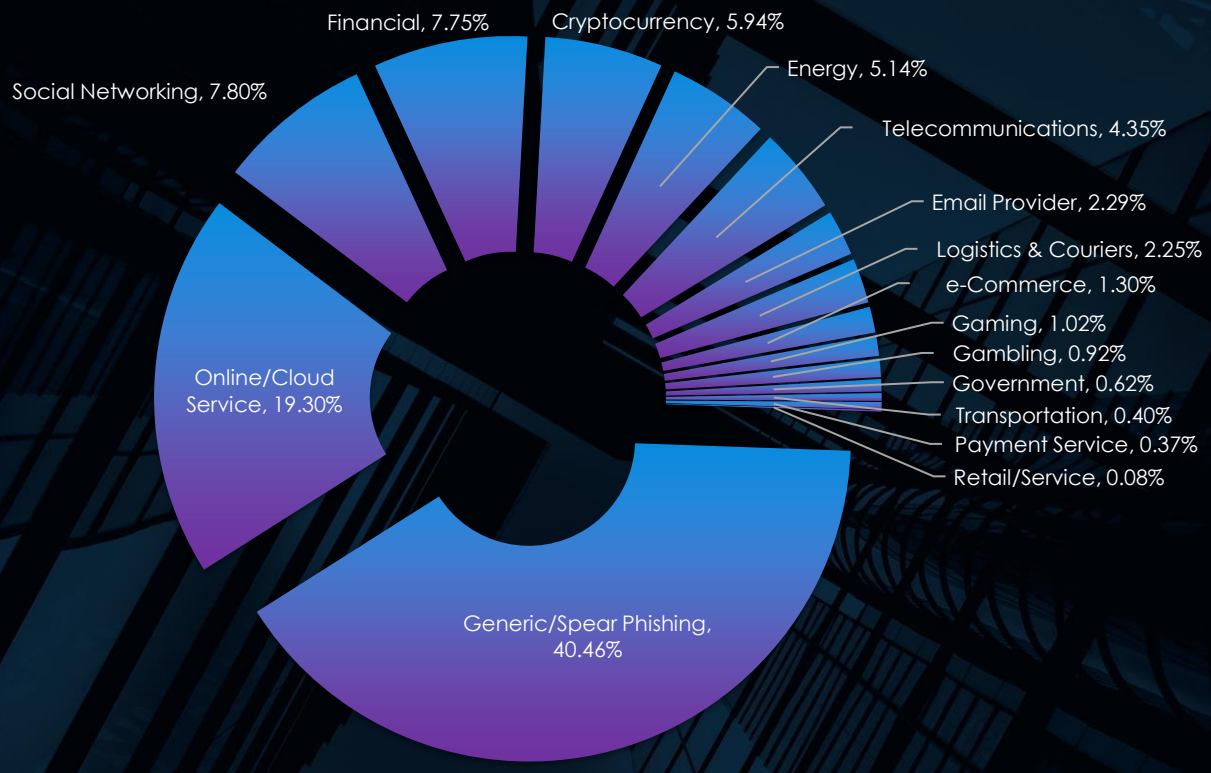
In terms of methodologies, 2024 saw a surge in the use of custom TTPs and commodity malware, reflecting a dual emphasis on innovation and accessibility. Custom/unique and commodity malware's share rose from 7% in 2023 to 35%, highlighting a pivot toward more tailored and impactful attack strategies. Cobalt Strike remained a tool of choice across multiple actor types, valued for its efficiency and plausible deniability. Furthermore, attackers increasingly relied on stolen credentials for direct access to remote systems, bypassing traditional vulnerability exploitation.

Despite the moderate rise in overall campaigns, the external threat landscape became more diverse and sophisticated. These developments underscore the importance of adaptive ETLM strategies to address evolving threats, focusing on region-specific vulnerabilities, sector-based targeting trends, and the increasing use of advanced adversarial techniques.

PHISHING DATA ANALYSIS

Over the past year, CYFIRMA's telemetry recorded 1,046,569 phishing campaigns. This is just a sample of all phishing in the world; however, it provides insight into trends such as phishing themes, impersonated brands, and the largest sources of phishing.

DISTRIBUTION OF THEMES PER SECTOR



Phishing themes in the captured sample reveal significant focus areas for attackers. Generic and spear phishing dominate, accounting for the largest share, highlighting the vast number of small and unique scams and phishing spams.

Online and cloud services, along with social networking, represent key targets due to their central role in digital interactions.

Financial and cryptocurrency themes remain prominent, reflecting attackers' interest in direct monetary exploitation.

Critical sectors like energy and telecommunications also face notable targeting, but do not offer the same direct monetization.

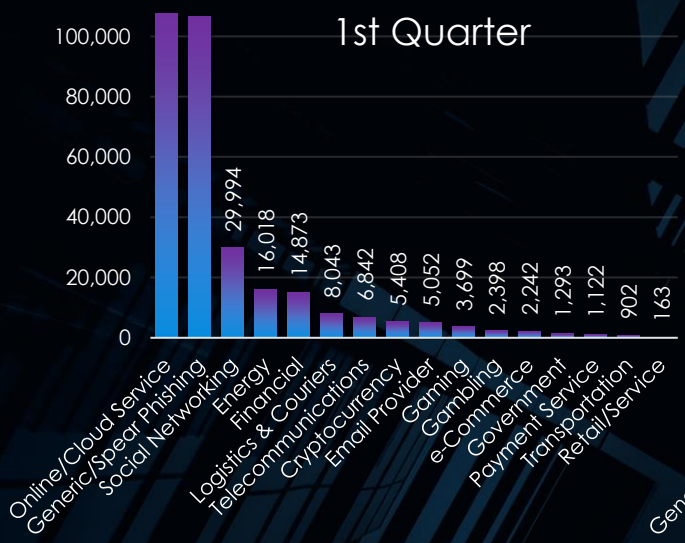
Meanwhile, lower-volume themes such as logistics, gaming, and government indicate region-specific but still impactful focus areas within the threat landscape.

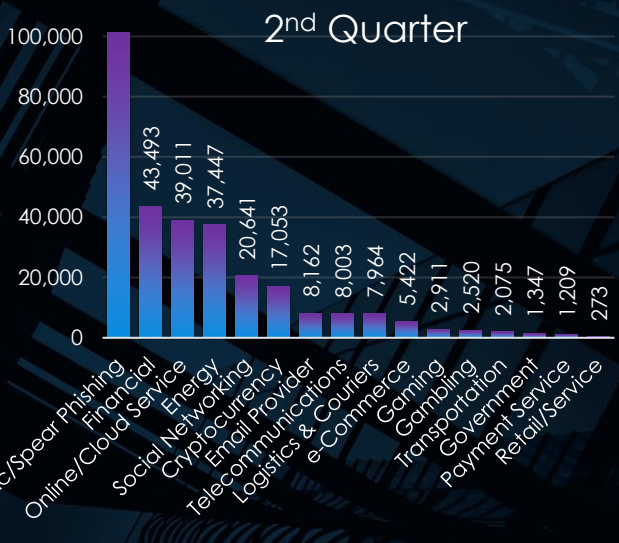
CYFIRMA
DECODING THREATS

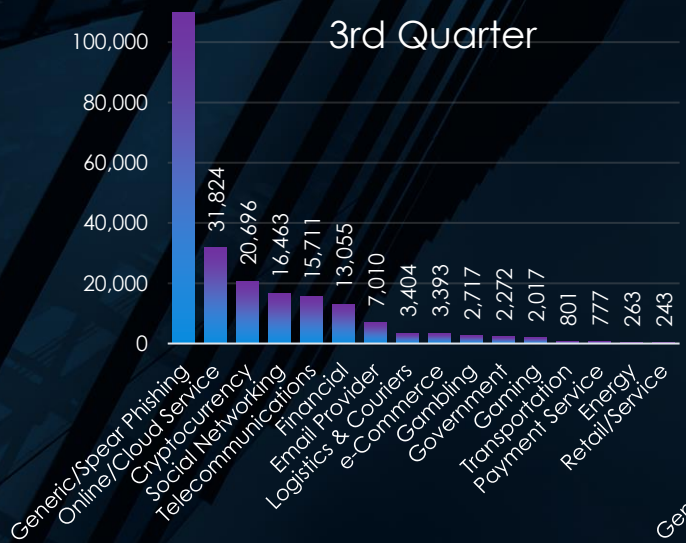
DISTRIBUTION OF THEMES PER SECTOR PER QUARTER

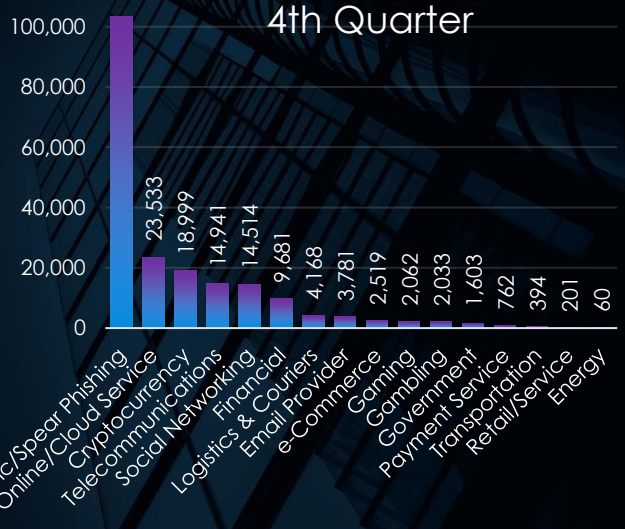
Analyzing phishing themes quarterly reveals evolving trends throughout 2024.

For instance, the year began with a significant surge in energy-themed phishing, driven by a large-scale Gazprom impersonation campaign. However, this theme almost entirely disappeared by the third and fourth quarters, reflecting the conclusion of the campaign and a shift in adversary focus.









CYFIRMA
DECODING THREATS

TOP IMPERSONATED BRANDS IN 2024

Despite being active only during the first two quarters of the year, **Gazprom** emerged as the third most impersonated brand, reflecting the scale and impact of the early-year phishing campaign leveraging its identity. This aligns with the significant energy-themed phishing observed in Q1 and Q2.

Office 365 secured the top spot with more than double the count of the second most impersonated theme, showcasing its continued popularity among attackers. Its widespread use across industries makes it a prime target for delivering social engineering lures, including highly tailored spear-phishing campaigns aimed at accessing corporate environments.

Cryptocurrency and wallet-related brands, in second place, saw extensive exploitation, likely driven by the early-year surge in cryptocurrency valuations to all-time highs. These campaigns provide attackers with straightforward opportunities for financial gain through phishing targeting users of digital wallets and exchanges.

Regional banks such as Credit Agricole, Societe Generale, Bancolombia, and DBS Bank also feature prominently in the list, highlighting attackers' interest in localized financial institutions. This trend suggests that phishing campaigns are increasingly tailored to regional markets, aiming to exploit users' trust in familiar, geographically relevant brands.

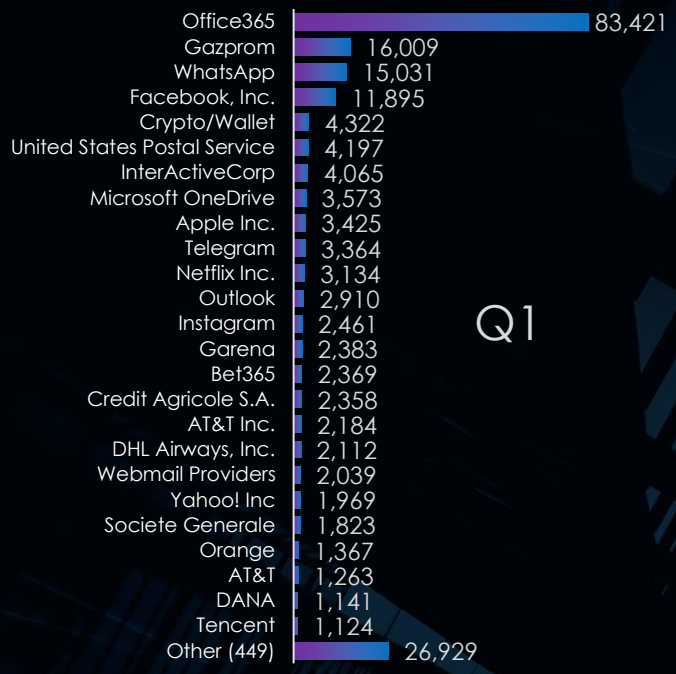
Gaming platforms like Steam, Garena, and Tencent are gaining traction as phishing targets, underscoring the growing appeal of digital gaming communities. The high volume of user engagement and financial transactions within these platforms makes them attractive for credential theft and fraud.

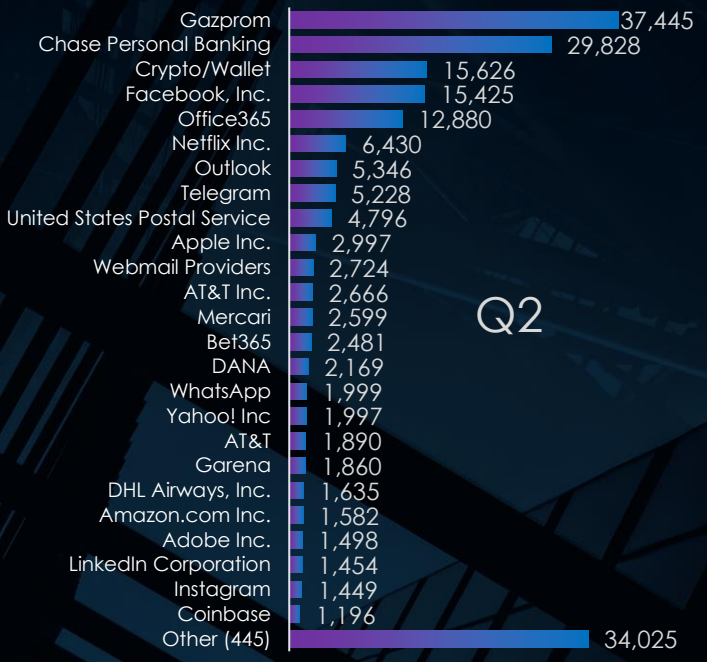
Other notable impersonation targets include Facebook, Telegram, and Netflix, which highlight the persistent focus on **platforms with massive global user bases**. Additionally, brands like Amazon, AT&T, and DHL point to phishing campaigns **leveraging trusted names** to deceive victims.

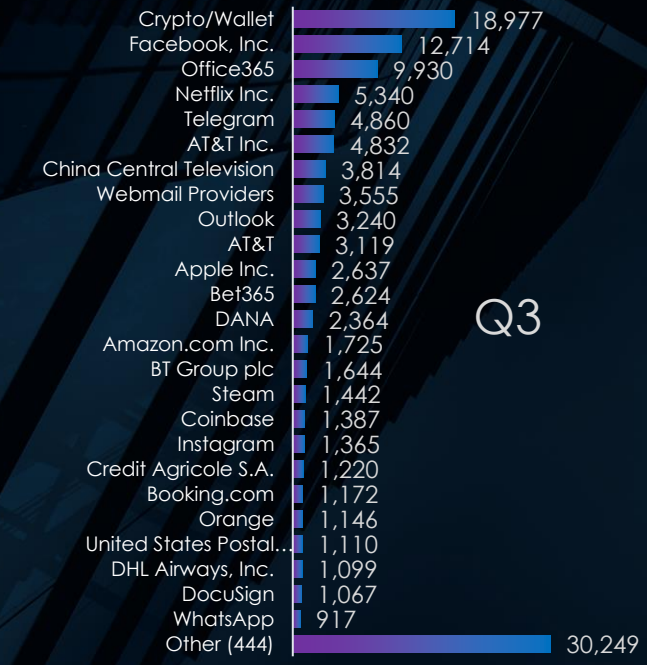
The data demonstrates how attackers strategically select brands based on global trends, regional relevance, and user trust to maximize the success of their campaigns, revealing a diverse and evolving phishing landscape.

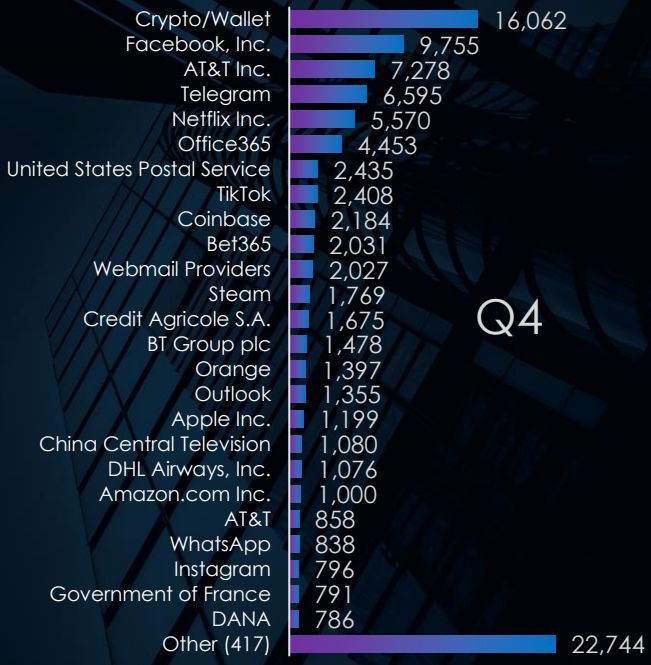
CYFIRMA
DECODING THREATS

TOP IMPERSONATED BRANDS IN 2024







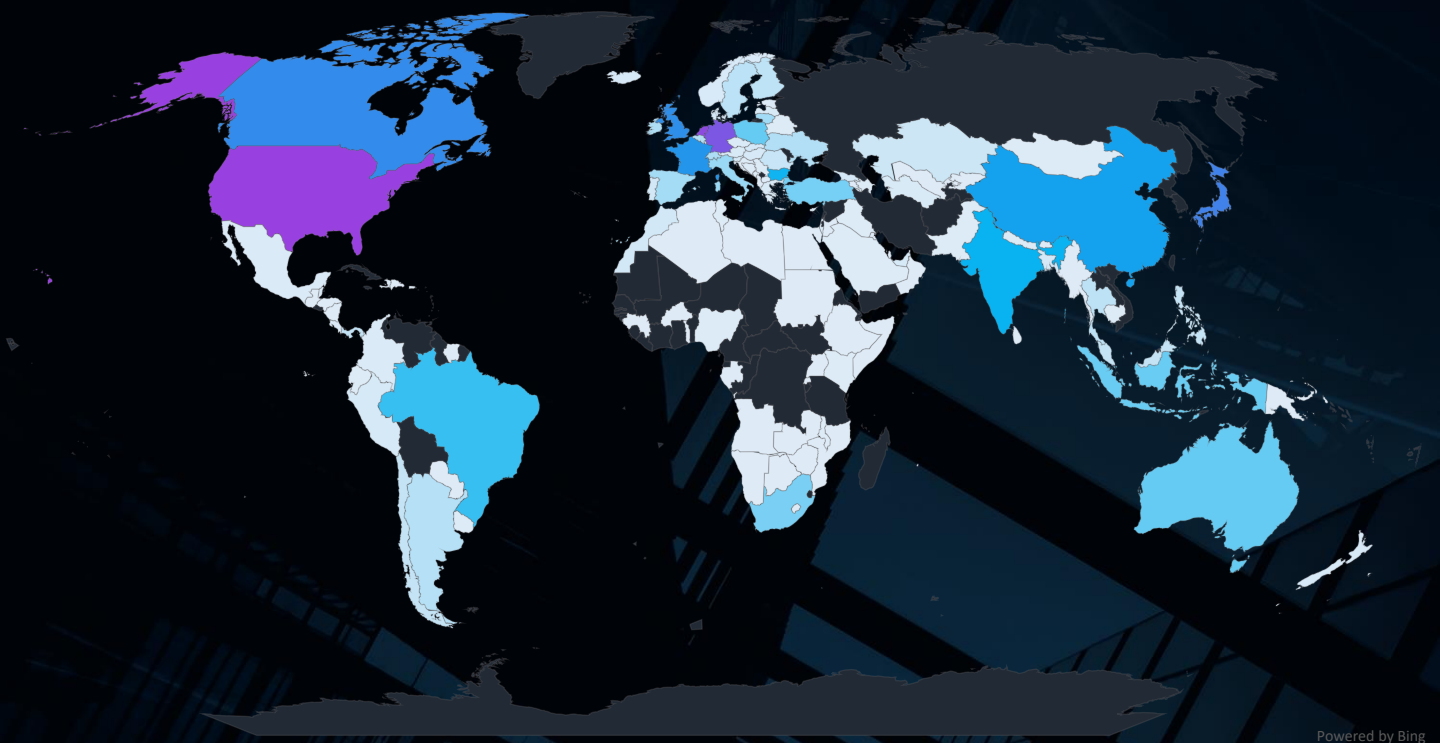


A quarterly breakdown further highlights shifting trends, as for example seen with Gazprom and cryptocurrency-related themes.

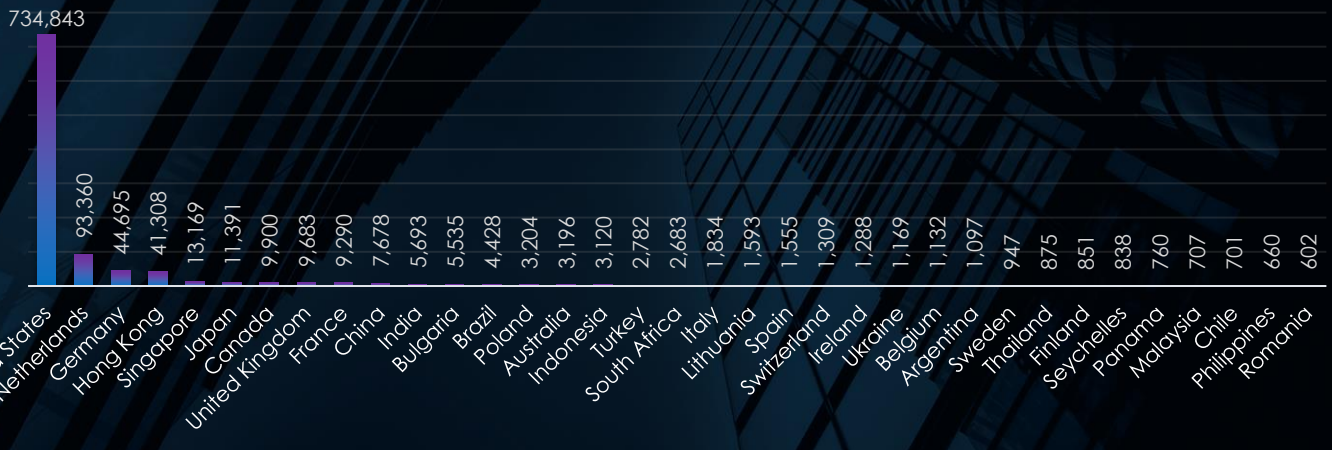
As the Gazprom campaign faded after the second quarter and cryptocurrency values surged, phishing campaigns targeting crypto wallets and exchanges surged, propelling cryptocurrency-related themes to the top spot in the third and fourth quarters.

CYFIRMA
DECODING THREATS

COUNTRIES OF ORIGIN (by ASN)



The global heatmap highlights the widespread reach of cybercrime and the diverse sources of phishing activity worldwide. Notably, Russia is excluded from the data due to widespread blacklisting by filters, effectively deleting its visibility as a source of phishing in our captured samples.



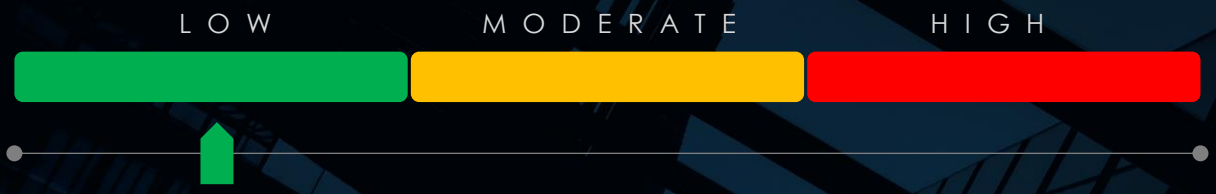
The United States ranks first in both phishing targeting and as a source of phishing activity. Historically, it has hosted the largest number of compromised devices, which are frequently incorporated into extensive botnet networks. These networks serve as proxies for distributing large-scale phishing campaigns, further solidifying the U.S.'s prominent role in the phishing landscape.

In Europe, the Netherlands and Germany hold similar positions, serving as significant hubs for phishing activity. Hong Kong and Singapore are often exploited as proxy locations by Chinese threat actors, reflecting their strategic importance in regional cyber operations.

CYFIRMA
DECODING THREATS

PHISHING EXTERNAL THREAT LANDSCAPE MANAGEMENT (ETLM) OVERVIEW

Throughout the year Elevation: Low



CYFIRMA's telemetry recorded over 1 million phishing campaigns in the past year, offering valuable insights into attacker trends, including key themes, impersonated brands, and the largest sources of phishing activity.

Generic and spear phishing continued to dominate, emphasizing the vast number of smaller and unique phishing spams. Online and cloud services, along with social networking platforms, remained primary targets due to their central role in digital interactions. Financial and cryptocurrency themes also featured prominently, reflecting attackers' focus on direct monetary exploitation, while sectors like energy and telecommunications faced moderate targeting, offering less immediate monetization opportunities.

Quarterly trends revealed significant shifts. Early 2024 saw a surge in energy-themed phishing, largely driven by a Gazprom impersonation campaign. However, this theme faded by mid-year, giving way to cryptocurrency-related campaigns as cryptocurrency values surged, propelling these themes to the forefront in Q3 and Q4.

Office 365 ranked as the most impersonated brand, highlighting its widespread use and value for delivering social engineering lures. Cryptocurrency wallets and exchanges claimed the second spot, reflecting their attractiveness as lucrative phishing targets during periods of high market activity. Gazprom emerged as the third most impersonated brand despite its activity being limited to the first half of the year, demonstrating the significant impact of its associated campaign.

Regional banks such as Credit Agricole, Societe Generale, Bancolombia, and DBS Bank were frequently targeted, suggesting an increasing focus on localized campaigns exploiting geographic familiarity and trust. Gaming platforms like Steam, Garena, and Tencent also saw growing targeting, reflecting attackers' interest in gaming communities with high engagement and financial transactions.

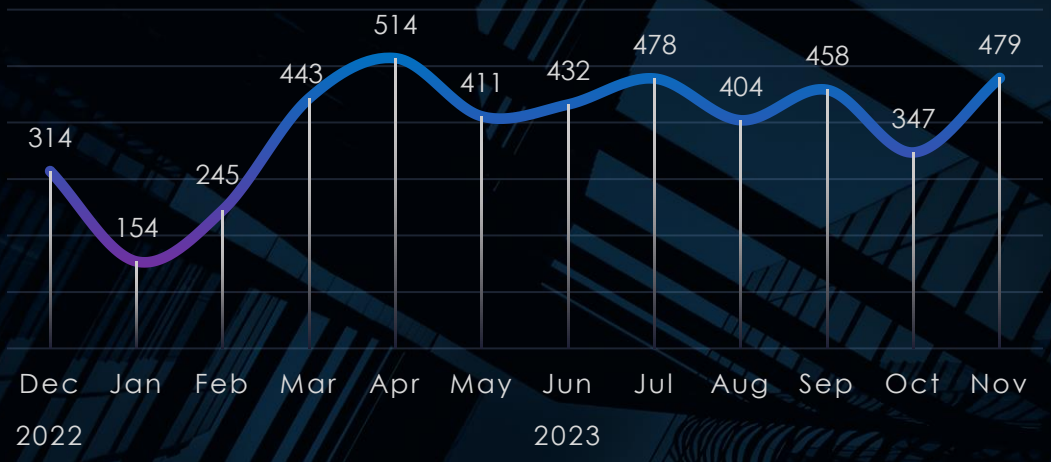
The United States leads as both the largest source and target of phishing, driven by its large population of compromised devices that feed global botnet operations. In Europe, the Netherlands and Germany serve as significant hubs for phishing activity, while in Asia, Hong Kong and Singapore are frequently exploited as proxy locations for Chinese threat actors, emphasizing their strategic regional roles.

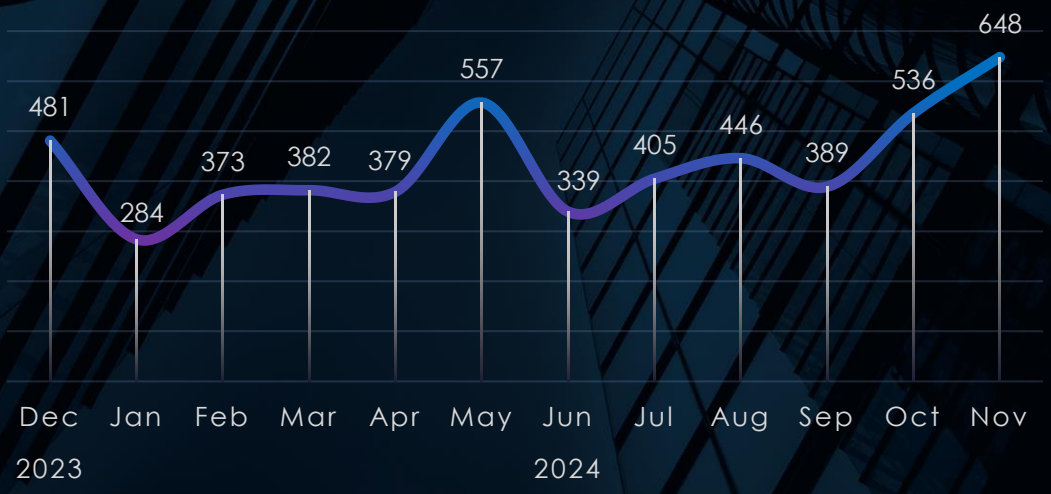
CYFIRMA
DECODING THREATS

RANSOMWARE VICTIMOLOGY

In 2023, CYFIRMA recorded 4,679 verified ransomware victims, while in 2024, the number increased to 5,219, representing a 11.5% year-over-year growth across all industries.

THE MONTHLY ACTIVITY CHARTS



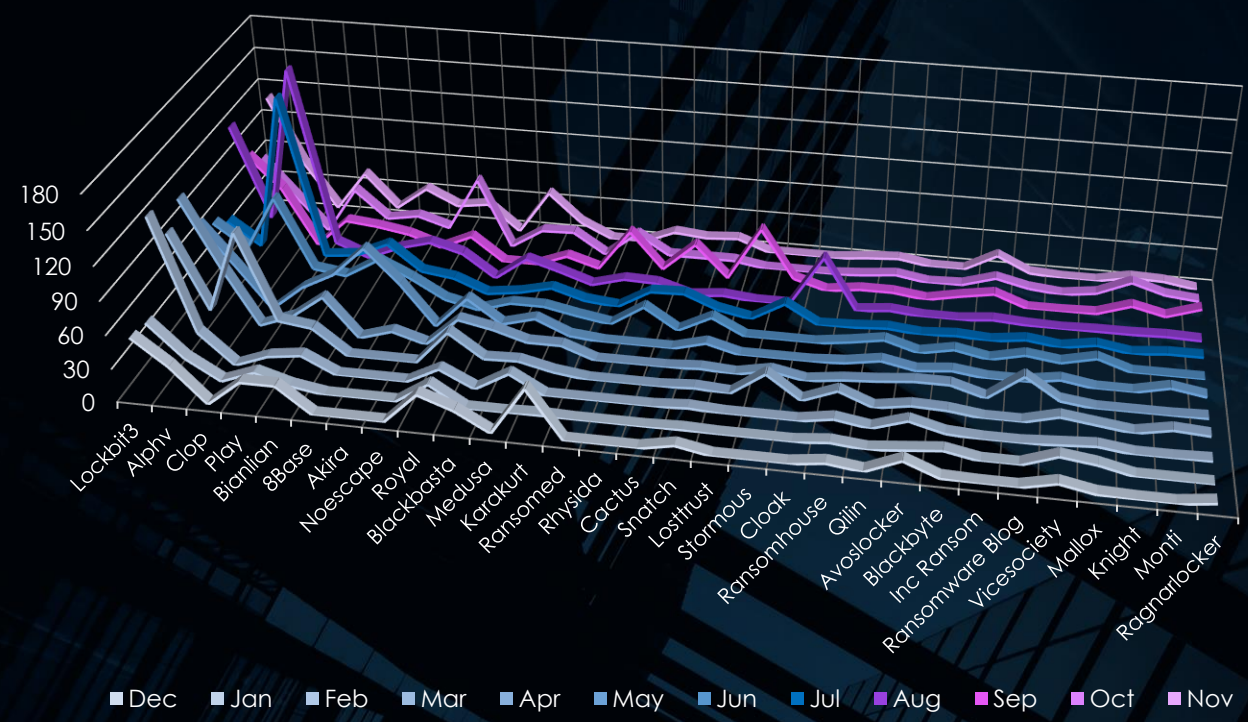


In early 2023, the takedown of Hive caused a temporary slowdown in ransomware activity. However, this was followed by a surge driven by Cl0p, leveraging the MOVEit vulnerability.

Similarly, the early 2024 slowdown caused by the Lockbit3 takedown was short-lived, as affiliates switched to other Ransomware-as-a-Service (RaaS) and Ransomhub quickly emerged to fill the void in the RaaS ecosystem.

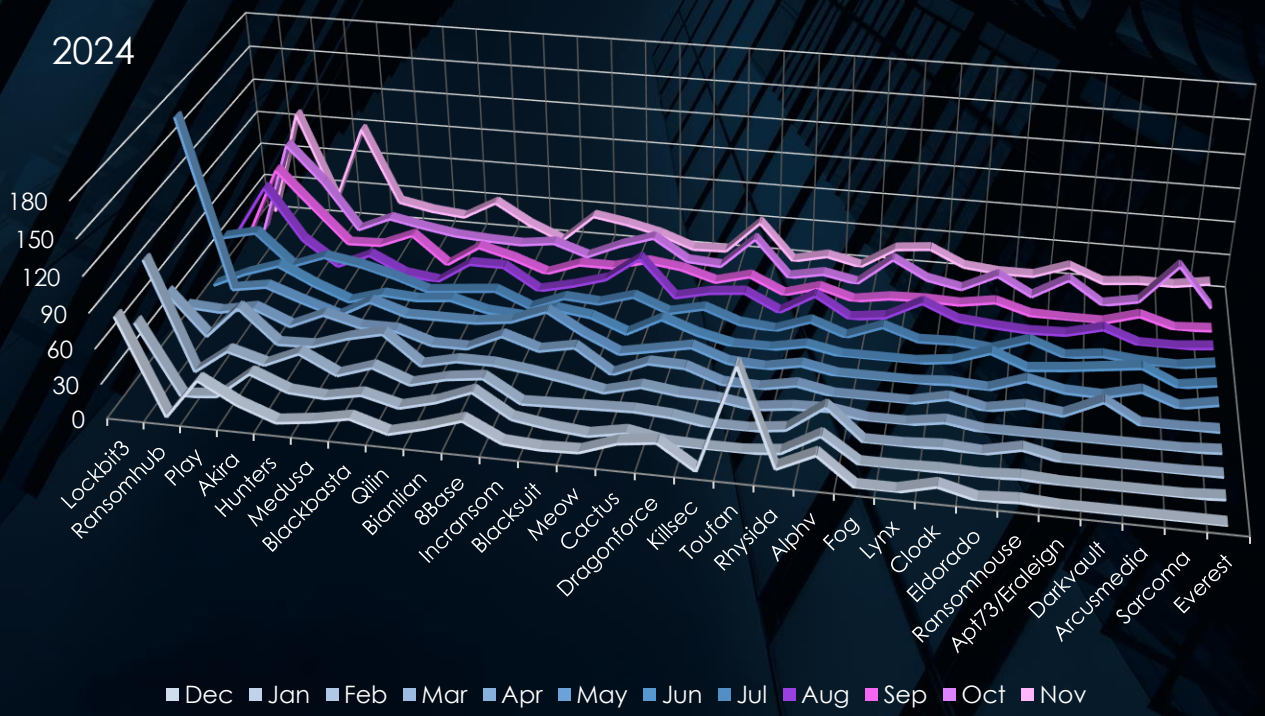
CYFIRMA
DECODING THREATS

MONTHLY ACTIVITY BREAKDOWN BY GANG



These charts illustrate the monthly activity of the top 30 ransomware gangs for each year, organized by overall activity from left to right on the X-axis. Lockbit3 consistently had the highest number of victims in both years but showed a decline in activity later in 2024.

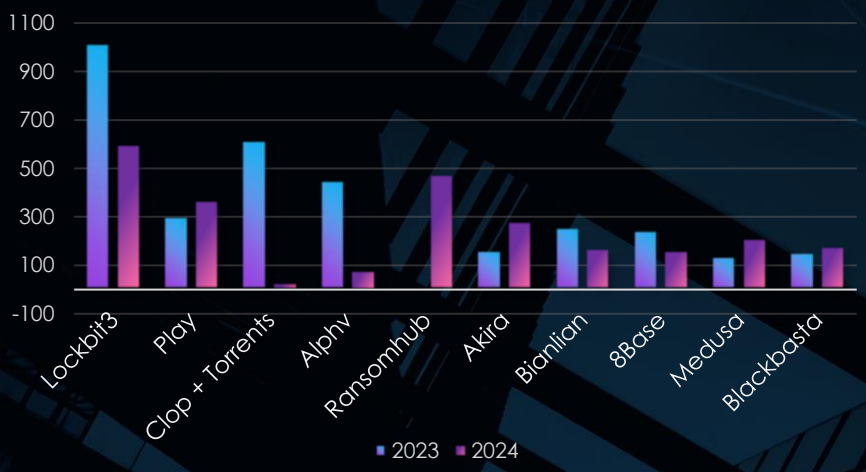
The Toufan gang recorded a spike in activity during December 2023 before disappearing entirely for the remainder of the following year.



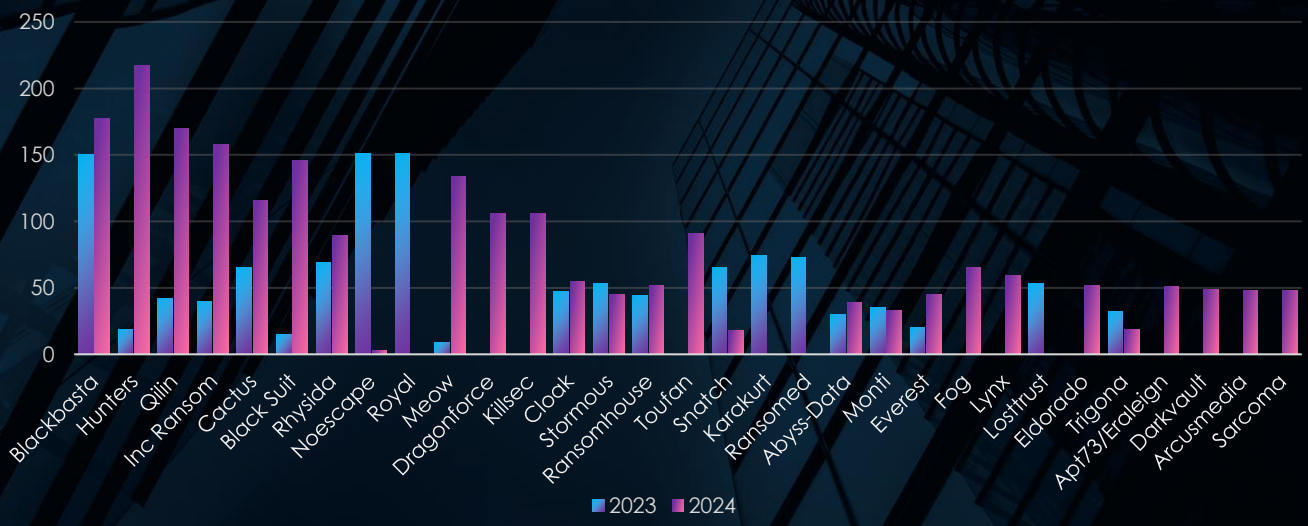
CYFIRMA
DECODING THREATS

RANSOMWARE VICTIMS PER GANG

In 2023, 67 ransomware groups were active, growing to 97 in 2024. This increase was partly driven by rebranding and splintering of existing groups from 2023, as well as a global surge in ransomware activity, particularly in regions like South Asia and Southeast Asia.



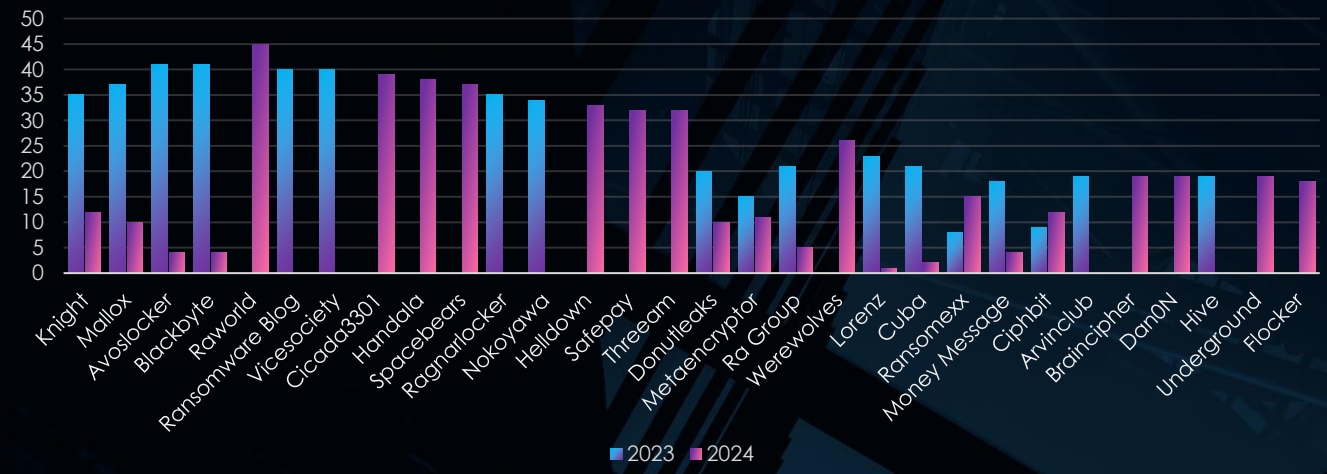
The chart above displays the top 10 ransomware groups with the highest victim counts across 2023 and 2024. Notably, Cl0p recorded significant activity exclusively in 2023. ALPHV's infrastructure was dismantled by law enforcement in early 2024, while Ransomhub emerged to fill the void left by the Lockbit3 takedown later that year.



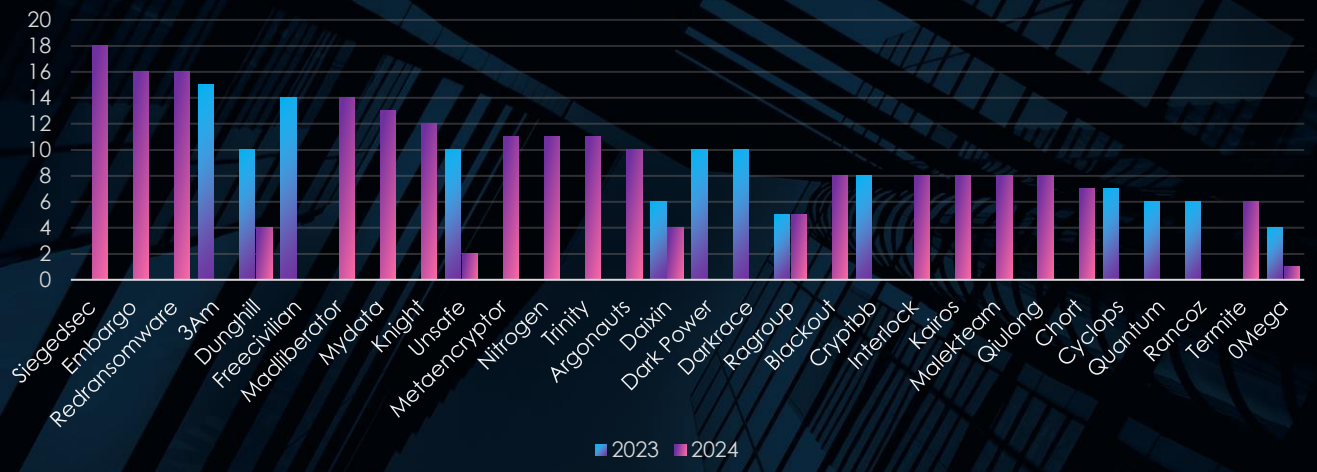
The chart above highlights ransomware groups ranked 11th to 40th, sorted by total victim count across 2023 and 2024. Most high-count groups are emerging players from 2024, with exceptions like Noescape and Royal, which were active in 2023.

Additionally, Blackbasta demonstrated resilience, remaining active and maintaining strong operations throughout both years, particularly in 2024.

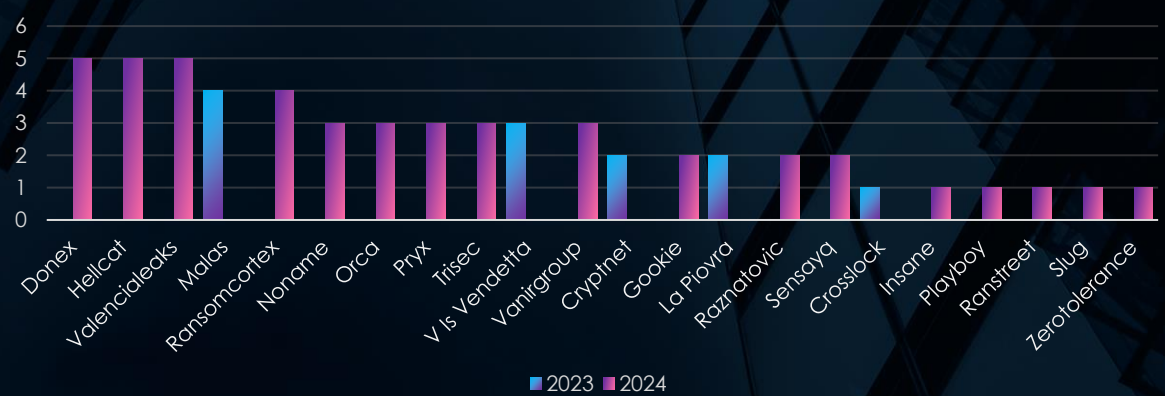
RANSOMWARE VICTIMS PER GANG



The chart above features ransomware groups ranked 41st to 70th. This segment includes some of the most active groups from 2023, indirectly reflecting the surge in activity during 2024. The emergence and intensified operations of 2024 groups, as shown in the previous chart, pushed many of their 2023 counterparts further down the rankings.

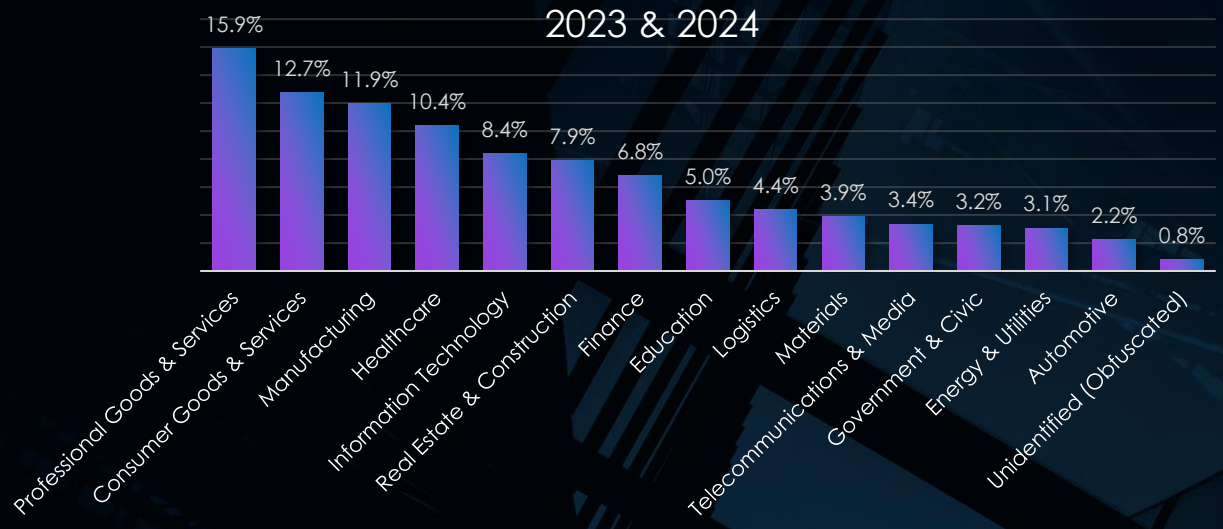


The charts above and below represent ransomware groups ranked 71st to 100th and 101st to 122nd, respectively. A notable observation is the high number of groups in 2024 that recorded only a small number of victims, reflecting the emerging or less prolific groups.

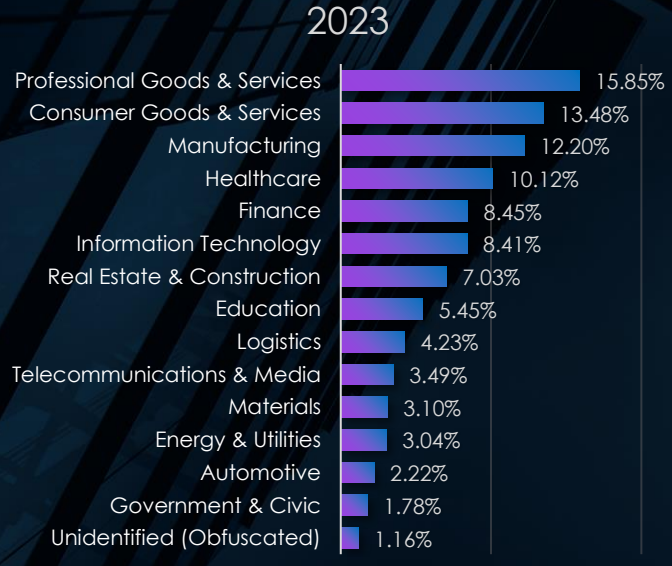


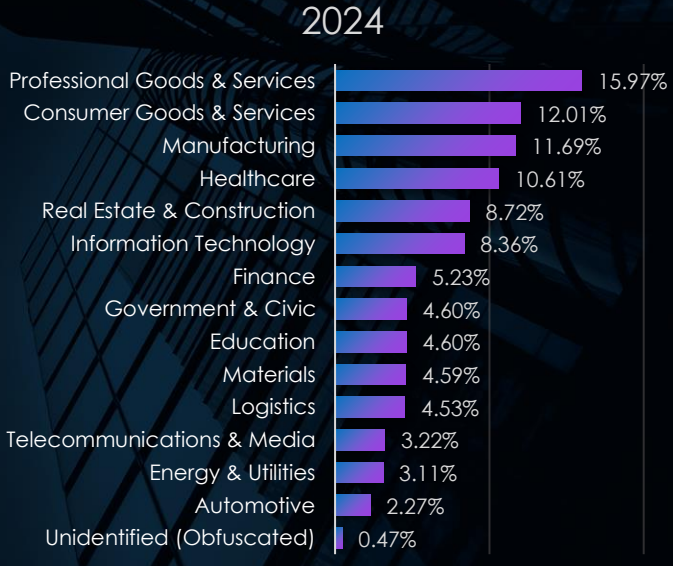
CYFIRMA
DECODING THREATS

RANSOMWARE VICTIMS PER INDUSTRY



Over the past two years, Professional Goods & Services remained the most frequently targeted industry, consistently maintaining its top position with nearly 16% of all attacks. Consumer Goods & Services and Manufacturing followed closely, reflecting many smaller business attacked. Meanwhile, Real Estate & Construction saw notable growth, climbing from 7.03% in 2023 to 8.72% in 2024, advancing two spots in the rankings.



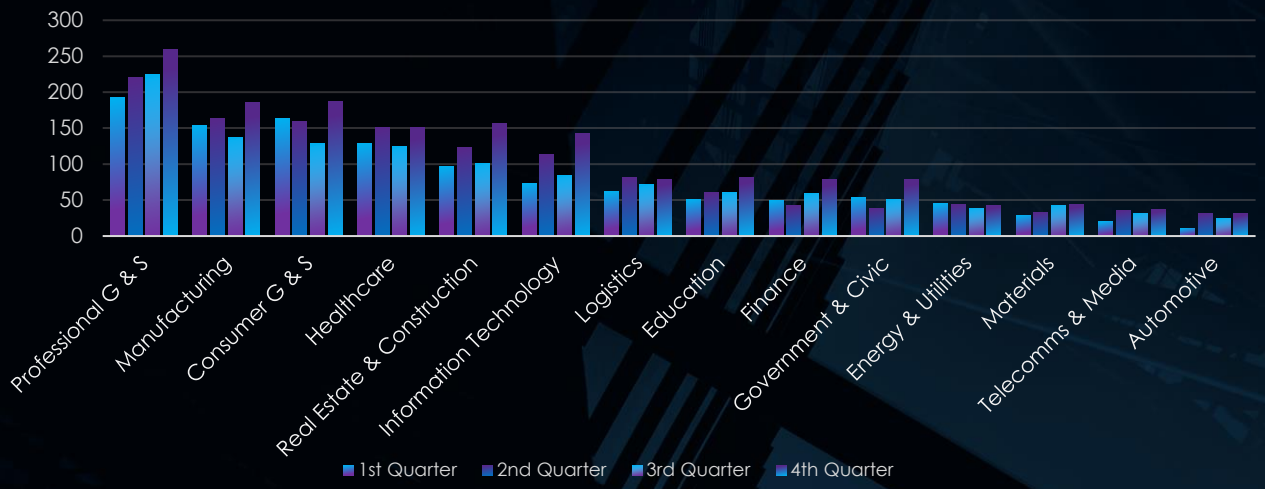


In contrast, Finance experienced a significant decline, dropping from 8.45% in 2023 to 5.23% in 2024, possibly due to improved defenses or shifts in attacker priorities. Other sectors, such as Education and Government & Civic, gained traction in 2024, both accounting for 4.60% of attacks.

The data highlights evolving trends, with attackers diversifying their targets. While sectors like Healthcare, Manufacturing, and Professional Goods & Services remain consistently attractive, other industries such as Logistics, Telecommunications, and Materials are gaining moderately more attention, reflecting strategic adjustments in threat actor operations.

CYFIRMA
DECODING THREATS

RANSOMWARE VICTIMS PER INDUSTRY

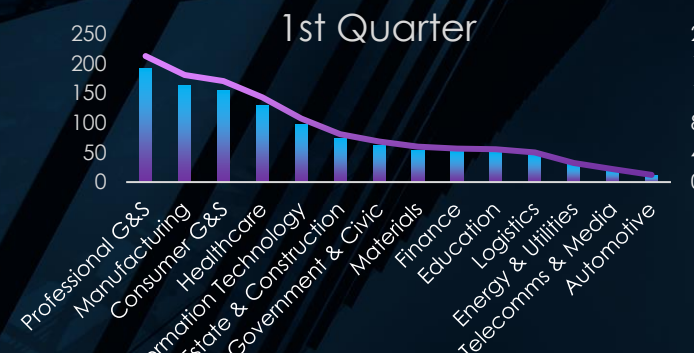


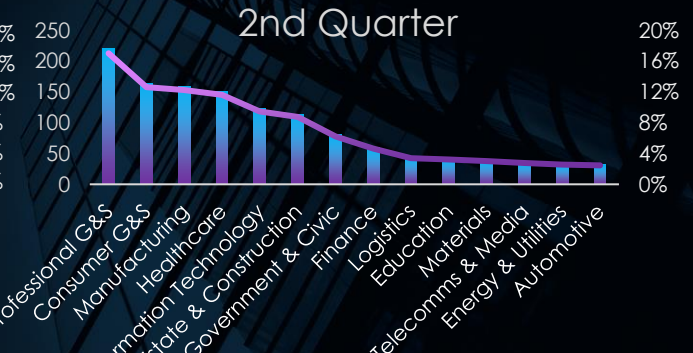
Throughout 2024, Professional Goods & Services led as the most targeted sector, with steady quarterly growth and a peak of 260 incidents in Q4. Similarly, Manufacturing and Consumer Goods & Services remained prominent, showing a rebound in Q4 following a mid-year dip.

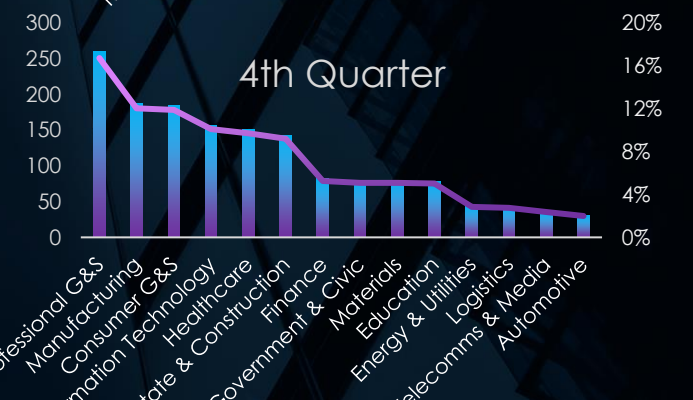
Real Estate & Construction recorded significant growth, increasing from 97 incidents in Q1 to 157 in Q4. Likewise, Information Technology more than doubled its Q1 count, reaching 143 incidents in Q4.

Both Education and Government & Civic sectors saw sharp increases, particularly in Q4, where incidents nearly doubled.

Energy & Utilities, Materials, and Telecommunications & Media experienced relatively stable activity with modest increases in Q3 and Q4. Automotive also showed gradual growth, culminating in 31 incidents in Q4, reflecting steady interest from attackers.

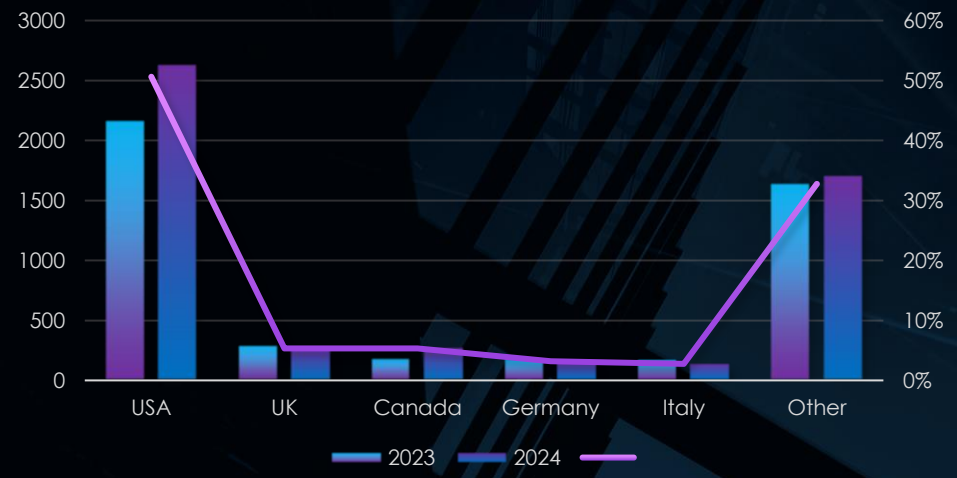




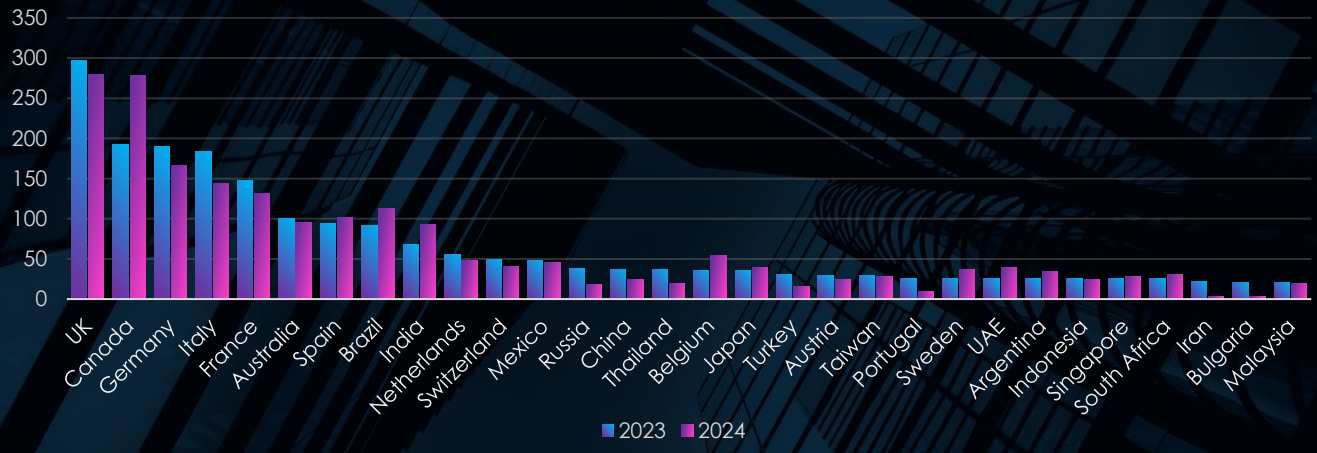


CYFIRMA
DECODING THREATS

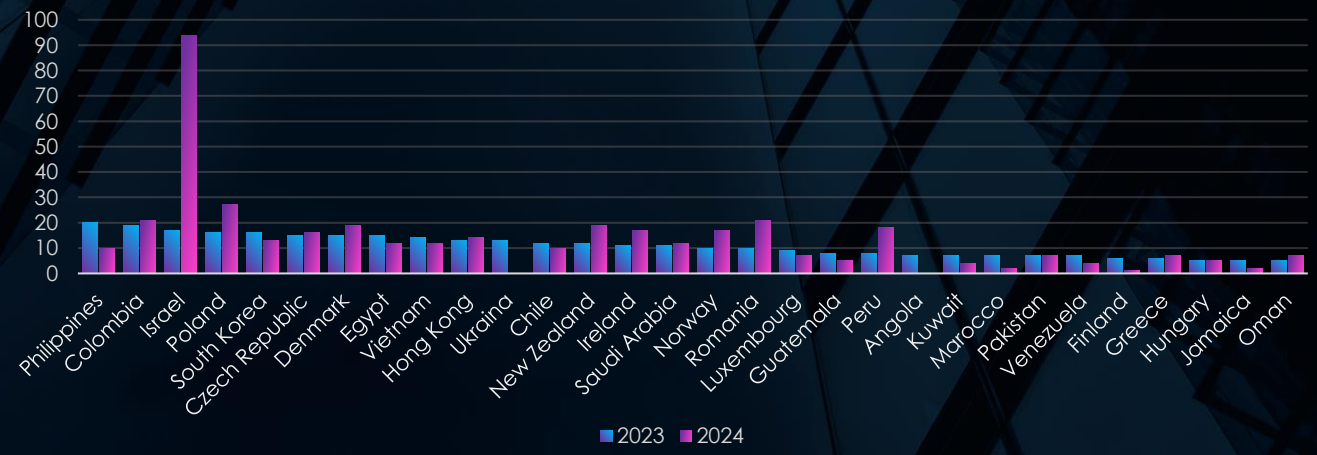
RANSOMWARE VICTIMS PER COUNTRY



The United States is the most frequent victim of ransomware by a significant margin, accounting for 46.3% and 50.6% of all victims in 2023 and 2024, respectively. Its dominance completely overshadows other countries in any visualization. The chart above displays the top five and all other countries combined for ransomware victims in 2023 and 2024.



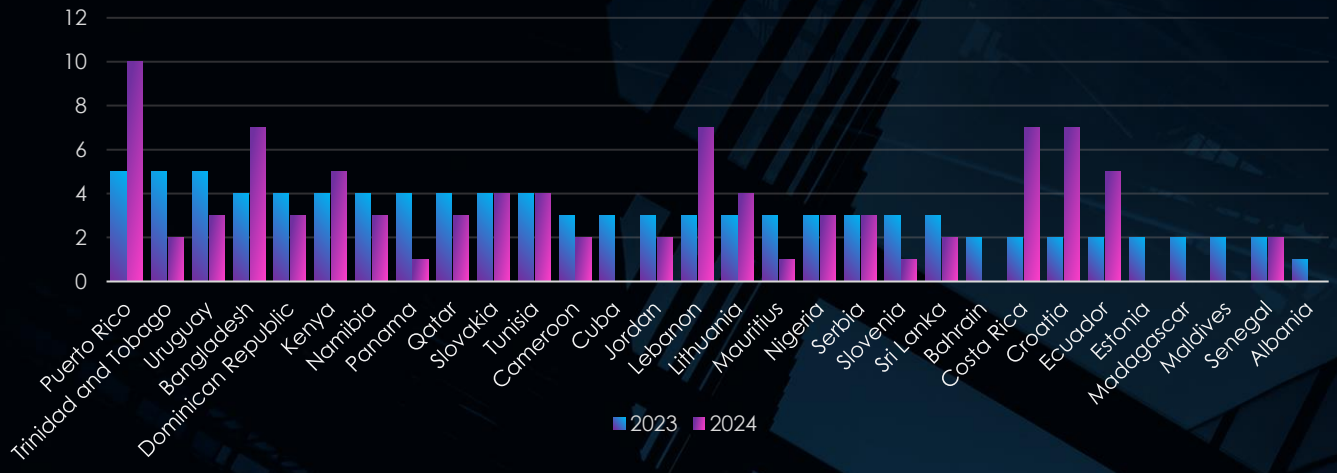
The charts above and below display the top 60 countries, sorted by the number of victims in 2023, along with their respective 2023-to-2024 change data. Some countries, such as Canada, Israel, and India, recorded significant increases in ransomware activity during 2024, while others, like Italy and Thailand, experienced declines.

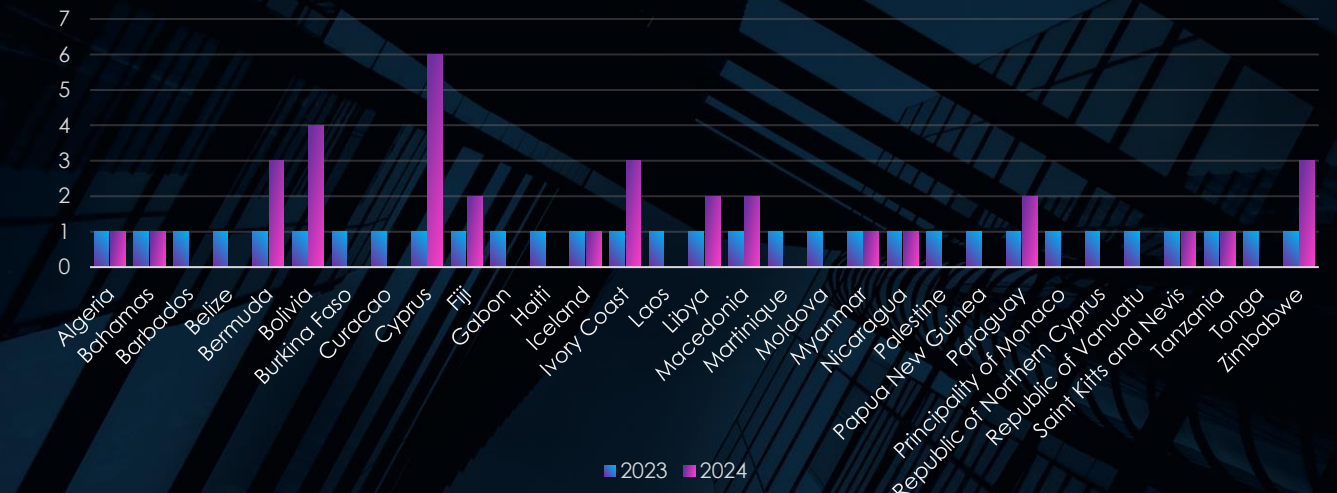


CYFIRMA
DECODING THREATS

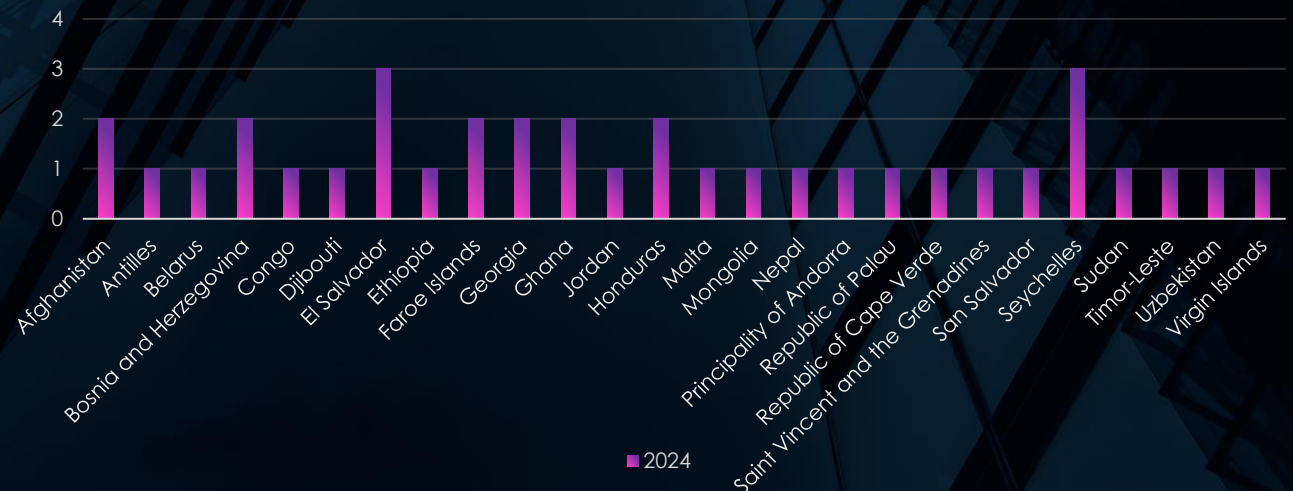
RANSOMWARE VICTIMS PER COUNTRY

Continuation of 2023-to-2024 change data for every recorded country.





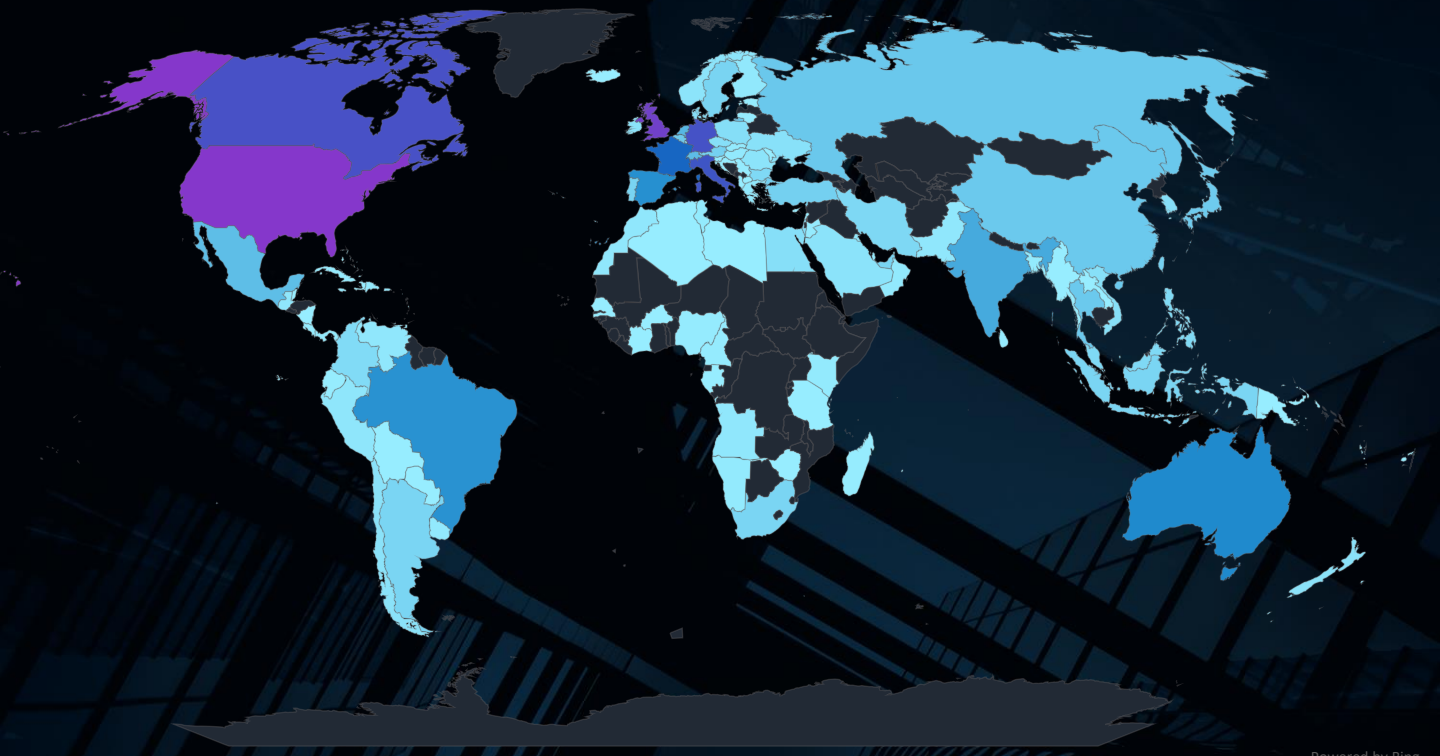
Finally, the last chart with new countries recording victims only in 2024.

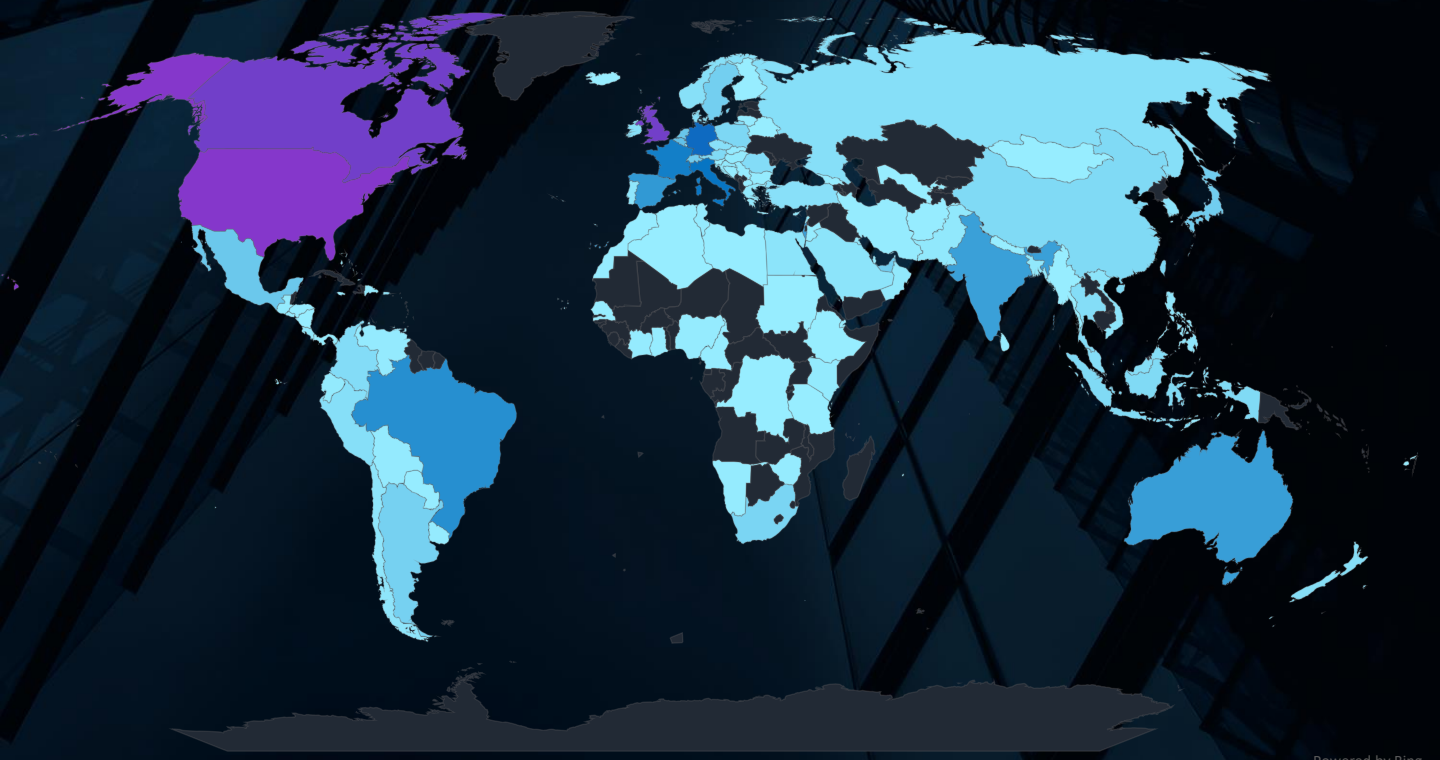


CYFIRMA
DECODING THREATS

RANSOMWARE VICTIMS PER COUNTRY

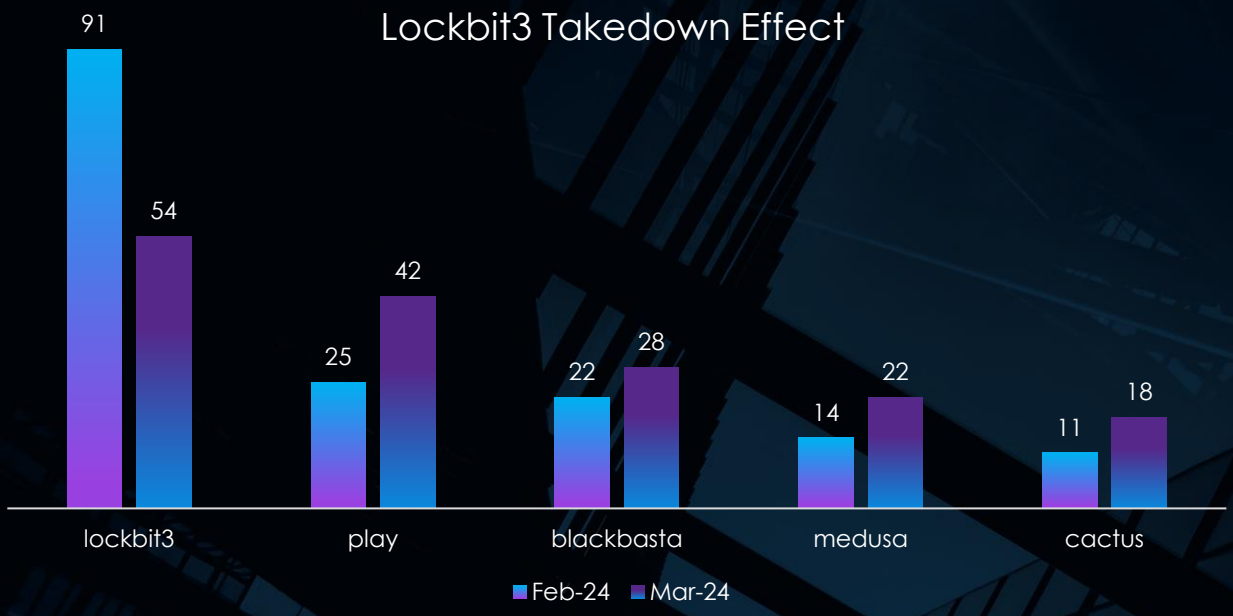
The heatmap of geographic distribution highlights the truly global reach of ransomware while visually illustrating the changes between 2023 and 2024.





CYFIRMA
DECODING THREATS

RANSOMWARE AFFILIATES



To gain a deeper understanding of the current affiliate-based structure of ransomware operations, the chart above illustrates the impact of the Lockbit3 takedown. It demonstrates how affiliates swiftly transitioned to other Ransomware-as-a-Service (RaaS) platforms, resulting in only a slight decrease in the overall number of attacks. This adaptability underscores the resilience of the RaaS model, as affiliates ensured the continuity of operations even amidst significant disruptions.

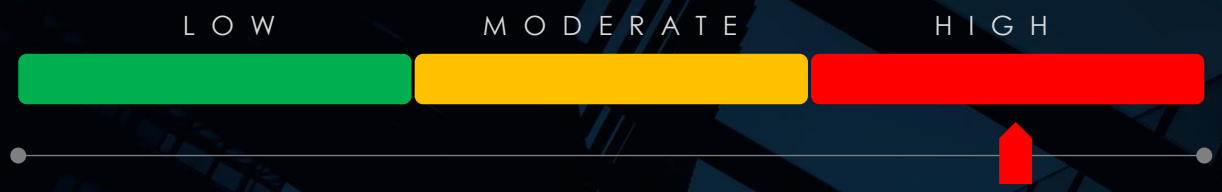
The evolution of dominant ransomware threats reflects the adaptability of this model. In 2023, Cl0p capitalized on high-profile vulnerabilities like MOVEit to dominate the ransomware landscape. By early 2024, Lockbit3 emerged as the most active threat, but within weeks, Ransomhub rose to prominence, filling the void and asserting dominance over the ransomware threat landscape.

This trend highlights that while the specific "flavors" of ransomware—individual strains and RaaS platforms—change over time, the affiliates responsible for the attacks remain consistent and continue to expand. Their international and regional presence not only enhances operational resilience but also contributes to the global spread of ransomware, making it a persistent and evolving threat in the cyber landscape.

The rise of both international and local affiliates has played a pivotal role in the global proliferation of ransomware. In regions such as Latin America, South Asia, Southeast Asia, and even parts of Africa, local affiliates have leveraged their regional knowledge and networks to contribute to the expansion of ransomware activity. This localized growth is complemented by the scalability of international affiliates, creating a powerful force that drives ransomware's increasing reach and impact.

RANSOMWARE EXTERNAL THREAT LANDSCAPE MANAGEMENT (ETLM) OVERVIEW

Year-over-Year Elevation: High



CYFIRMA identified 4,679 ransomware victims in 2023 and 5,219 in 2024, representing an 11.5% increase year-over-year. This growth reflects a dynamic and evolving threat landscape, with significant shifts in attacker tactics, targets, and regional focus.

Ransomware activity in 2023 was marked by the takedown of Hive, causing a temporary slowdown, followed by a surge from Cl0p exploiting the MOVEit vulnerability. Similarly, the early 2024 slowdown from the Lockbit3 takedown was brief, as affiliates shifted to other RaaS platforms and RansomHub quickly filled the void.

In 2023, 67 ransomware groups were active, rising to 97 in 2024. This increase was fuelled by splintering and rebranding of existing groups, and a global surge in activity, particularly in South and Southeast Asia and Latin America. The largest gangs like Lockbit3 dominated both years, though its activity declined after law enforcement takedown in early 2024. Meanwhile, RansomHub emerged strongly in 2024 after ALPHV and Lockbit3 faced setbacks.

Professional Goods & Services consistently led as the most targeted industry, maintaining nearly 16% share of all attacks. Consumer Goods & Services and Manufacturing followed closely, with Real Estate & Construction climbing from 7.03% in 2023 to 8.72% in 2024, advancing two positions. Conversely, Finance dropped from 8.45% to 5.23%, likely due to improved defences or reduced attacker focus.

In 2024, Education and Government & Civic sectors saw notable increases, particularly in Q4. Other sectors, such as Logistics, Telecommunications & Media, and Materials, showed steady growth, while Energy & Utilities and Automotive saw modest but consistent activity.

The United States remained the most targeted country by a significant margin, accounting for 46.3% and 50.6% of all victims in 2023 and 2024, respectively. Its dominance overshadowed other countries. Other regions like Canada, Israel, and India saw significant increases in 2024, while Italy and Thailand experienced declines.

The ransomware landscape in 2024 demonstrated high year-over-year elevation, with increased diversification among attackers and shifts in industry and regional targeting.

CYFIRMA
DECODING THREATS

BREAKDOWN OF INDUSTRY CATEGORIES IN 2024

The following section delves into the Advanced Persistent Threat (APT) campaigns and ransomware victimology of 2024, offering an in-depth analysis of 13 industry categories. Each industry's unique characteristics, vulnerabilities, and operational priorities have shaped how threat actors target and exploit them, providing valuable insights into the evolving cyber threat landscape.

This comprehensive overview highlights key trends, shifts in attacker focus, and the tactics, techniques, and procedures (TTPs) observed across sectors. The industries covered include:

- **Finance**: Covers banking, insurance, investment firms, and financial technology (FinTech) companies and other finance organizations.
- **Energy & Utilities**: Includes power generation, distribution, oil and gas, renewable energy, and water utilities.
- **Healthcare**: Encompasses hospitals, clinics, pharmaceutical companies, biotechnology firms, and health insurance providers.
- **Logistics**: Covers supply chain management, shipping, warehousing, and freight companies.
- **Manufacturing**: Focuses on general production sectors, with Automotive and Materials addressed separately.
- **Automotive**: Includes vehicle manufacturers, parts suppliers, and related service industries.
- **Materials**: Comprises sectors such as mining, chemicals, metals, construction materials, packaging (glass, plastic), paper and forest products, and agricultural materials.
- **Telecommunications & Media**: Encompasses publishing, advertising, broadcasting, printing, and other communication services.
- **Information Technology**: Includes software development, IT services, computers, and relevant hardware production.
- **Professional Goods & Services**: Covers business consulting, legal services, auditing, and other professional sectors.
- **Consumer Goods & Services**: Focuses on retail, food and beverage, apparel, and hospitality.
- **Real Estate & Construction**: Includes property development, construction companies, architects, and interior design services.
- **Government & Civic**: Encompasses government institutions, civic organizations, religious groups, and non-profits.

By examining the APT campaigns and ransomware victimology, this section delivers a granular view of the threats impacting these industries. It highlights both the overarching trends influencing the global threat landscape and the distinct challenges faced by each industry, providing stakeholders with critical insights to navigate the evolving cyber threat landscape heading into 2025.

FINANCE INDUSTRY IN 2024

ADVANCED PERSISTENT THREATS

Over the past 12 months, financial organizations recorded victims across 30 of the 34 Advanced Persistent Threat (APT) campaigns observed - an incidence rate of 94%.

These victims spanned multiple segments within the financial industry as shown below.

OBSERVED CAMPAIGNS PER MONTH

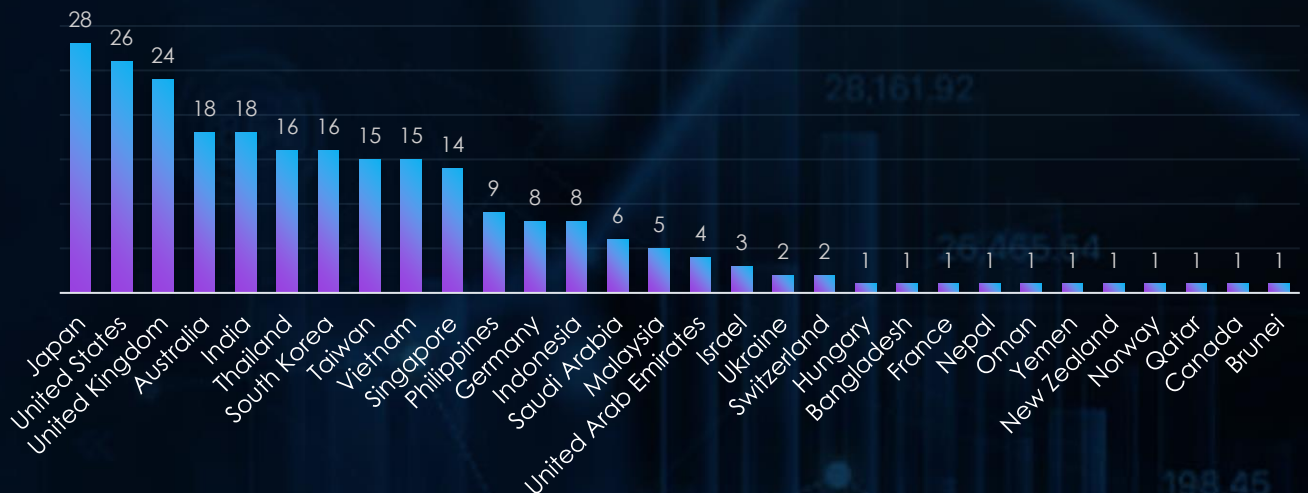
CYFIRMA
DECODING THREATS

APT CAMPAIGNS - FINANCE

SUSPECTED THREAT ACTORS

The finance industry faces threats from both financially motivated cybercrime groups and nation-state actors. Groups like Lazarus, FIN7, and TA505 focus on direct monetary exploitation, often through data theft and ransomware, while nation-state entities such as Mustang Panda, Cozy Bear, and Gamaredon target financial institutions for espionage or geopolitical purposes. Emerging and lesser-known groups, including regionally focused actors like unknown Thai- and Vietnamese-speaking TAs, add complexity to the landscape, underscoring the diverse and evolving nature of threats in the sector.

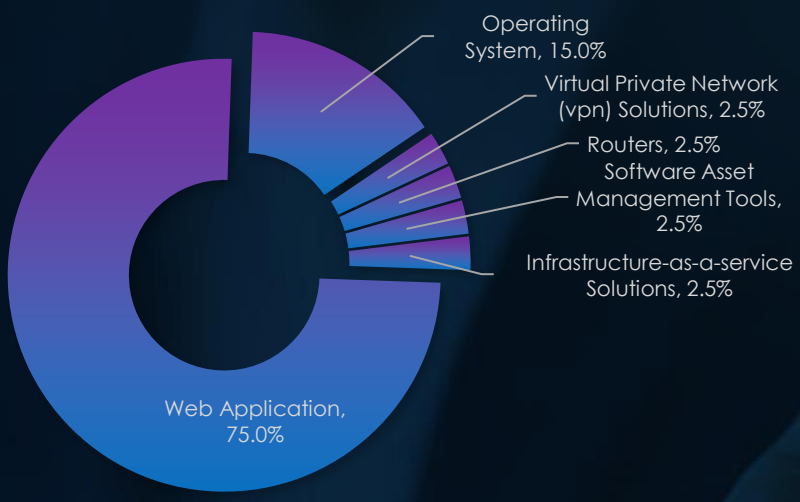
GEOGRAPHICAL DISTRIBUTION



The chart shows APT campaigns targeting the finance sector across 30 countries, with a clear focus on North America, East Asia, and Southeast Asia. The United States, Japan, and the United Kingdom lead in incidents, while countries like Taiwan, Thailand, and India highlight regional emphasis. Emerging economies, including Saudi Arabia and the Philippines, further demonstrate the expanding reach of these threats.

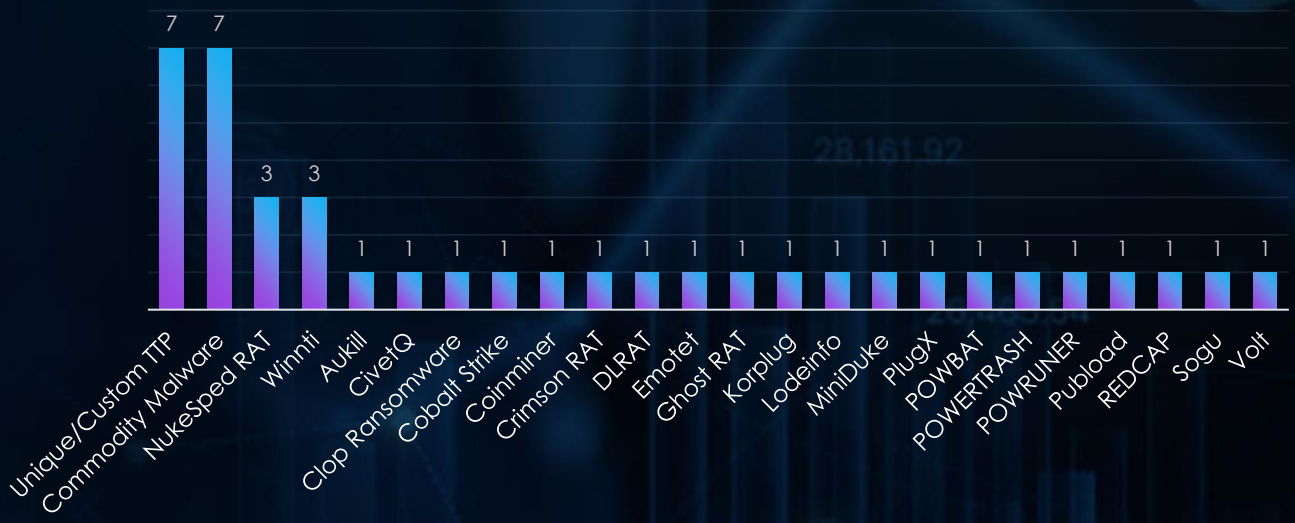
APT CAMPAIGNS - FINANCE

TOP ATTACKED TECHNOLOGY



The chart highlights the top technologies targeted in attacks, with web applications standing out as the primary focus, emphasizing their vulnerability as internet-facing systems. Operating systems follow, reflecting their ubiquity across devices and critical role in operations. While VPN solutions, routers, and infrastructure-as-a-service solutions have lower incident counts, they remain vital targets.

TOP MALWARE



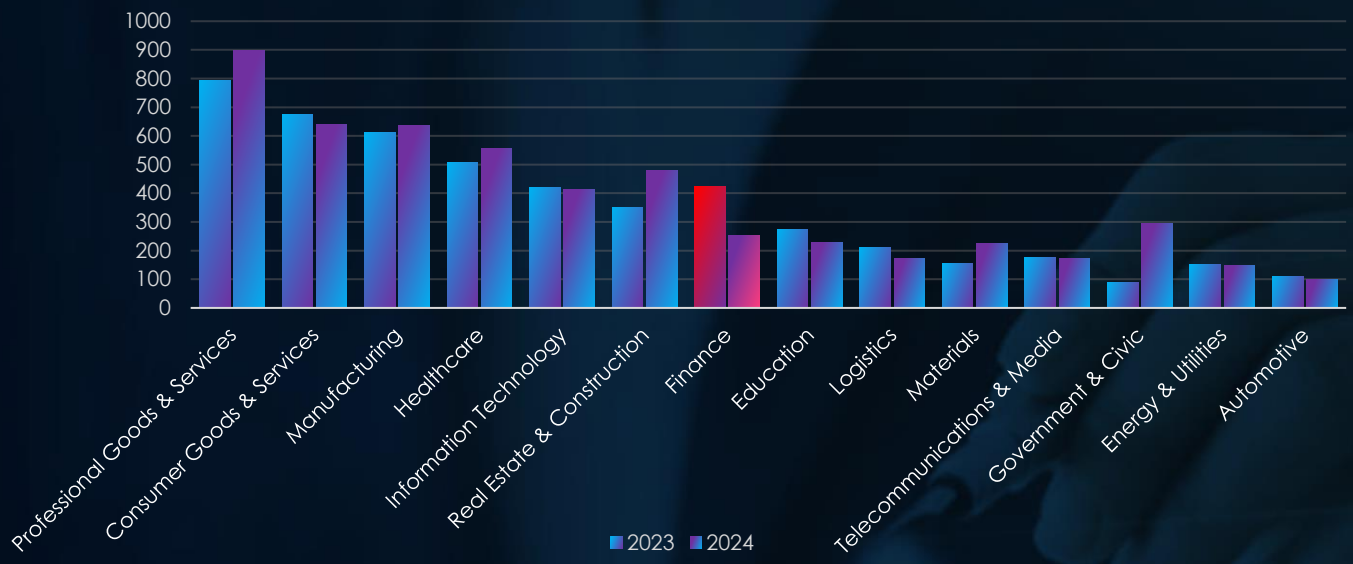
The chart highlights the top malware used in attacks, with custom TTPs and commodity malware leading the list. Together with Cobalt Strike, they emphasize attackers' adaptability in leveraging both custom and widely available malware.

Notable strains like NukeSped RAT and Winnti reflect their continued evolution and use by respective threat actors.

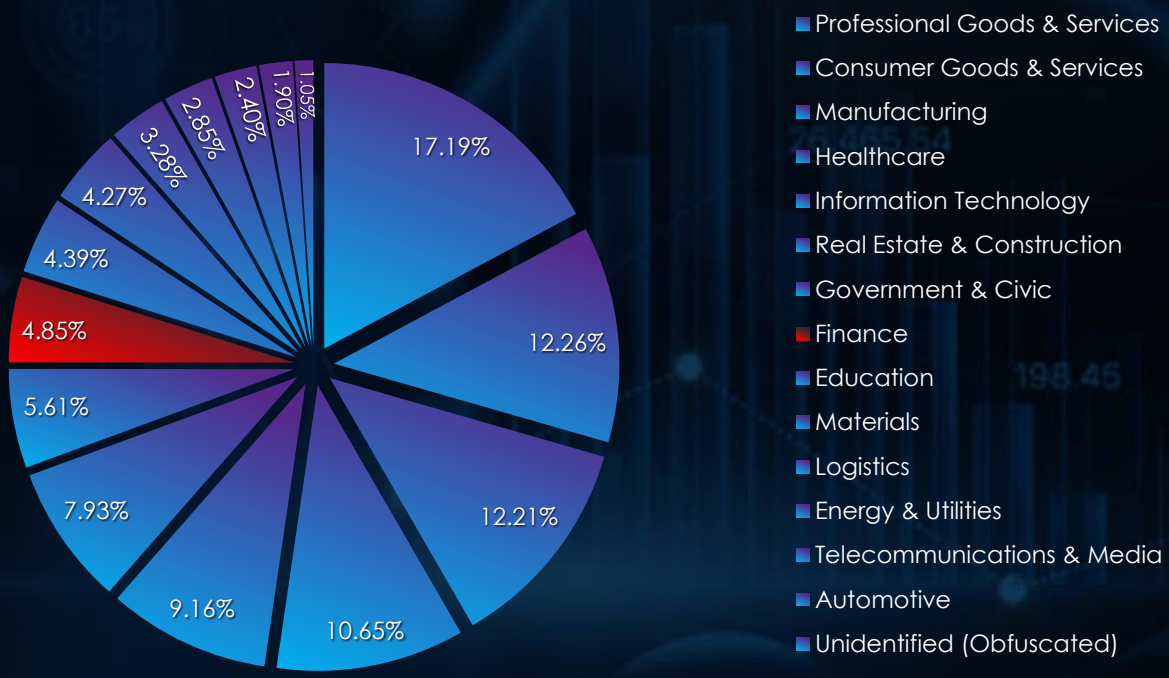
RANSOMWARE VICTIMOLOGY FINANCE

In the past 12 months, CYFIRMA has identified 253 verified finance organization ransomware victims. This accounts for 4.85% of the overall total of 5,219 ransomware victims during the same period.

GLOBAL DISTRIBUTION BY INDUSTRY

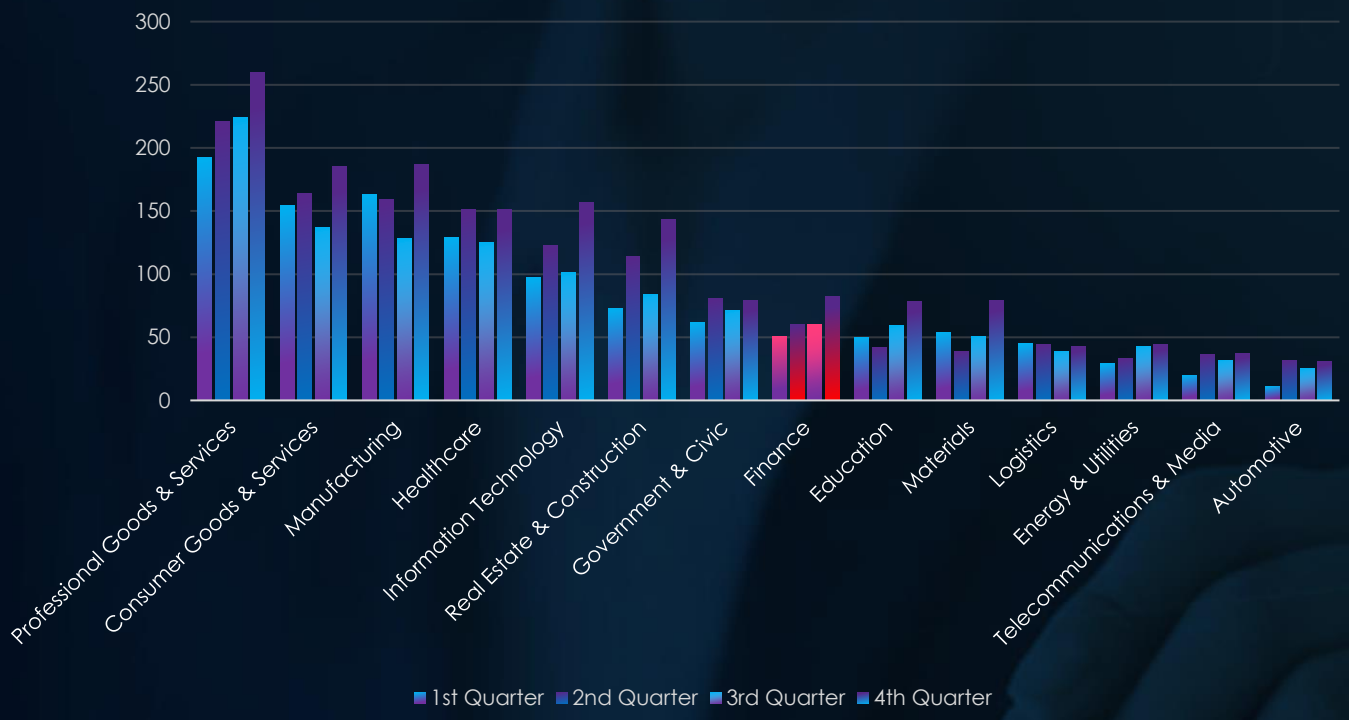


The finance industry recorded a significant decline of -40.19% in recorded victims from previous year. Placing 7th overall in combined years of 2023 and 2024, it moved down from 5th to 8th most frequent victim. In respective years.



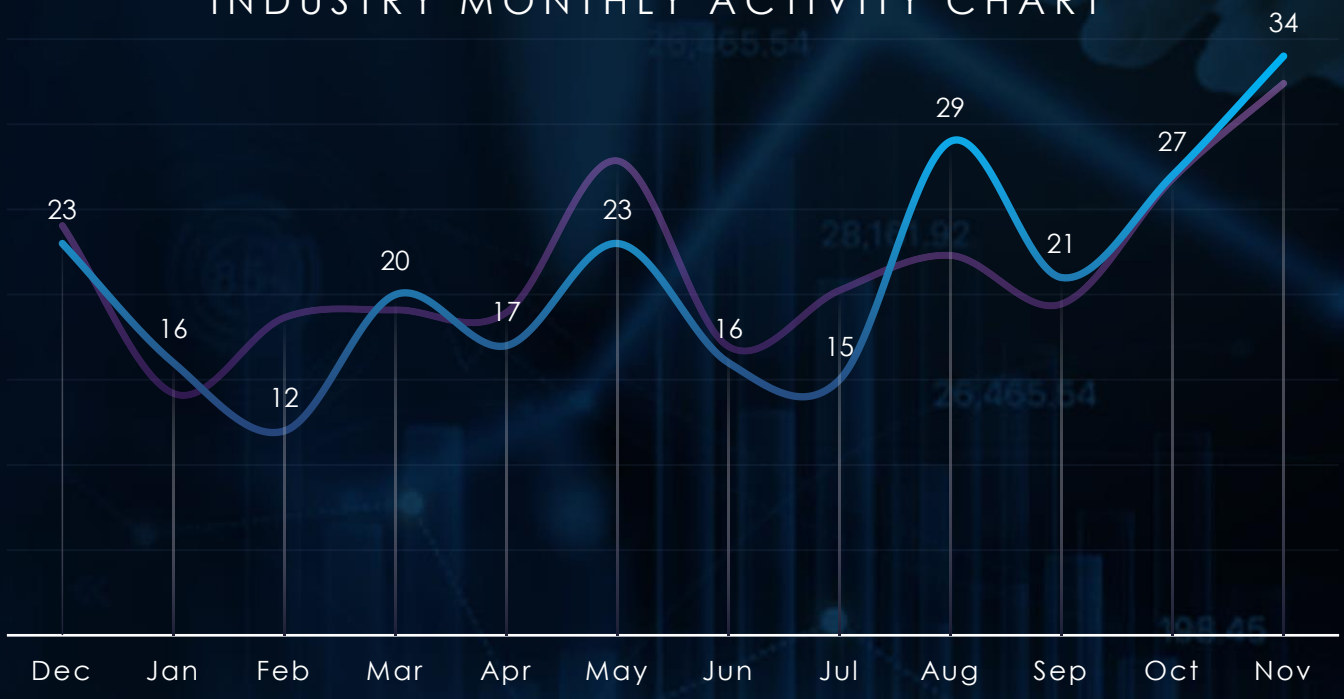
CYFIRMA
DECODING THREATS

QUARTERLY CHANGES DURING 2024



First and especially second quarters were significantly lower, and the number of victims grew substantially towards the end of the year.

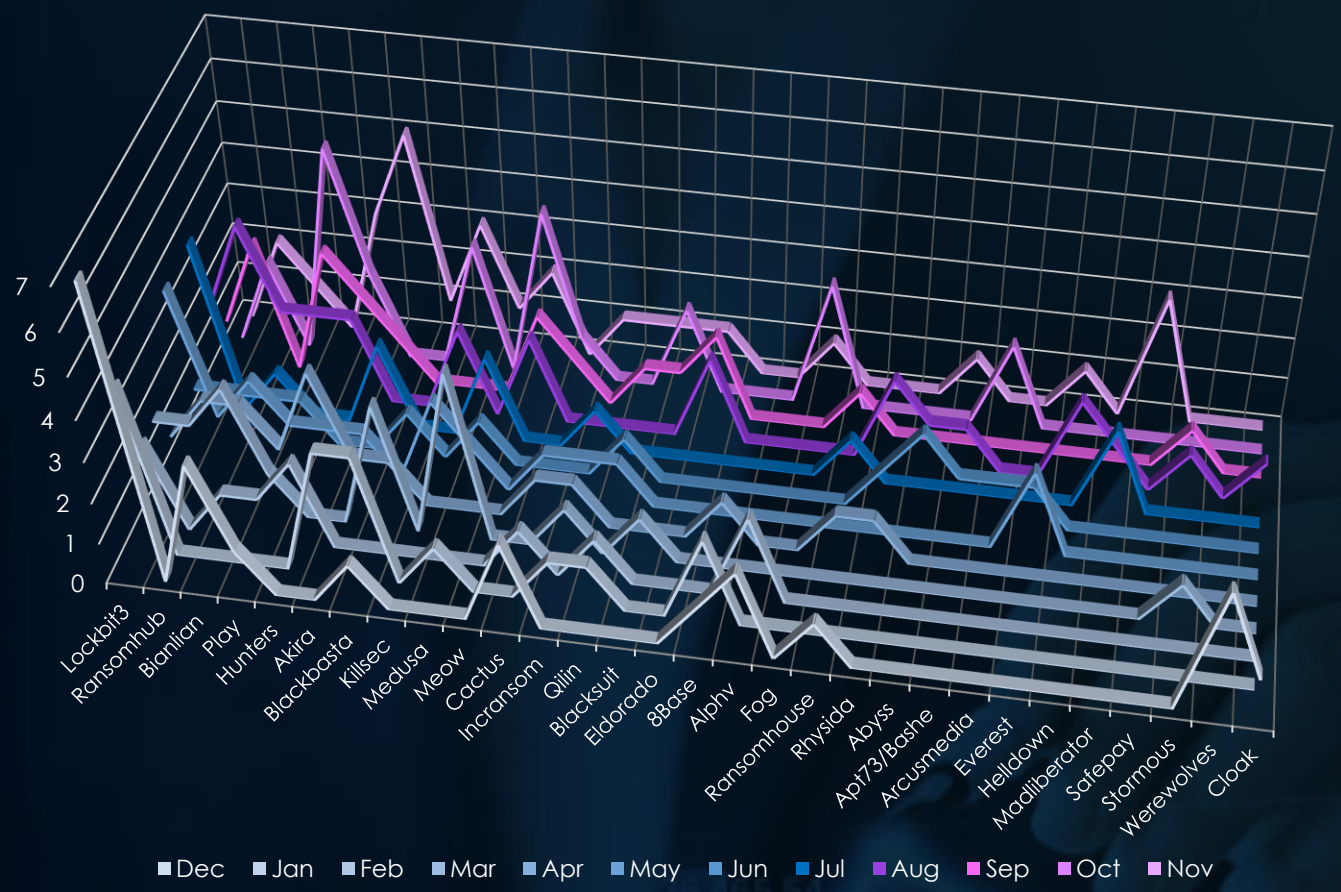
INDUSTRY MONTHLY ACTIVITY CHART



Monthly activity in finance mostly follows the scaled-down global trendline. August and November recorded significant spikes and are implying a growing trend into 2025.

CYFIRMA
DECODING THREATS

BREAKDOWN OF ACTIVITY PER GANG



A total of 54 out of 97 ransomware gangs, representing 56%, targeted the finance industry.

A breakdown of the top 30 gangs' monthly activity offers insights into their operational patterns throughout the year.

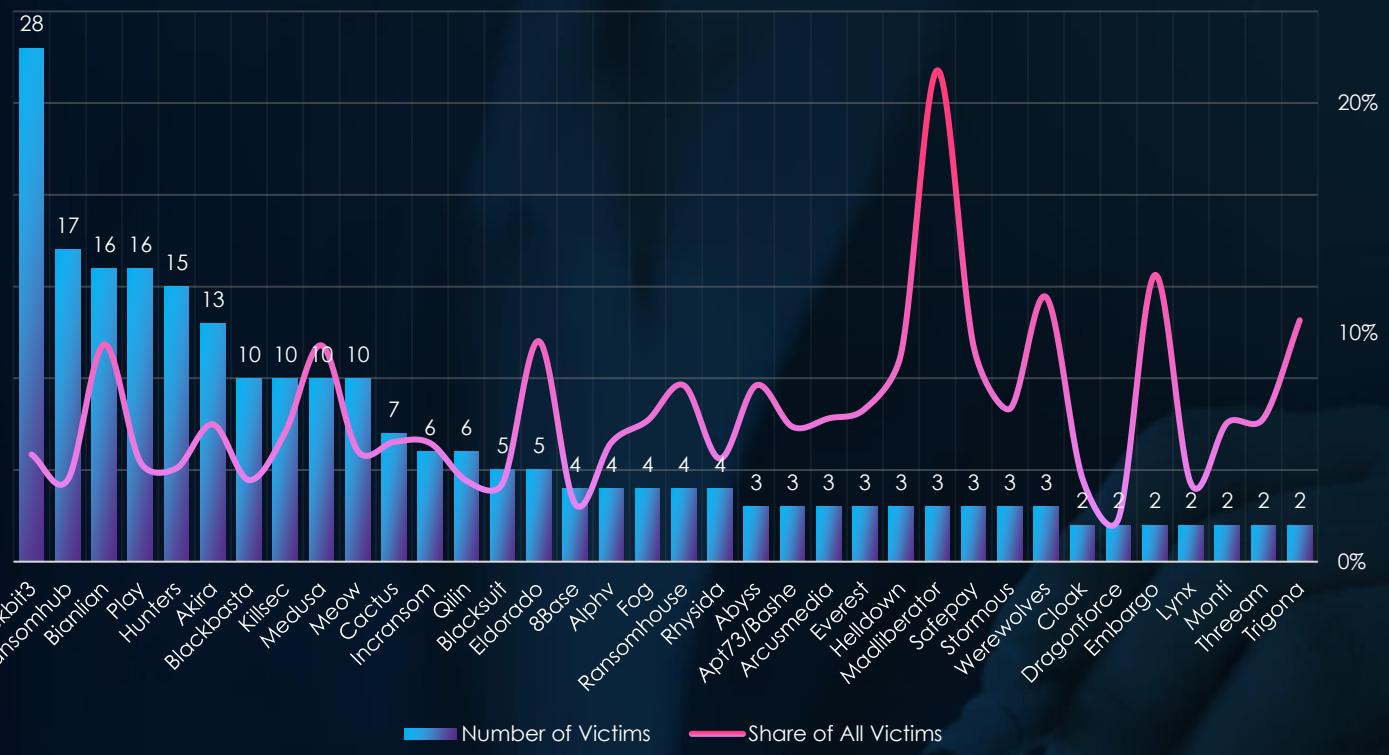
Lockbit3 was the most active ransomware gang, impacting 28 victims, with peaks in December (7 victims). Ransomhub followed with 17 victims, focusing on late-year attacks, particularly in August, September, and November. Play and Bianlian each targeted 16 victims, with Play peaking in September-October and Bianlian active in December, March, and mid-year months.

Hunters impacted 15 victims, with notable activity in March, September, and November. Akira targeted 13 victims, with most activity occurring late in the year, especially in November. Blackbasta and Killsec (10 victims each) were active early and late in the year, respectively, with Killsec peaking in September-November.

Medusa and Meow each had 10 victims, with Medusa active in March and July, and Meow peaking between August and November. Smaller gangs like Cactus (7 victims), Incransom, Qilin, and Rhysida (6 each) had sporadic but focused campaigns.

Emerging groups like Blacksuit, Eldorado, and Alphv (4-5 victims each) had limited activity, while Safepay concentrated its attacks on three victims in November.

INDUSTRY RANSOMWARE VICTIMS PER GANG



Analyzing top 35 active gangs, Lockbit3 leads in activity within the finance sector, with 28 victims (4.67%), reflecting significant activity but broad targeting across industries. Ransomhub (17 victims, 3.58%) and Play (16 victims, 4.35%) also exhibit moderate activity in this sector. Other active gangs include Bianlian (16 victims, 9.47%) and Medusa (10 victims, 9.43%), which show higher focus relative to their activity levels.

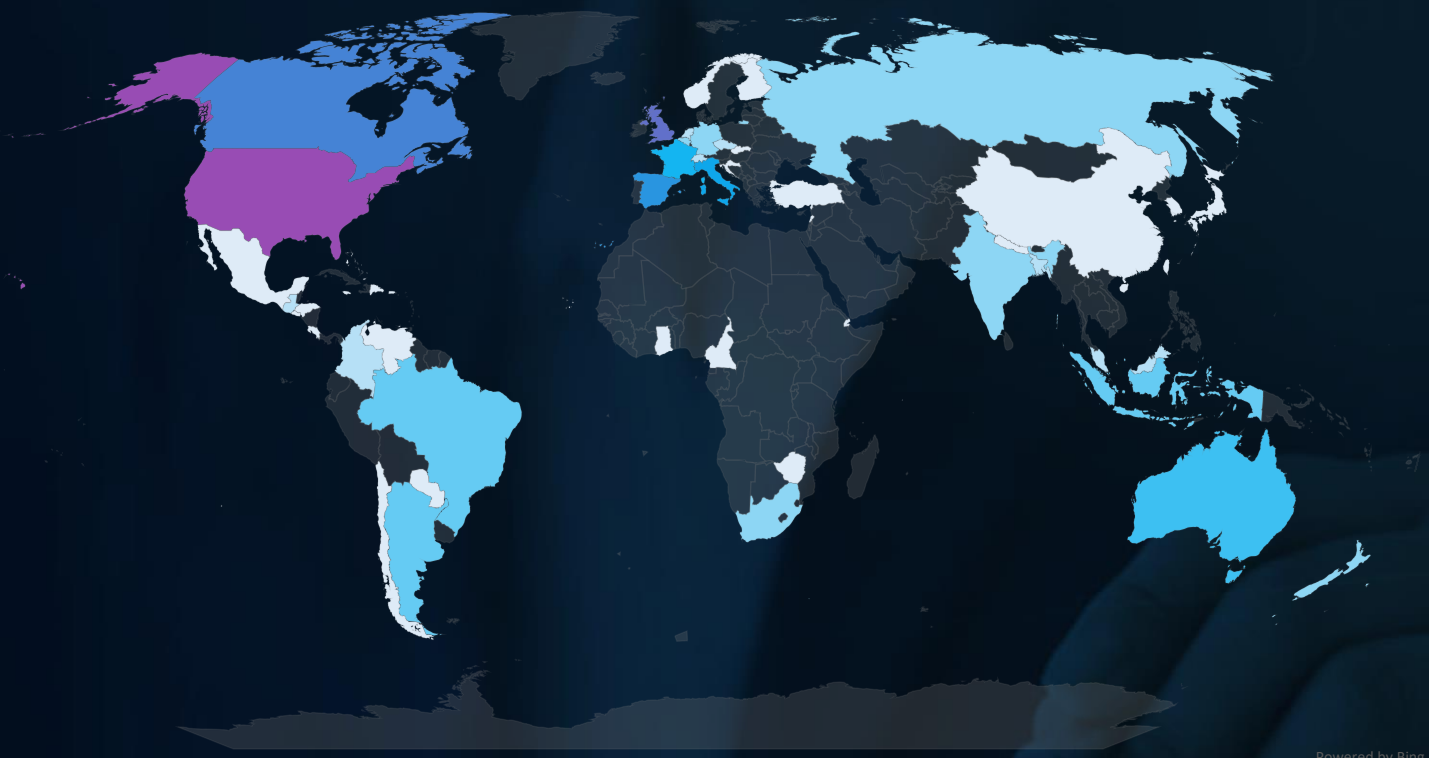
Several gangs exhibit significant focus on the finance industry:

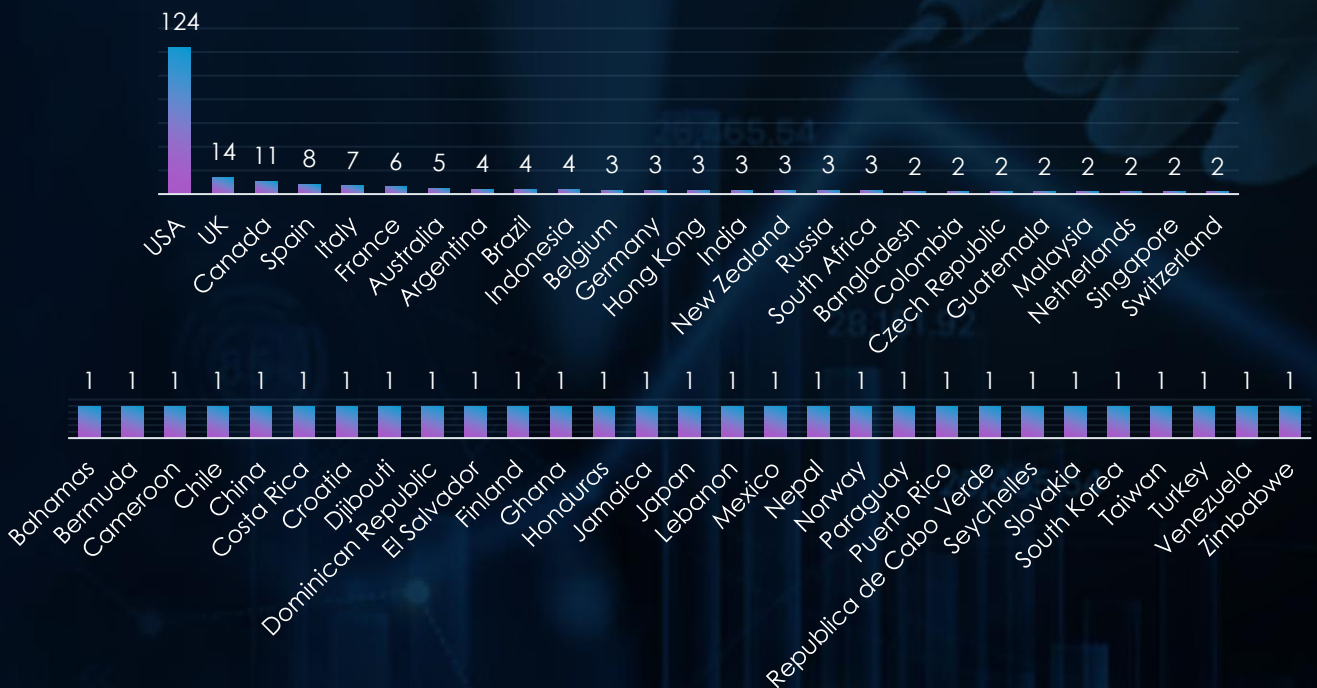
- Bianlian (16 victims, 9.47%) and Medusa (10 victims, 9.43%) indicate strong attention to the sector.
- Eldorado (5 victims, 9.62%) and Safepay (3 victims, 9.38%) demonstrate concentrated efforts with smaller victim counts.
- Werewolves (3 victims, 11.54%) reflects a focused targeting strategy despite its small activity level.

Some gangs exhibit disproportionately high percentages due to low victim counts:

- Madliberator (3 victims, 21.43%) and Embargo (2 victims, 12.50%) reflect high percentages driven by minimal activity.
- Helldown (3 victims, 9.09%) and Werewolves (3 victims, 11.54%) also highlight concentrated efforts that may not indicate widespread impact.
- Smaller gangs like Abyss (3 victims, 7.69%) and Ransomhouse (4 victims, 7.69%) show elevated percentages but limited activity.

GEOGRAPHIC DISTRIBUTION OF VICTIMS





The USA accounts for 49.4% of ransomware victims in the finance industry in 2024. The next most affected countries are the UK with 14 victims, Canada with 11, Spain with 8, and Italy with 7.

In total, 54 countries reported victims, and 27 of these countries had only one victim each.

CYFIRMA
DECODING THREATS

FINANCE INDUSTRY EXTERNAL THREAT LANDSCAPE MANAGEMENT (ETLM) OVERVIEW

Risk Level Indicator: High

APT Campaigns

Financial organizations experienced a 94% incidence rate across observed APT campaigns, targeting both monetary assets and sensitive data. Threat actors range from financially motivated groups (e.g., Lazarus, FIN7) to nation-state entities (e.g., Mustang Panda, Cozy Bear). Emerging regional threats add complexity. Key focus areas include North America, East Asia, and Southeast Asia, with critical vulnerabilities in web applications and operating systems.

Actors: Lazarus, FIN7, TA505; Mustang Panda, Cozy Bear, Gamaredon; regional groups.

Geographic Focus: U.S., Japan, U.K., Taiwan, Thailand, India; emerging economies like Saudi Arabia.

Targets: Web apps, operating systems, VPNs, IaaS solutions.

Malware: Cobalt Strike, NukeSped RAT, Winnti.

Ransomware

The finance industry recorded 253 ransomware victims in the past year (4.85% of global total), with a significant -40.19% decline from the previous year. LockBit 3 led attacks, followed by BianLian and Medusa, with emerging groups like RansomHub and Madliberator also targeting finance. Spikes in activity during August and November hint at a growing trend into 2025.

Victim Trends: Lower activity early in 2024, spikes in August/November.

Key Actors: LockBit 3, BianLian, Medusa, RansomHub, Madliberator.

Ranking: Finance ranked 8th most targeted sector globally in 2024.

CYFIRMA
DECODING THREATS

FINANCE INDUSTRY EXTERNAL THREAT LANDSCAPE MANAGEMENT (ETLM) OVERVIEW

Risk Level Indicator: High

APT Campaigns

Financial organizations experienced a 94% incidence rate across observed APT campaigns, targeting both monetary assets and sensitive data. Threat actors range from financially motivated groups (e.g., Lazarus, FIN7) to nation-state entities (e.g., Mustang Panda, Cozy Bear). Emerging regional threats add complexity. Key focus areas include North America, East Asia, and Southeast Asia, with critical vulnerabilities in web applications and operating systems.

Actors: Lazarus, FIN7, TA505; Mustang Panda, Cozy Bear, Gamaredon; regional groups.

Geographic Focus: U.S., Japan, U.K., Taiwan, Thailand, India; emerging economies like Saudi Arabia.

Targets: Web apps, operating systems, VPNs, IaaS solutions.

Malware: Cobalt Strike, NukeSped RAT, Winnti.

Ransomware

The finance industry recorded 253 ransomware victims in the past year (4.85% of global total), with a significant -40.19% decline from the previous year. LockBit 3 led attacks, followed by BianLian and Medusa, with emerging groups like RansomHub and Madliberator also targeting finance. Spikes in activity during August and November hint at a growing trend into 2025.

Victim Trends: Lower activity early in 2024, spikes in August/November.

Key Actors: LockBit 3, BianLian, Medusa, RansomHub, Madliberator.

Ranking: Finance ranked 8th most targeted sector globally in 2024.

CYFIRMA
DECODING THREATS

ENERGY & UTILITIES INDUSTRY IN 2024

ADVANCED PERSISTENT THREATS

Over the past 12 months, energy & utilities organizations recorded victims across 7 of the 34 Advanced Persistent Threat (APT) campaigns observed - an incidence rate of 21%.

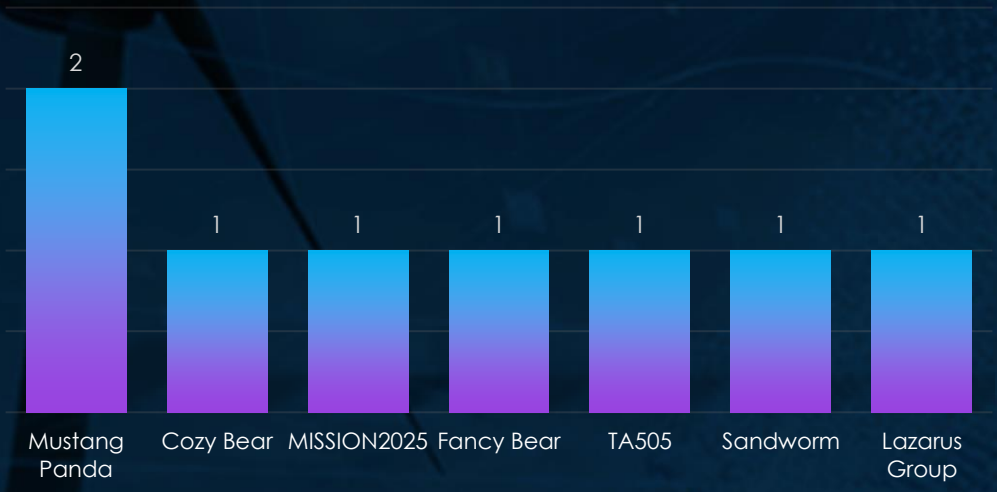
These victims spanned multiple segments within the energy & utilities industry as shown below

OBSERVED CAMPAIGNS PER MONTH

CYFIRMA
DECODING THREATS

APT CAMPAIGNS – ENERGY & UTILITIES

SUSPECTED THREAT ACTORS



The energy and utilities industry faces threats from both nation-state and financially motivated groups. Mustang Panda and MISSION2025 (China) target the sector for espionage, while Russian actors like Cozy Bear, Fancy Bear, and Sandworm focus on both intelligence and disruption. Lazarus Group (North Korea) and TA505 highlight the financial motivations, targeting resources for state funding and profit.

GEOGRAPHICAL DISTRIBUTION

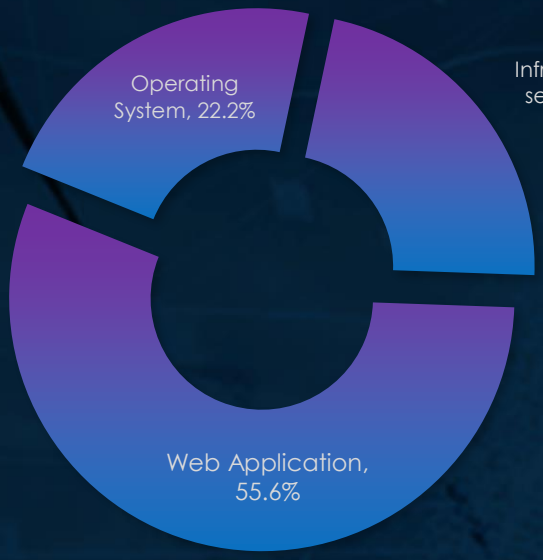
The geographic targeting of the energy and utilities sector highlights its global significance, with a strong focus on advanced economies like Japan, the United States, and the United Kingdom, alongside growing activity in Asia-Pacific regions such as Vietnam, Taiwan, and Thailand.

Emerging markets, including India and the Philippines, are also increasingly targeted, while smaller nations like Saudi Arabia and Norway with significant energy resources also attract attention.

CYFIRMA
DECODING THREATS

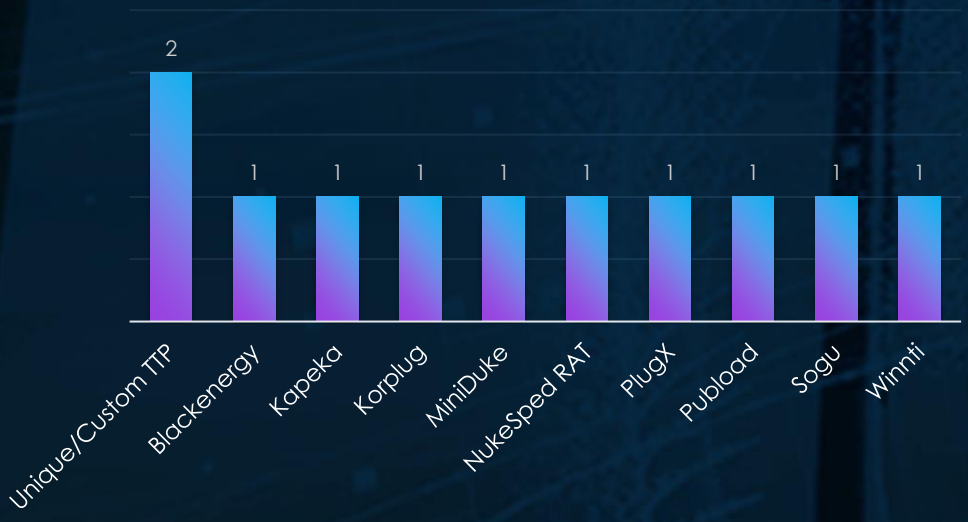
APT CAMPAIGNS – ENERGY & UTILITIES

TOP ATTACKED TECHNOLOGY



Web applications are the primary target, highlighting their vulnerability as internet-facing systems. Operating systems and infrastructure-as-a-service solutions are also key targets, emphasizing the attackers' aim to exploit foundational technologies critical to operational continuity.

TOP MALWARE



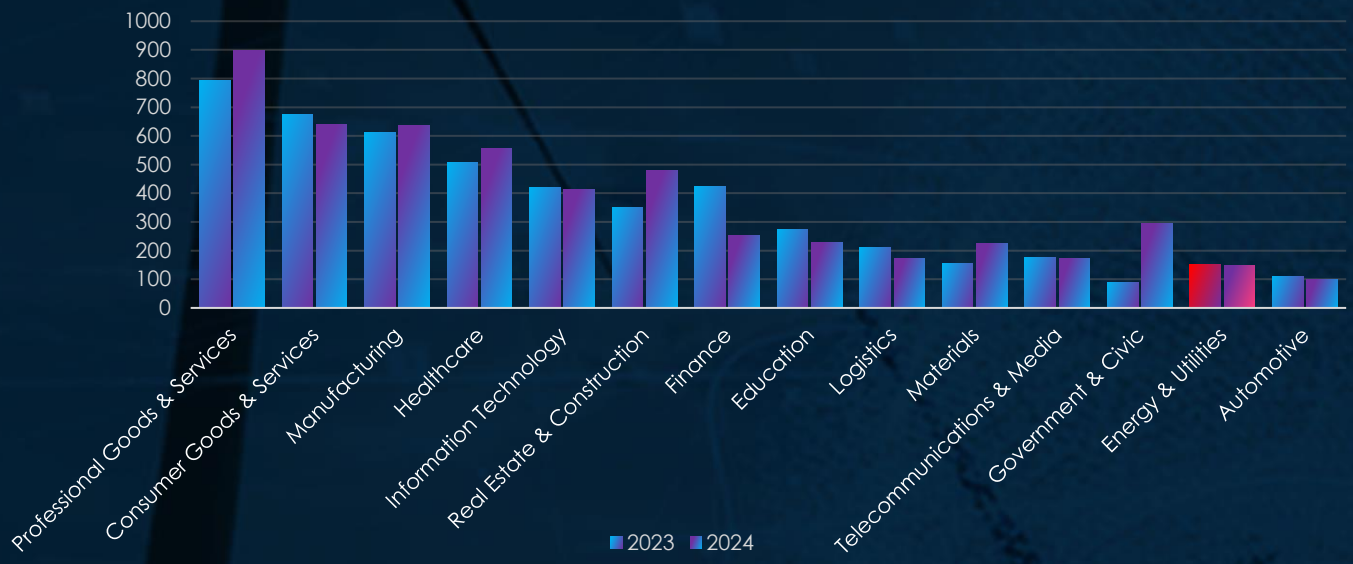
The malware targeting the energy and utilities sector demonstrates a mix of unique, custom TTPs and well-known strains. Custom TTPs lead, reflecting attackers' tailored approaches to compromising critical infrastructure. Notable malware such as BlackEnergy, NukeSped RAT, and PlugX highlight a focus on espionage and operational disruption, while tools like Winnti and Korplug emphasize long-term persistence and data theft.

CYFIRMA
DECODING THREATS

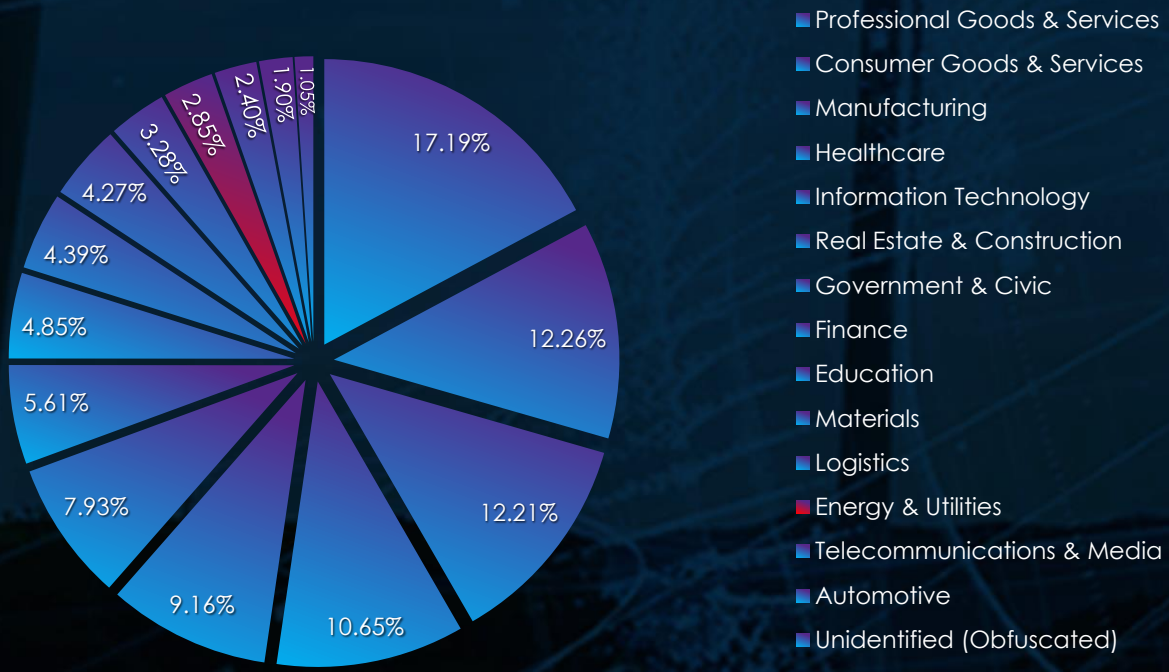
RANSOMWARE VICTIMOLOGY
ENERGY & UTILITIES

In the past 12 months, CYFIRMA has identified 149 verified energy & utilities organization ransomware victims. This accounts for 2.85% of the overall total of 5,219 ransomware victims during the same period.

GLOBAL DISTRIBUTION BY INDUSTRY

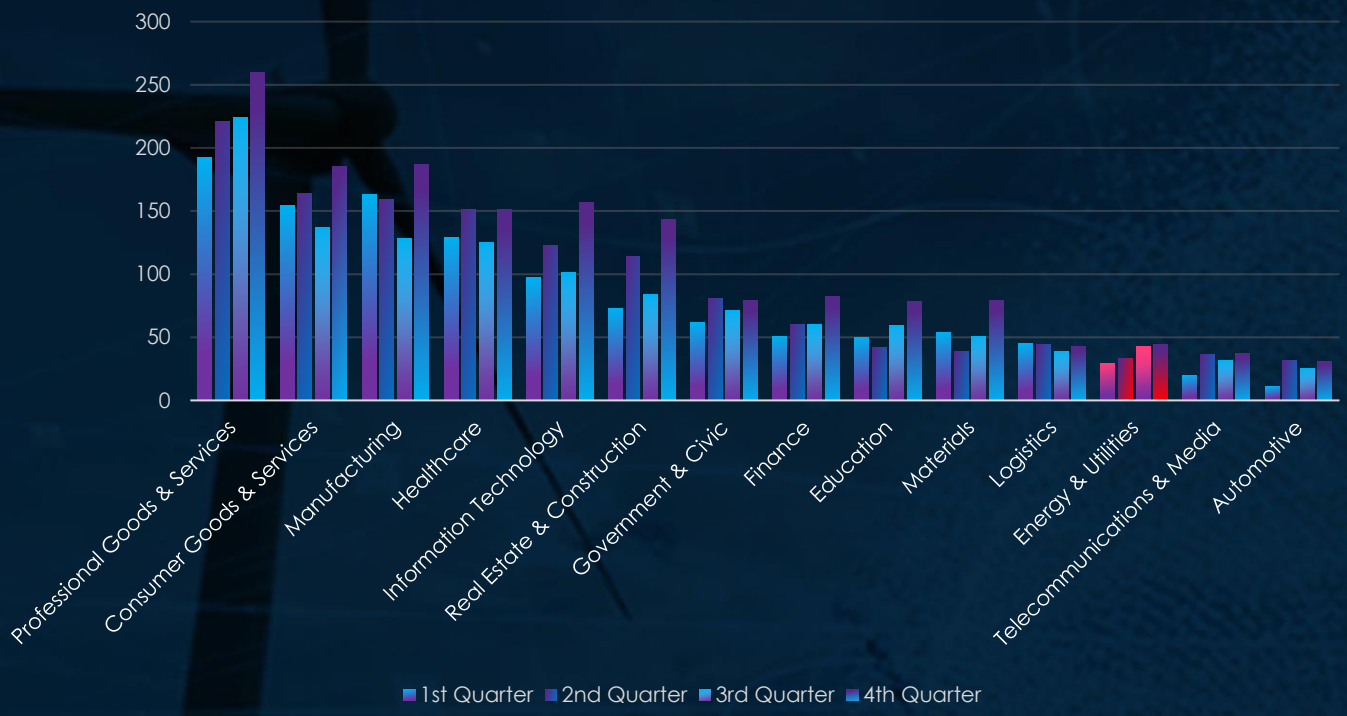


The industry recorded a minor decline of -1.97% in recorded victims from previous year. And although bumped down one position in combined 2023 and 2024 number of victims, it retained 12th position as the third least frequent victim for respective years.



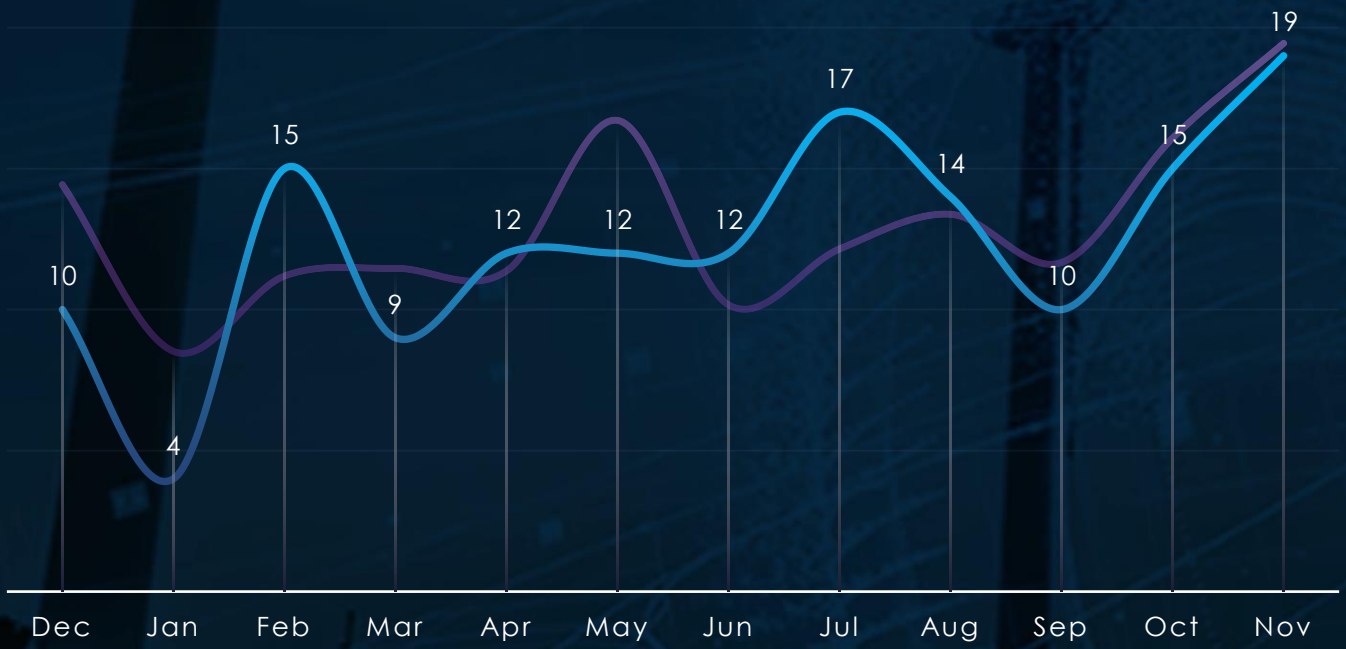
CYFIRMA
DECODING THREATS

QUARTERLY CHANGES DURING 2024



Energy & utilities show sustained numbers of victims. Start of the year was little slower, but number of victims started to pick up in second half.

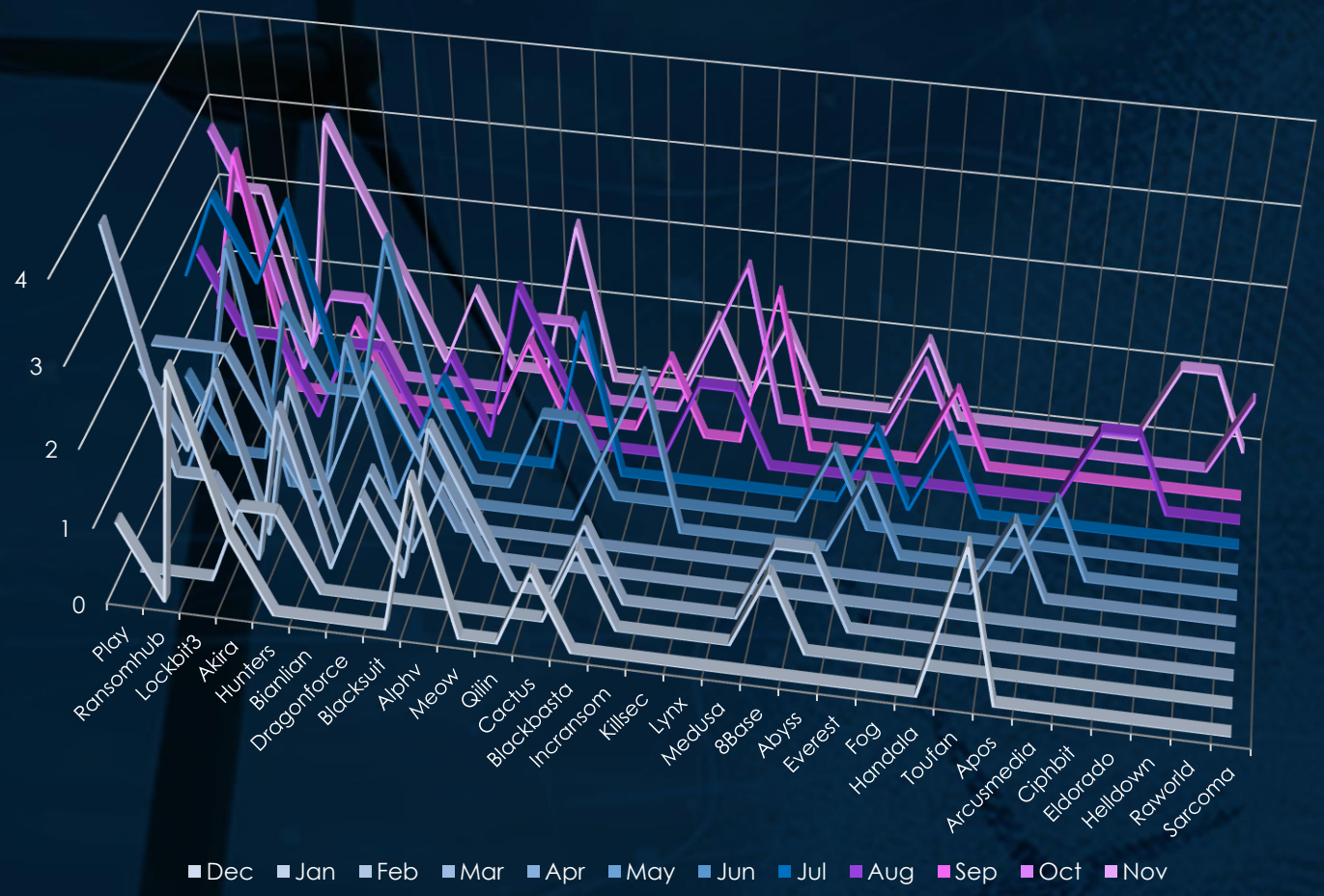
INDUSTRY MONTHLY ACTIVITY CHART



Monthly activity diverged in the middle months from scaled down global trendline. Start of the year was slow in line with global trend, then February recorded significant spike and then another during July. In October and November we see upwards trend, implying increase of activity into 2025.

CYFIRMA
DECODING THREATS

BREAKDOWN OF ACTIVITY PER GANG



In total 32 out of 97 gangs recorded victims in healthcare industry, 33% participation.

A breakdown of top 30 gangs' monthly activity provides insights into which gangs were active each month.

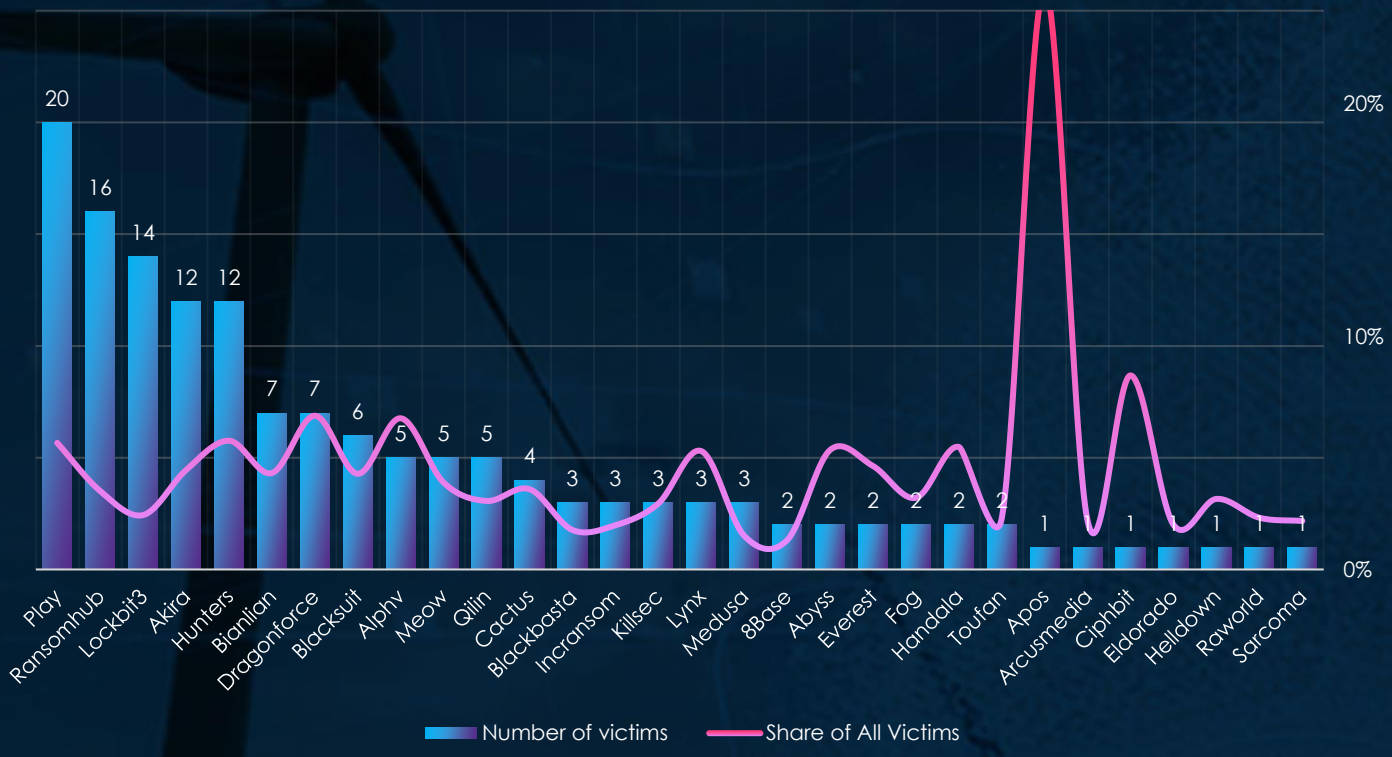
Play was the most active gang, targeting 20 victims throughout the year, with notable spikes in February (4 victims) and steady activity across multiple months, including March, April, and November. Ransomhub followed with 16 victims, focusing its efforts on the latter half of the year, particularly in July, September, October, and November.

Lockbit3 impacted 14 victims, with most activity concentrated in December. Akira and Hunters each targeted 12 victims. Akira was especially active in July and November, while Hunters maintained steady activity, peaking in February, March, and late in the year.

Smaller groups like Bianlian and Dragonforce targeted seven victims each, with Dragonforce peaking in May and June. Blacksuit (6 victims) and Alphv, Meow, and Qilin (5 each) had sporadic activity, with Alphv active early in the year and Qilin showing later-year spikes.

Cactus impacted four victims, primarily mid-year. Several smaller groups, such as Blackbasta, Killsec, and Incransom (3 victims each), displayed limited and scattered campaigns. Minor actors like Toufan, Medusa, and Handala targeted one or two victims during specific months, reflecting isolated operations.

INDUSTRY RANSOMWARE VICTIMS PER GANG

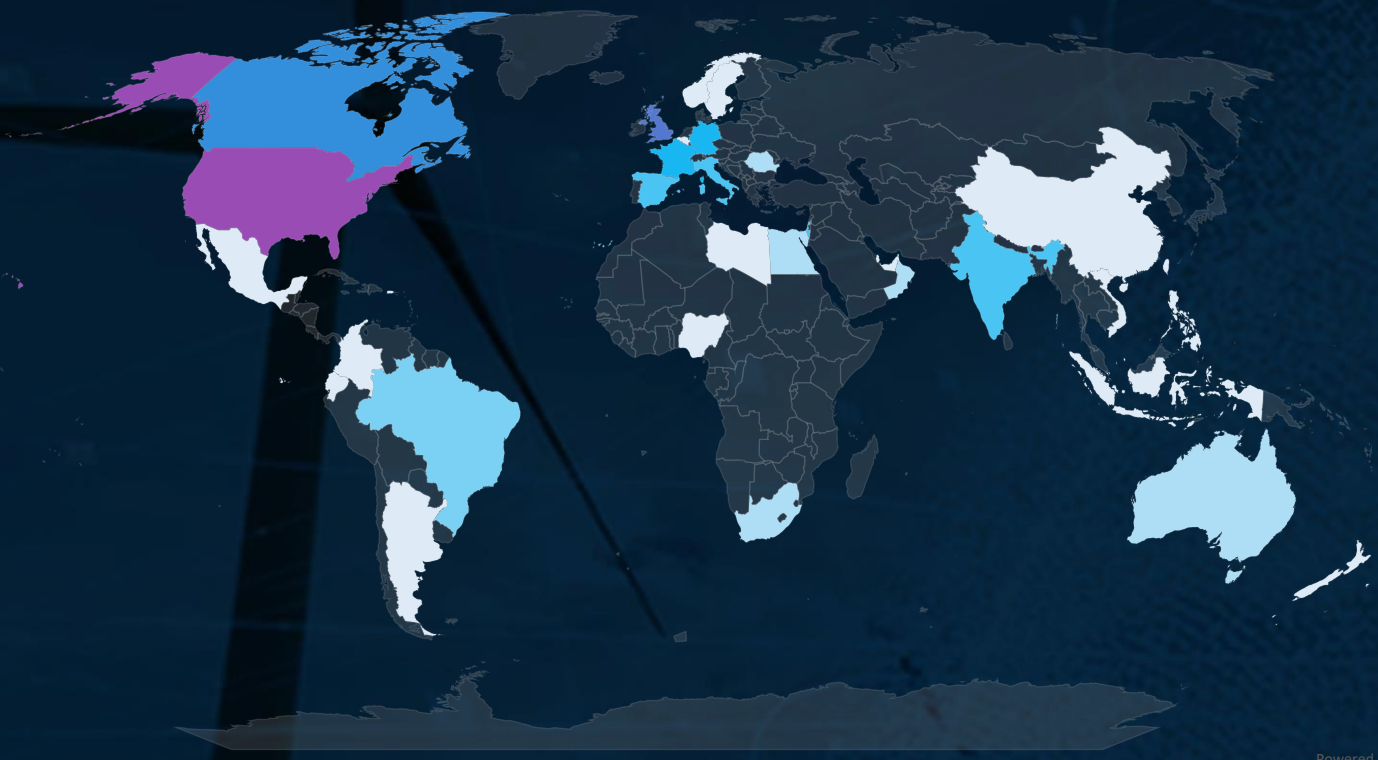


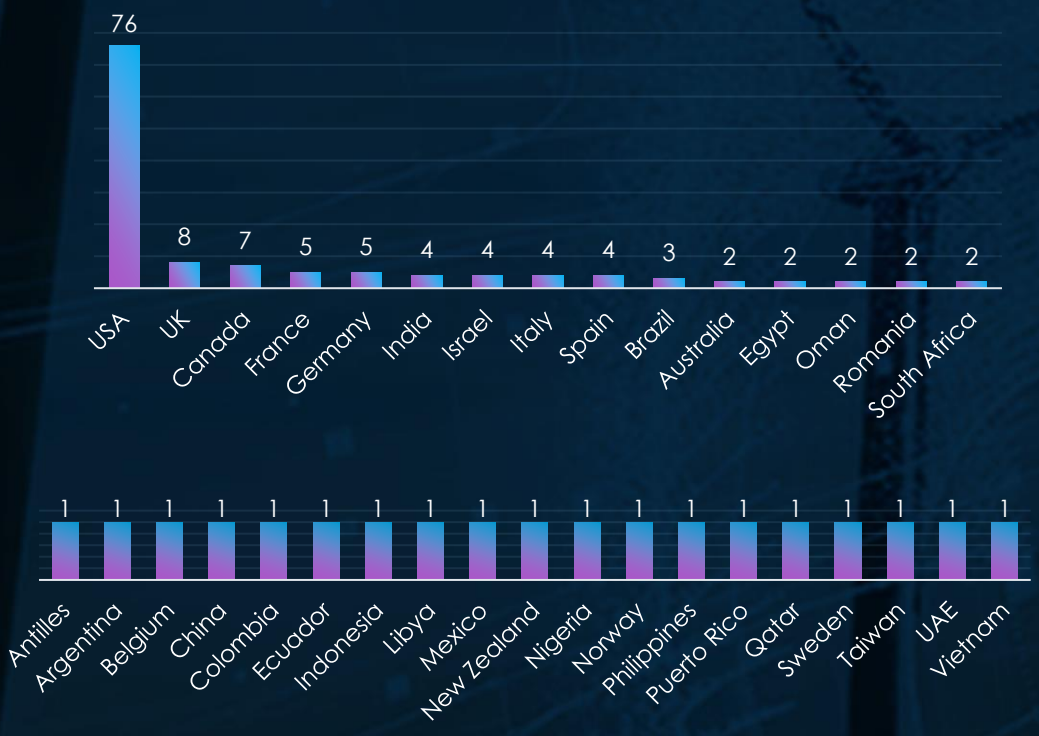
Play is the most active gang in this sector, with 20 victims (5.43%), followed by Ransomhub, with 16 victims (3.37%), and Lockbit3, with 14 victims (2.34%). These gangs exhibit broad targeting strategies across multiple industries, as reflected by their relatively low percentages in this sector. Akira and Hunters, with 12 victims each (4.27% and 5.53% respectively), also demonstrate moderate activity within energy and utilities.

No gangs exceed the 10% benchmark here, but some demonstrate noticeable focus with percentages above 5% and moderate victim counts. Dragonforce, with 7 victims (6.60%), and Alphv, with 5 victims (6.49%), stand out for their heightened attention to the energy sector. Lynx (3 victims, 5.08%) and Hunters (12 victims, 5.53%) also show signs of meaningful targeting in this sector.

Certain gangs exhibit disproportionately high percentages due to small victim counts. Apos, with only 1 victim but a striking 25.00%, reflects an extreme example of this skew. Similarly, Termite (1 victim, 16.67%) and Ciphbit (1 victim, 8.33%) show high percentages that do not indicate significant activity in the sector. Handala (2 victims, 5.26%) and Abyss (2 victims, 5.13%) also exhibit skewed percentages driven by their low absolute numbers of victims.

GEOGRAPHIC DISTRIBUTION OF VICTIMS





The USA accounts for 51.0% of ransomware victims in the Energy & Utilities industry in 2024. The next most affected countries are the UK with 8 victims, Canada with 7, and France and Germany each with 5 victims.

A total of 34 countries reported victims, with 19 of them having only one victim each.

CYFIRMA
DECODING THREATS

ENERGY & UTILITIES INDUSTRY EXTERNAL THREAT LANDSCAPE MANAGEMENT (ETLM) OVERVIEW

Risk Level Indicator: Low

APT Campaigns

Energy & utilities organizations experienced a 21% incidence rate across observed APT campaigns, with threats driven by both nation-state and financially motivated actors. Espionage-focused groups (e.g., Mustang Panda, Cozy Bear) target critical infrastructure, while others (e.g., Lazarus, TA505) exploit resources for financial gain. Advanced economies like the U.S., U.K., and Japan remain primary targets, with increasing activity in Asia-Pacific and emerging markets.

Actors: Mustang Panda, Cozy Bear, Sandworm; Lazarus Group, TA505.

Geographic Focus: U.S., U.K., Japan; rising activity in Vietnam, Taiwan, India, and the Philippines.

Targets: Web applications, operating systems, and IaaS solutions.

Malware: BlackEnergy, NukeSped RAT, PlugX; persistent tools like Winnti, Korplug.

Ransomware

The energy & utilities sector accounted for 149 ransomware victims in the past year (2.85% of the global total), with a minor decline of -1.97% from 2023. Activity spiked in February and July, with rising trends in October and November, suggesting increased targeting into 2025. Play ransomware was the most active group, but no gang showed a consistent focus on this industry.

Victim Trends: Slow start, spikes in February and July, upward trends in late 2024.

Key Actors: Play led activity, with Ransomhub rising later in the year.

Geography: U.S. accounted for 51% of geographically identified victims.

Ranking: Energy & utilities ranked 12th globally for ransomware targeting.

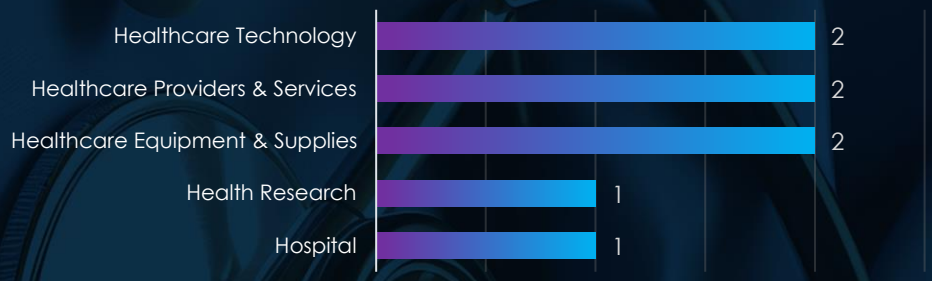
CYFIRMA
DECODING THREATS

HEALTHCARE INDUSTRY IN 2024

ADVANCED PERSISTENT THREATS

Over the past 12 months, healthcare organizations recorded victims across 2 of the 34 Advanced Persistent Threat (APT) campaigns observed - an incidence rate of 6%.

These victims spanned multiple segments within the healthcare industry as shown below:



OBSERVED CAMPAIGNS PER MONTH

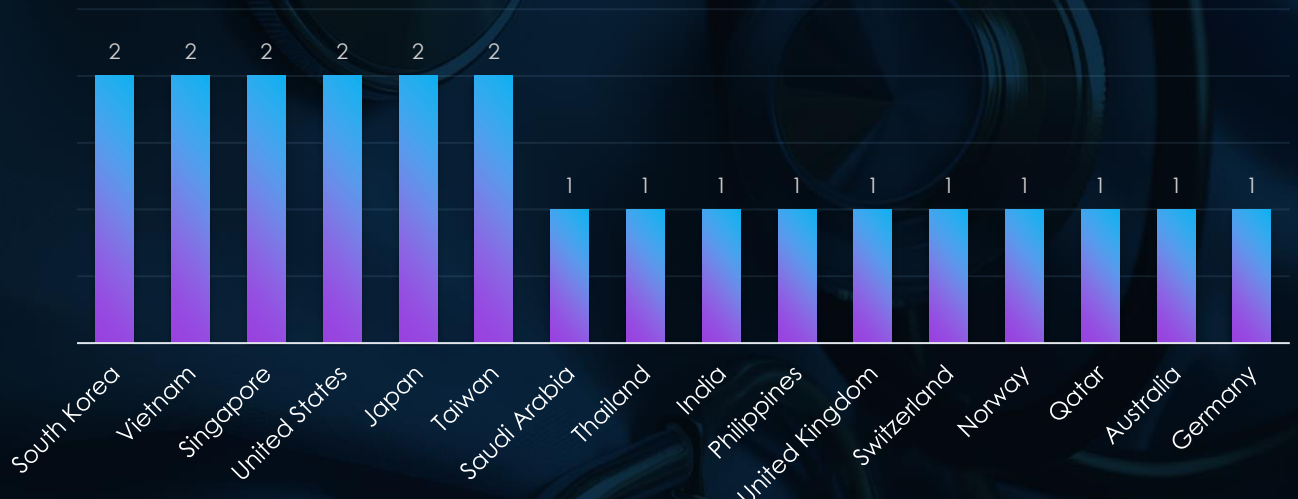
CYFIRMA
DECODING THREATS

APT CAMPAIGNS - HEALTHCARE

SUSPECTED THREAT ACTORS

The healthcare industry faces targeted threats from both nation-state and financially motivated actors. Fancy Bear (Russia) likely targets the sector for espionage and intelligence gathering, while Mustang Panda (China) focuses on geopolitical objectives. Lazarus Group (North Korea) represents a blend of financial motivation and state funding, while TA505 highlights the profit-driven cybercrime targeting healthcare's sensitive data. This mix of motivations underscores the sector's dual vulnerability to both espionage and financial exploitation.

GEOGRAPHICAL DISTRIBUTION

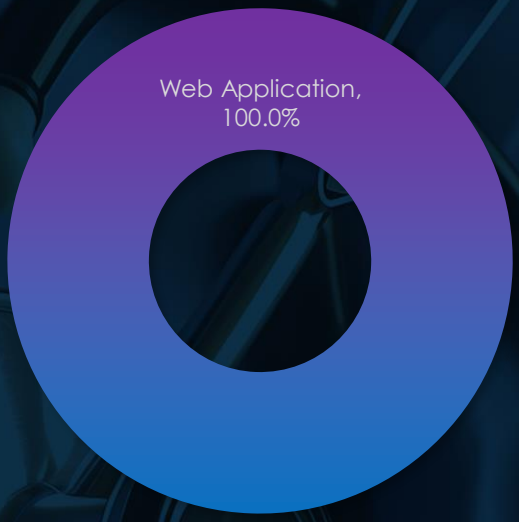


Nations like South Korea, Japan, Taiwan, and the United States are primary targets, highlighting their advanced healthcare infrastructure and valuable data. Meanwhile, countries such as Vietnam, Singapore, and India indicate a growing interest in the Asia-Pacific region. The inclusion of smaller nations like Norway, Qatar, and Saudi Arabia demonstrates the global nature of healthcare threats.

CYFIRMA
DECODING THREATS

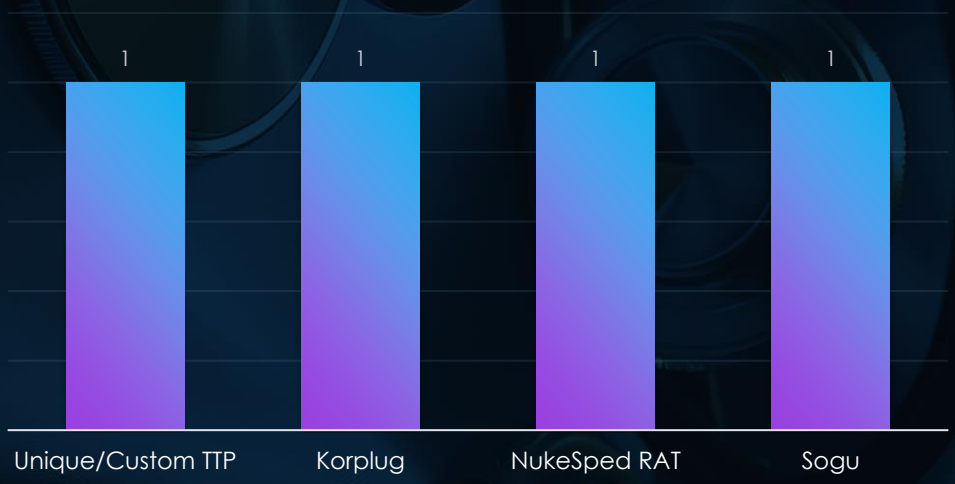
APT CAMPAIGNS - HEALTHCARE

TOP ATTACKED TECHNOLOGY



The healthcare industry's top targeted technology is web applications, reflecting their critical role in modern healthcare operations. As internet-facing systems, they are particularly vulnerable to exploitation, offering attackers access to sensitive patient data and operational systems.

TOP MALWARE



The malware targeting the healthcare industry highlights a mix of custom tools and well-known strains. Unique/Custom TTPs reflect attackers' tailored approaches to compromising healthcare systems.

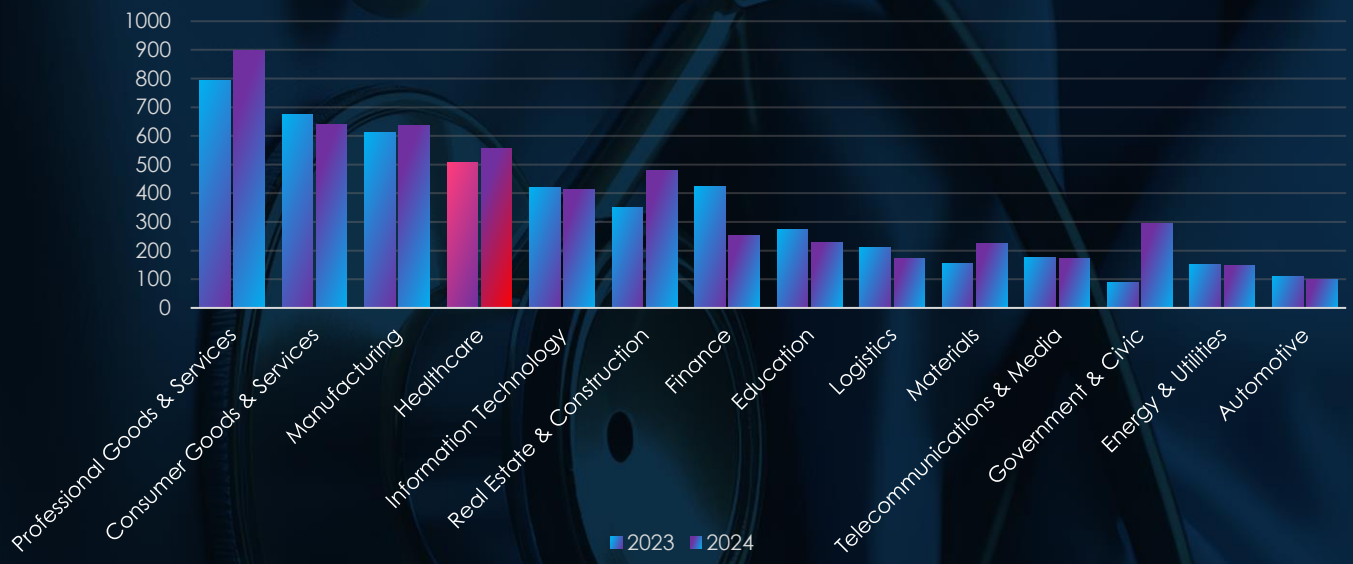
Korplug, NukeSped RAT, and Sogu emphasize espionage and data theft, aligning with the attackers' goals of accessing sensitive patient records and critical operational information.

CYFIRMA
DECODING THREATS

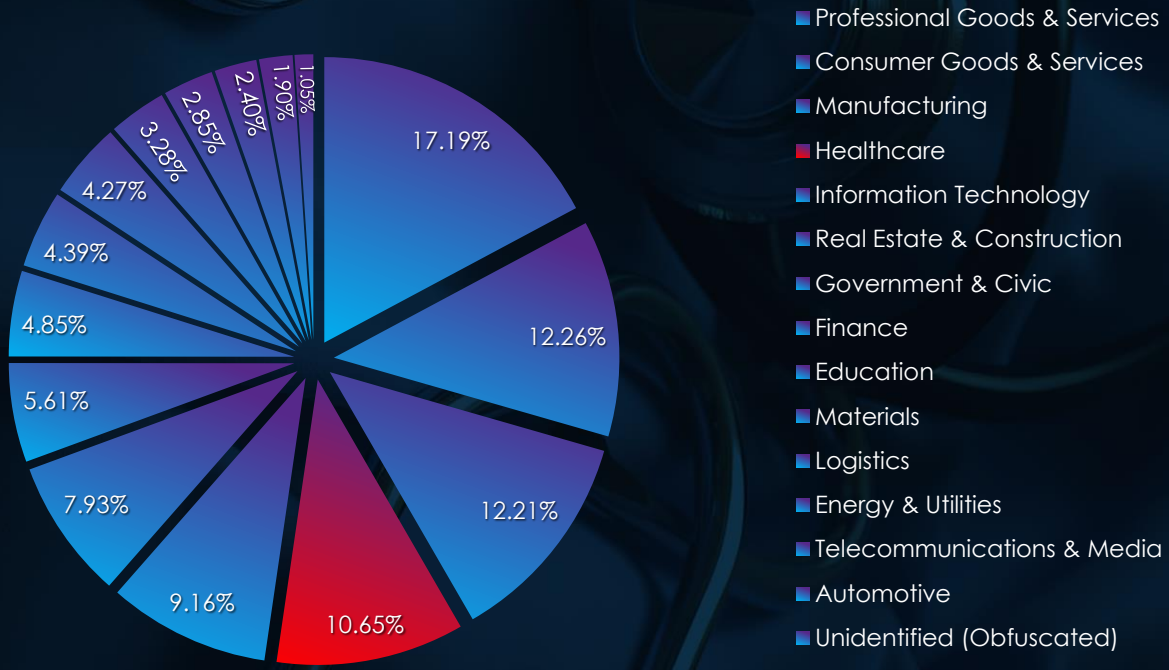
RANSOMWARE VICTIMOLOGY HEALTHCARE

In the past 12 months, CYFIRMA has identified 556 verified healthcare organization ransomware victims. This accounts for 10.65% of the overall total of 5,219 ransomware victims during the same period.

GLOBAL DISTRIBUTION BY INDUSTRY

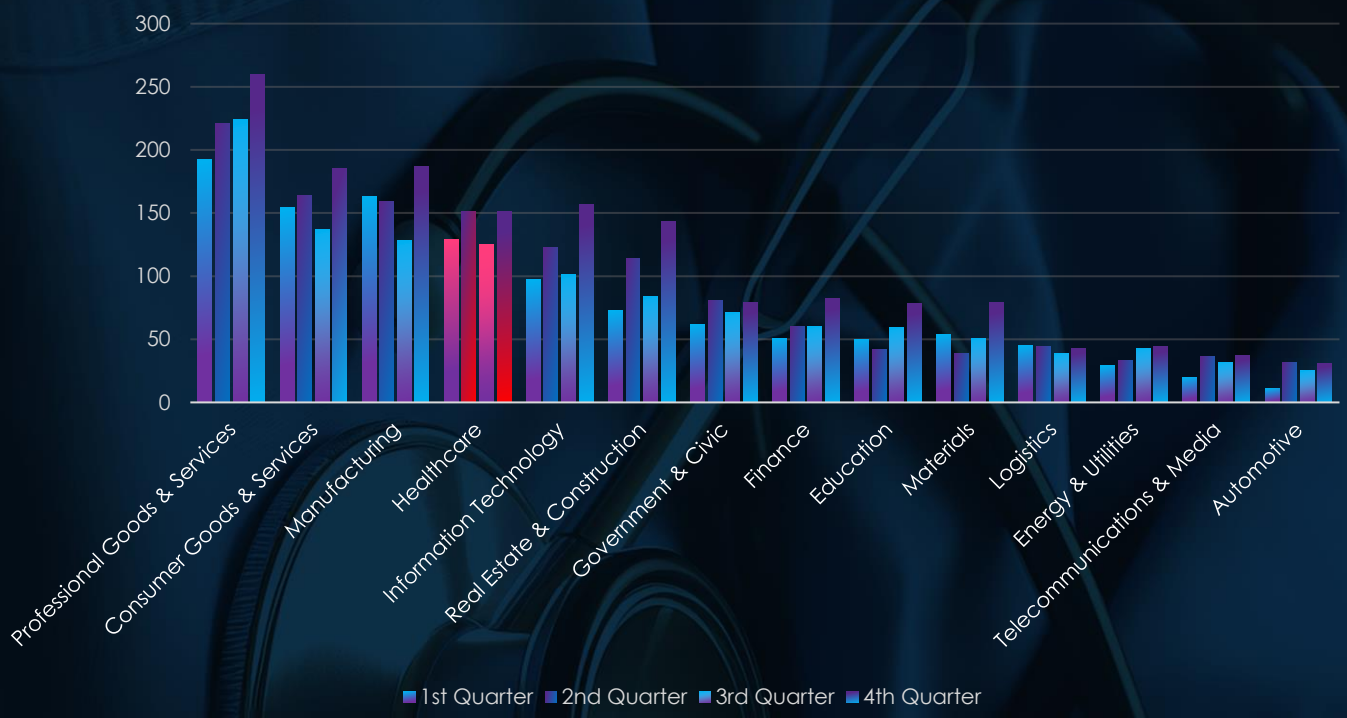


The industry recorded a substantial increase of 8.81% in recorded victims from previous year. And ranked at 4th place for combined victims in both years as well as retained 4th place in both respective years. Underlying the continued and sustained risk.



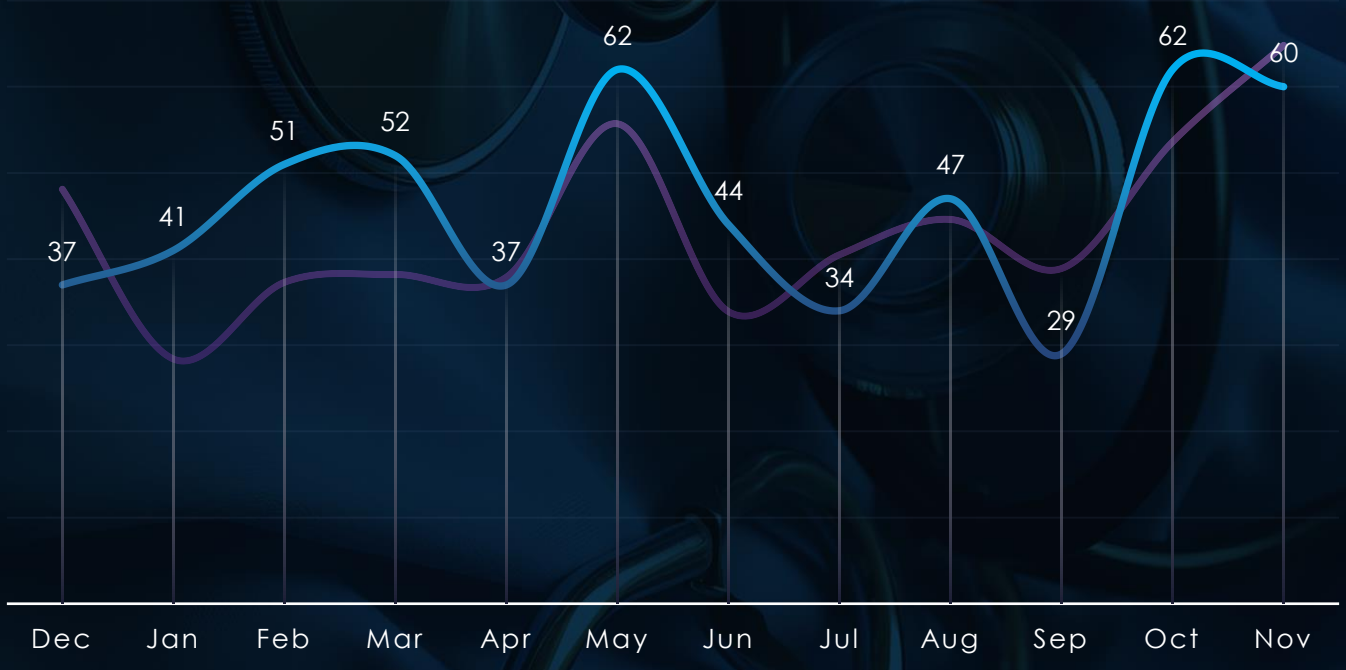
CYFIRMA
DECODING THREATS

QUARTERLY CHANGES DURING 2024



Healthcare show sustained numbers of victims. Curiously alternating nearly same numbers of victims between quarters.

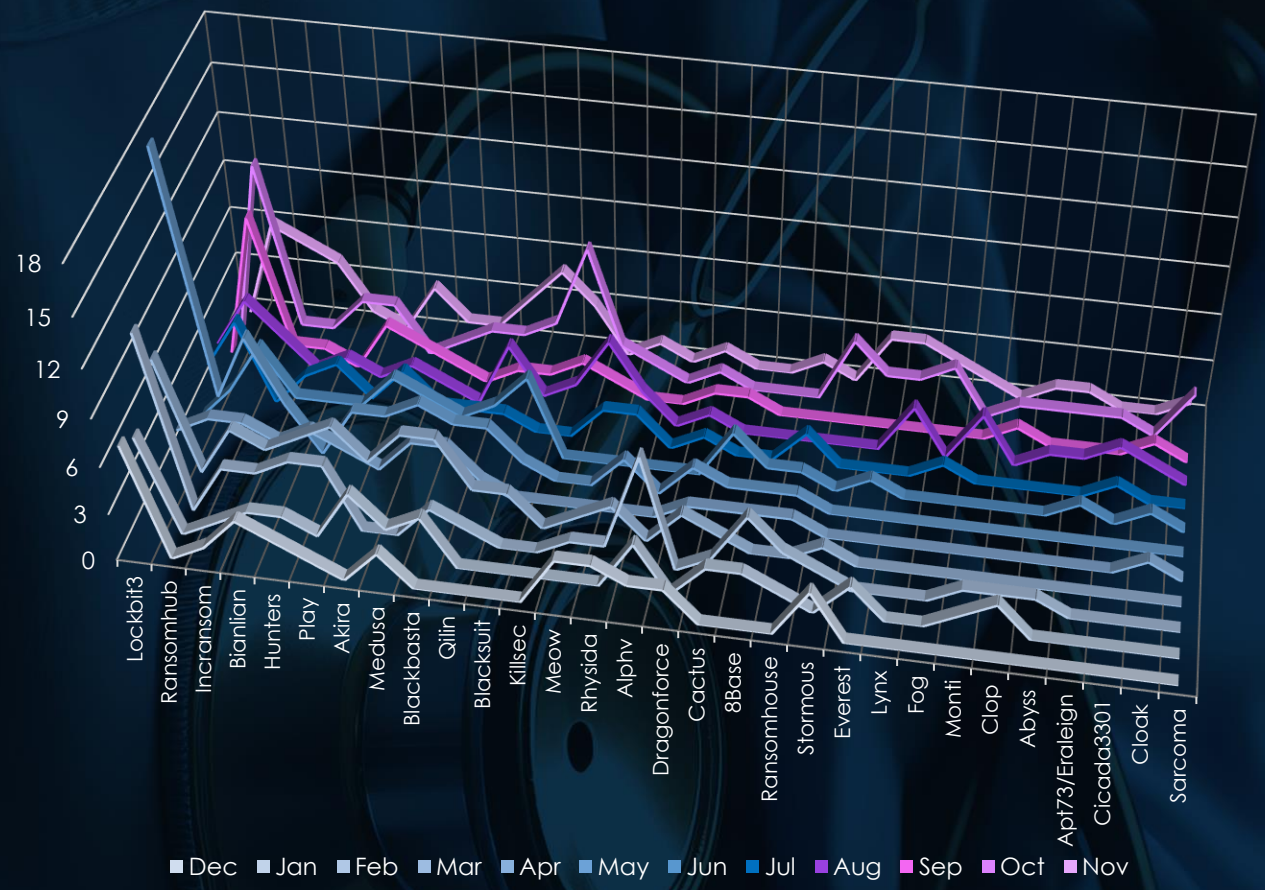
INDUSTRY MONTHLY ACTIVITY CHART



Monthly activity mostly follows the scaled down global trendline. With exception between January to March where we observed above average numbers. In October and November we see upwards trend, implying increase of activity into 2025.

CYFIRMA
DECODING THREATS

BREAKDOWN OF ACTIVITY PER GANG



In total, 77 out of 97 gangs recorded victims in the healthcare industry, with a 79% participation rate.

A breakdown of the top 30 gangs' monthly activity provides insights into which gangs were active each month.

Lockbit3 led ransomware activity, targeting 56 victims early in the year, with significant peaks in February (11 victims) and its activity waned in later months. Ransomhub followed closely with 45 victims, maintaining a steady increase in attacks from May onwards, peaking in September and October (9 and 11 victims, respectively).

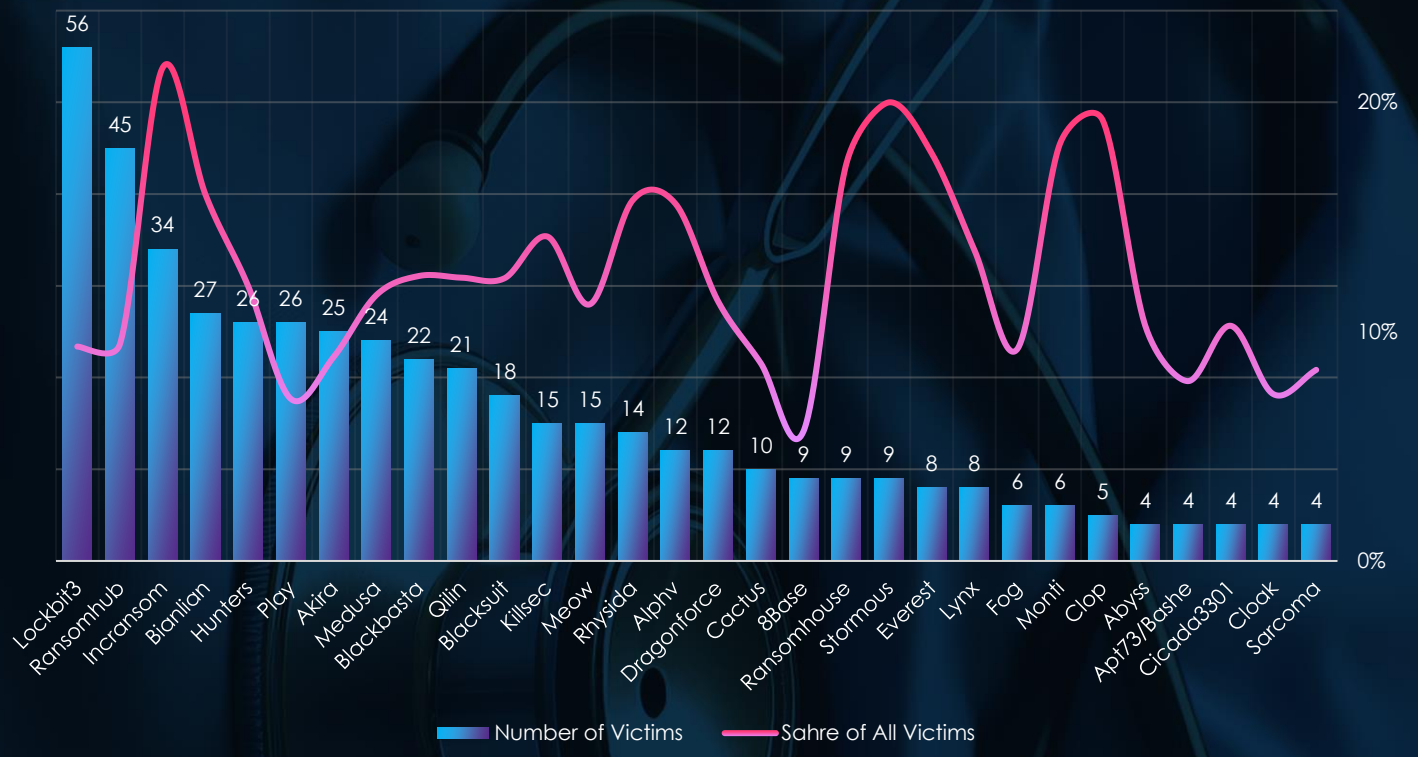
Incransom impacted 34 victims, with consistent activity peaking in May (7 victims) and sporadic surges across the year. Bianlian targeted 27 victims, with steady activity across all months and minor peaks in early and late months. Hunters and Play each accounted for 26 victims. Hunters showed even distribution throughout the year, while Play peaked in March (5 victims) and remained moderately active.

Akira targeted 25 victims, with notable spikes in January and July. Medusa, with 24 victims, concentrated its attacks in March, May, and June. Blackbasta (22 victims) was active early in the year, peaking in March and April. Qilin followed closely, targeting 21 victims with a strong presence in July and October.

Smaller groups like Blacksuit (18 victims), Killsec, and Meow (15 each) displayed periodic activity, with Killsec peaking late in the year. Alphv and Dragonforce (12 victims each) were more active early in the year, while others, like Cactus and 8Base (10 and 9 victims, respectively), had limited but consistent campaigns.

Lesser-known groups like Fog, Monti, and Everest each targeted fewer than 10 victims, showing sporadic spikes in specific months. Sarcoma, with just four victims, was active only in October and November, indicating isolated campaigns.

INDUSTRY RANSOMWARE VICTIMS PER GANG



Closer analysis of the top 35 gangs and percentage share of victims reveals the disturbing reality of how many gangs focus on the healthcare industry, exploiting its vulnerability to operational disruptions.

Lockbit3 leads in activity within the healthcare sector, with 56 victims (9.35%). Its high number of victims suggests a deliberate but broad targeting strategy. Ransomhub follows closely, with 45 victims (9.47%), indicating significant activity in the sector. Other active gangs include Incransom (34 victims, 21.52%) and Bianlian (27 victims, 15.98%), both of which demonstrate substantial focus on healthcare.

Several gangs exhibit significant focus on the healthcare sector:

• Incransom (34 victims, 21.52%) and Bianlian (27 victims, 15.98%) show strong focus and moderate-to-high victim counts.

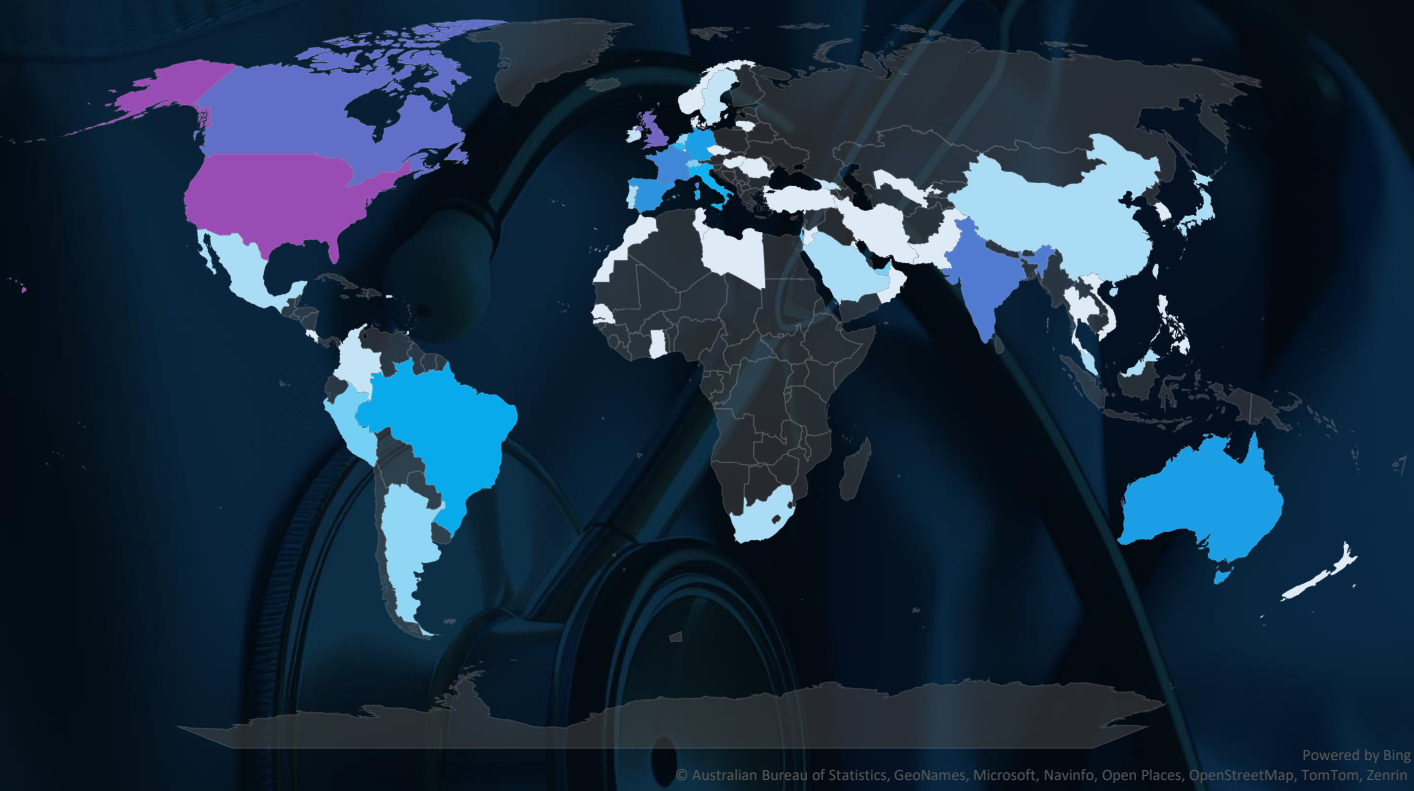
• Other gangs, such as Medusa (24 victims, 11.59%), Hunters (26 victims, 11.98%), Blackbasta (22 victims, 12.43%), Qilin (21 victims, 12.35%), and Blacksuit (18 victims, 12.33%), also display substantial activity and focus on healthcare.

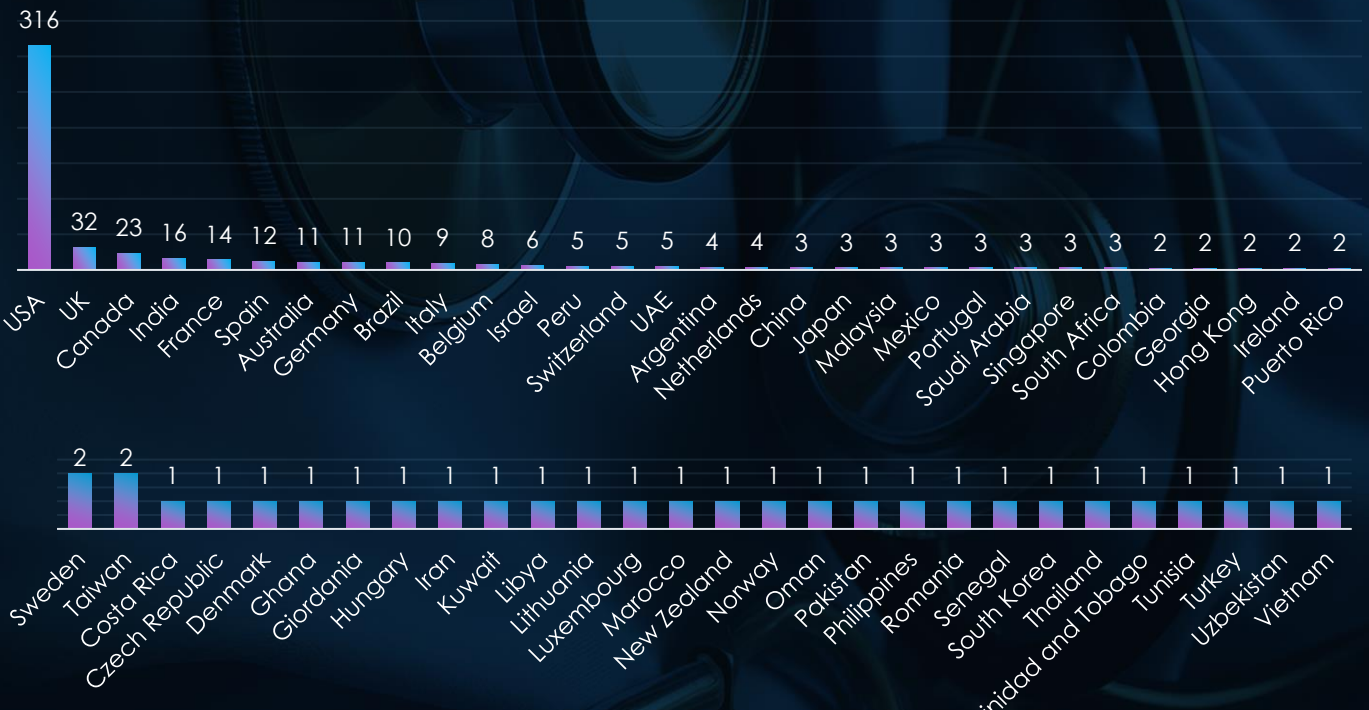
Some gangs show disproportionately high percentages due to low victim counts:

• Qiulong (3 victims, 37.50%), Donutleaks (3 victims, 30.00%), and Knight (3 victims, 25.00%) exhibit extremely high percentages driven by very small numbers of victims.

• Monti (6 victims, 18.18%), Everest (8 victims, 17.78%), and Ransomhouse (9 victims, 17.31%) similarly reflect elevated percentages with relatively lower activity in absolute terms.

GEOGRAPHIC DISTRIBUTION OF VICTIMS





The USA accounts for 57.1% of ransomware victims in the Healthcare industry in 2024. The next most affected countries are the UK with 32 victims, Canada with 23, India with 16, and France with 14.

A total of 58 countries reported victims, with 27 of them having only one victim each.

CYFIRMA
DECODING THREATS

HEALTHCARE INDUSTRY EXTERNAL THREAT LANDSCAPE MANAGEMENT (ETLM) OVERVIEW

Risk Level Indicator: Low/High

APT Campaigns

The healthcare industry experienced a low 6% incidence rate across observed APT campaigns, driven by both espionage and financially motivated actors. Groups like Fancy Bear and Mustang Panda focus on intelligence and geopolitical goals, while Lazarus and TA505 target financial gain and sensitive data. Key targets include nations with advanced healthcare systems and growing interest in Asia-Pacific regions.

Actors: Fancy Bear, Mustang Panda, Lazarus Group, TA505.

Geographic Focus: U.S., Japan, South Korea; emerging targets in Vietnam, Singapore, and India.

Targets: Web applications are primary, exposing patient data and operational systems.

Malware: Korplug, NukeSped RAT, Sogu, emphasizing espionage and data theft.

Ransomware

The healthcare sector accounted for 556 ransomware victims in the past year (10.65% of global total), with sustained activity and spikes in early 2024. LockBit 3 led in volume but faced setbacks, while RansomHub and other gangs exploited the sector's critical vulnerabilities. Healthcare organizations remain a top target due to their susceptibility to operational disruptions.

Victim Trends: Alternating quarterly activity; spikes in Q1, October, and November.

Key Actors: LockBit 3, RansomHub, Inc Ransom (21.52% of victims), Alphv, and Killsec.

Geography: U.S. accounted for 57% of victims, with activity in 59 countries.

Ranking: Healthcare ranked 4th globally for ransomware targeting.

CYFIRMA
DECODING THREATS

LOGISTICS INDUSTRY IN 2024

ADVANCED PERSISTENT THREATS

Over the past 12 months, logistics organizations recorded victims across 8 of the 34 Advanced Persistent Threat (APT) campaigns observed - an incidence rate of 24%.

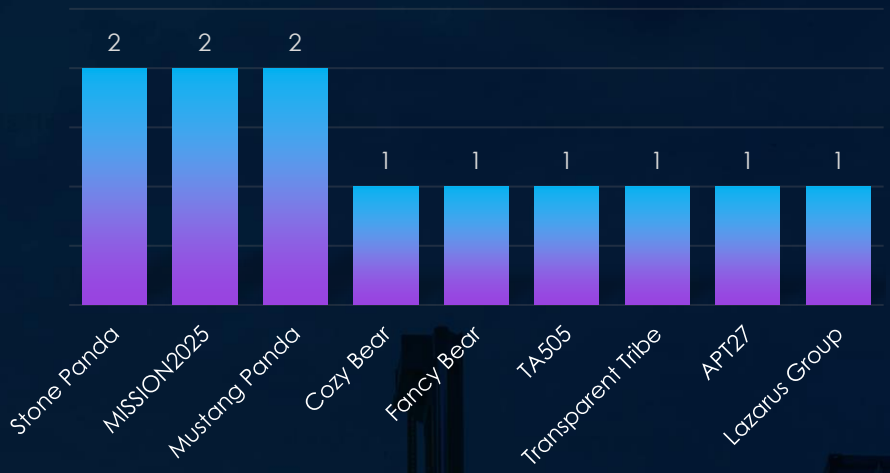
These victims spanned multiple segments within the logistics industry as shown below:

OBSERVED CAMPAIGNS PER MONTH

CYFIRMA
DECODING THREATS

APT CAMPAIGNS - LOGISTICS

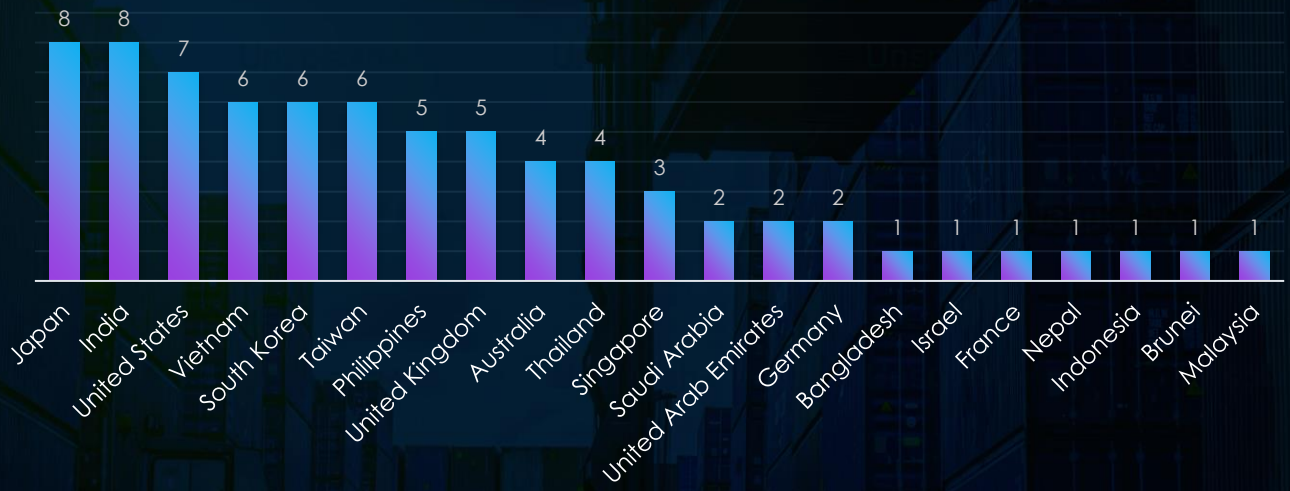
SUSPECTED THREAT ACTORS



The logistics industry is targeted by a mix of nation-state and financially motivated threat actors. Stone Panda, Mustang Panda, and MISSION2025, all linked to Chinese interests, focus on espionage and data theft, likely seeking supply chain intelligence.

Cozy Bear and Fancy Bear (Russia) reflect geopolitical motives, targeting logistics for strategic disruption or intelligence gathering. Lazarus Group (North Korea) blends financial objectives with state-sponsored motives, while TA505 represents profit-driven attacks, often aimed at ransomware and data extortion.

GEOGRAPHICAL DISTRIBUTION



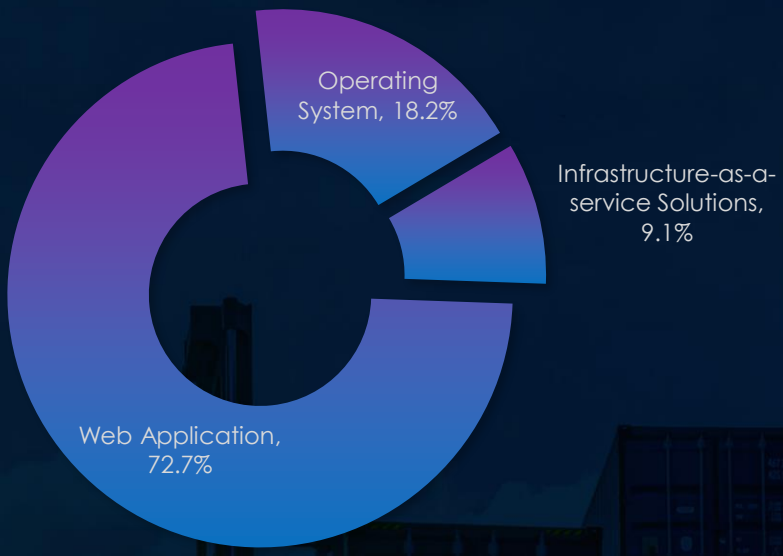
The geographic distribution of APT campaigns targeting the logistics industry reflects its global importance, with a strong focus on Asia and advanced economies. Japan and India lead, highlighting their role as major logistics hubs in the region, followed closely by the United States.

Vietnam, South Korea, and Taiwan further demonstrate the emphasis on Asia-Pacific, where logistics systems are vital to regional and global supply chains. Emerging economies like the Philippines and Thailand also show significant activity, while the inclusion of smaller nations like Nepal, Bangladesh, and Brunei underscores the expanding scope of attacks, targeting both major and developing logistics infrastructures worldwide.

CYFIRMA
DECODING THREATS

APT CAMPAIGNS - LOGISTICS

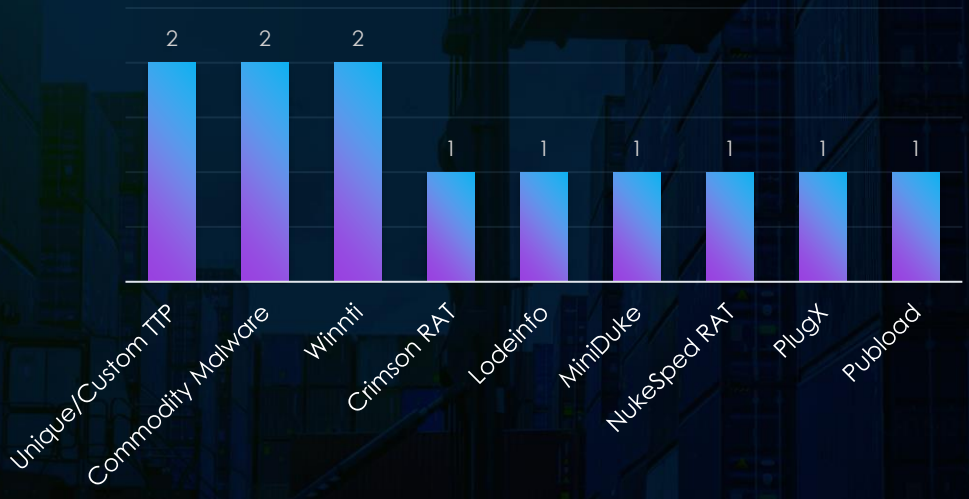
TOP ATTACKED TECHNOLOGY



The logistics industry's most targeted technologies highlight attackers' focus on critical systems. Web applications dominate, reflecting their vulnerability as internet-facing systems integral to logistics operations.

Operating systems are also key targets, emphasizing attackers' focus on foundational technologies critical for system functionality. Additionally, infrastructure-as-a-service solutions appear as a target, underscoring the importance of cloud-based systems in modern logistics and the risks they pose if compromised.

TOP MALWARE



Unique/Custom TTPs and Commodity Malware dominate, reflecting tailored approaches and accessible tools for exploiting logistics systems. Winnti highlights long-term persistence and espionage capabilities, aligning with nation-state objectives.

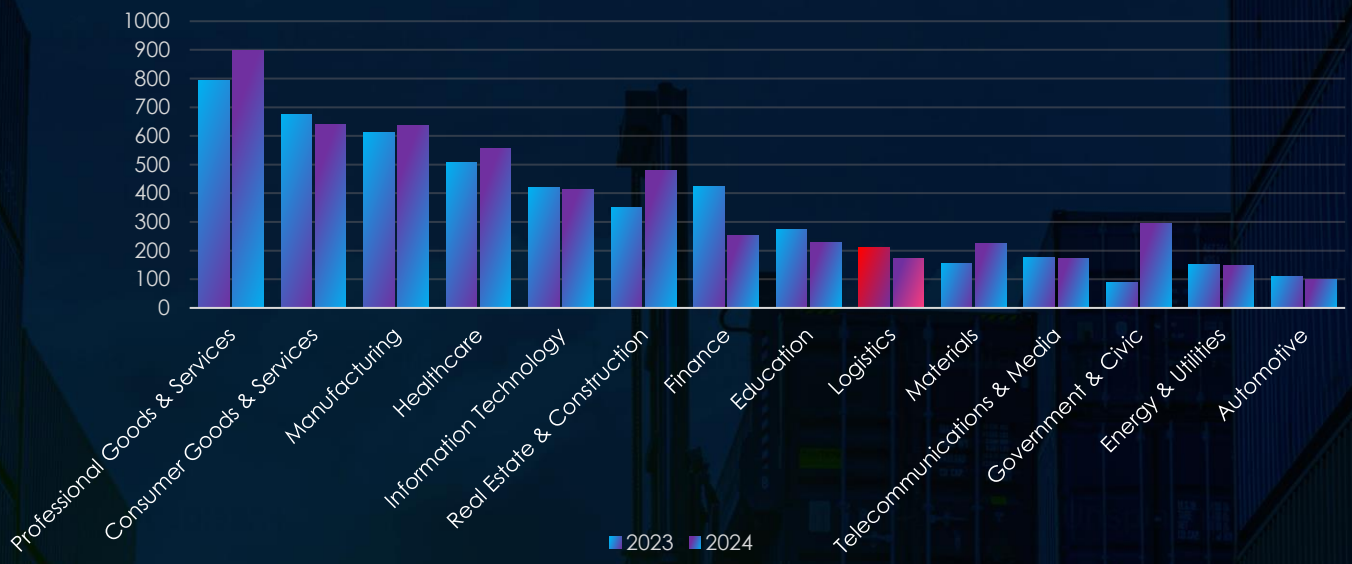
Other strains, such as Crimson RAT, PlugX, and NukeSped RAT, emphasize data theft and infiltration, while Lodeinfo and MiniDuke showcase attackers' focus on intelligence gathering.

CYFIRMA
DECODING THREATS

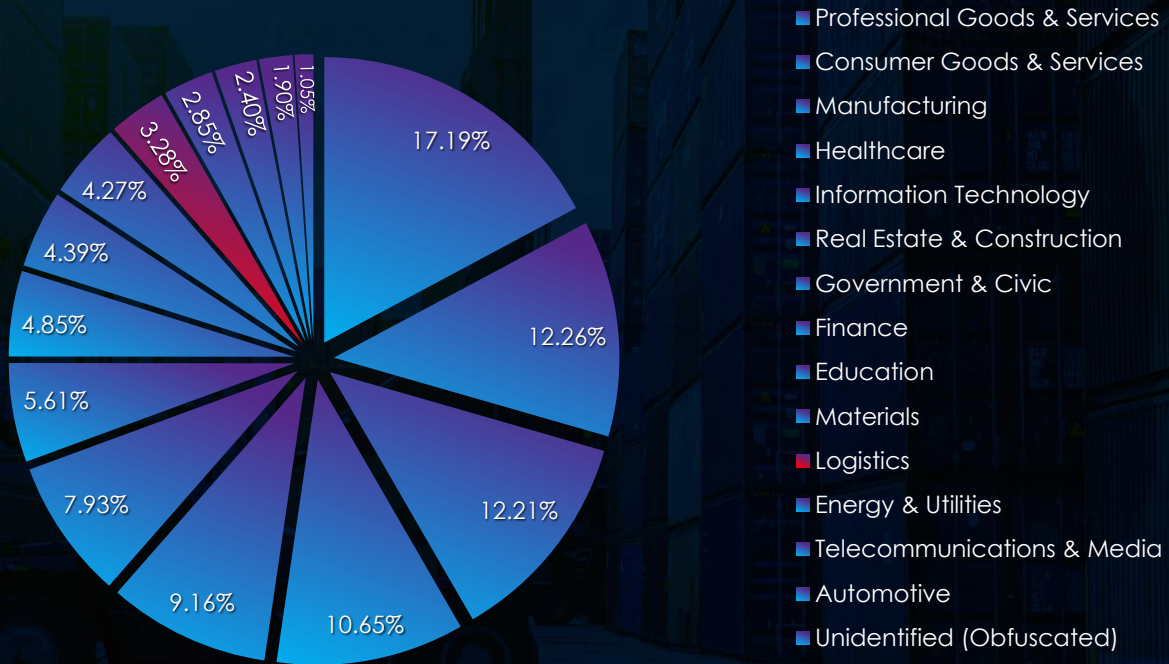
RANSOMWARE VICTIMOLOGY LOGISTICS

In the past 12 months, CYFIRMA has identified 171 verified logistics industry ransomware victims. This accounts for 3.28% of the overall total of 5,219 ransomware victims during the same period.

GLOBAL DISTRIBUTION BY INDUSTRY

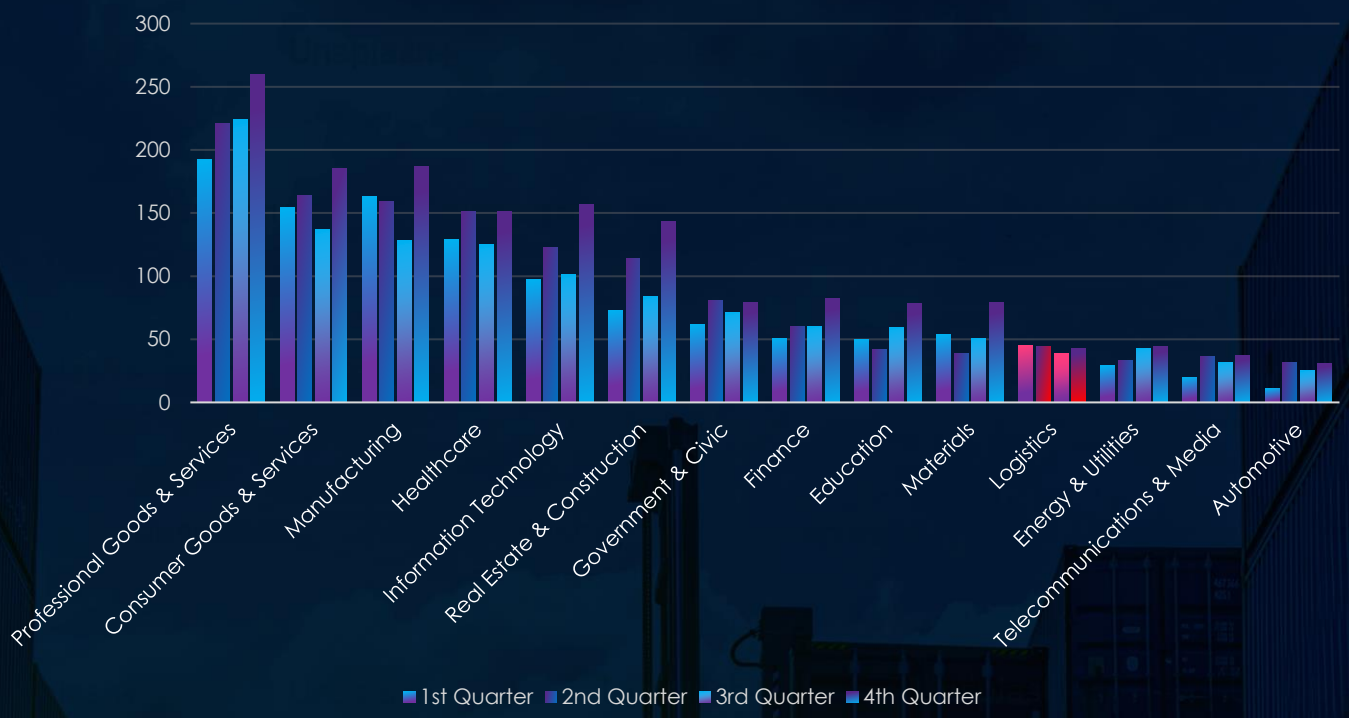


The industry recorded a significant decrease of 19.34% in recorded victims from previous year. And ranked at 9th place for combined victims in both years. For year-to-year change it dropped down from 9th to 11th place as fourth least frequent victim.



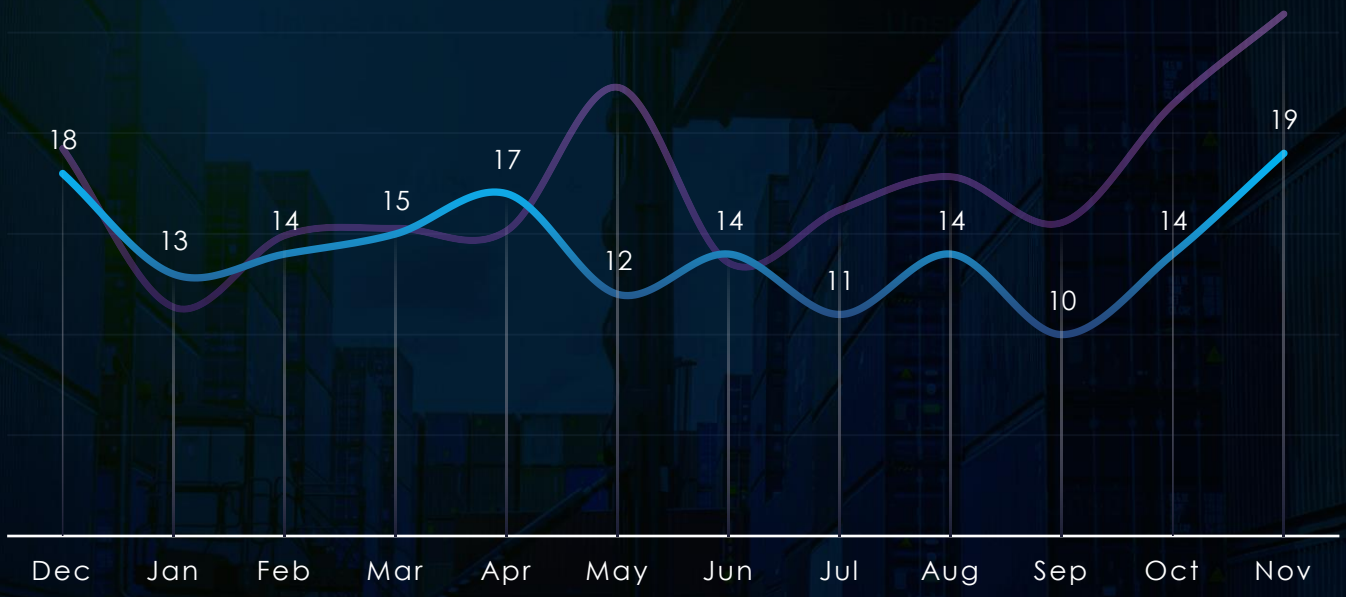
CYFIRMA
DECODING THREATS

QUARTERLY CHANGES DURING 2024



Logistics industry shows sustained numbers of victims across all four quarters. Only minor dip occurring during 3rd quarter.

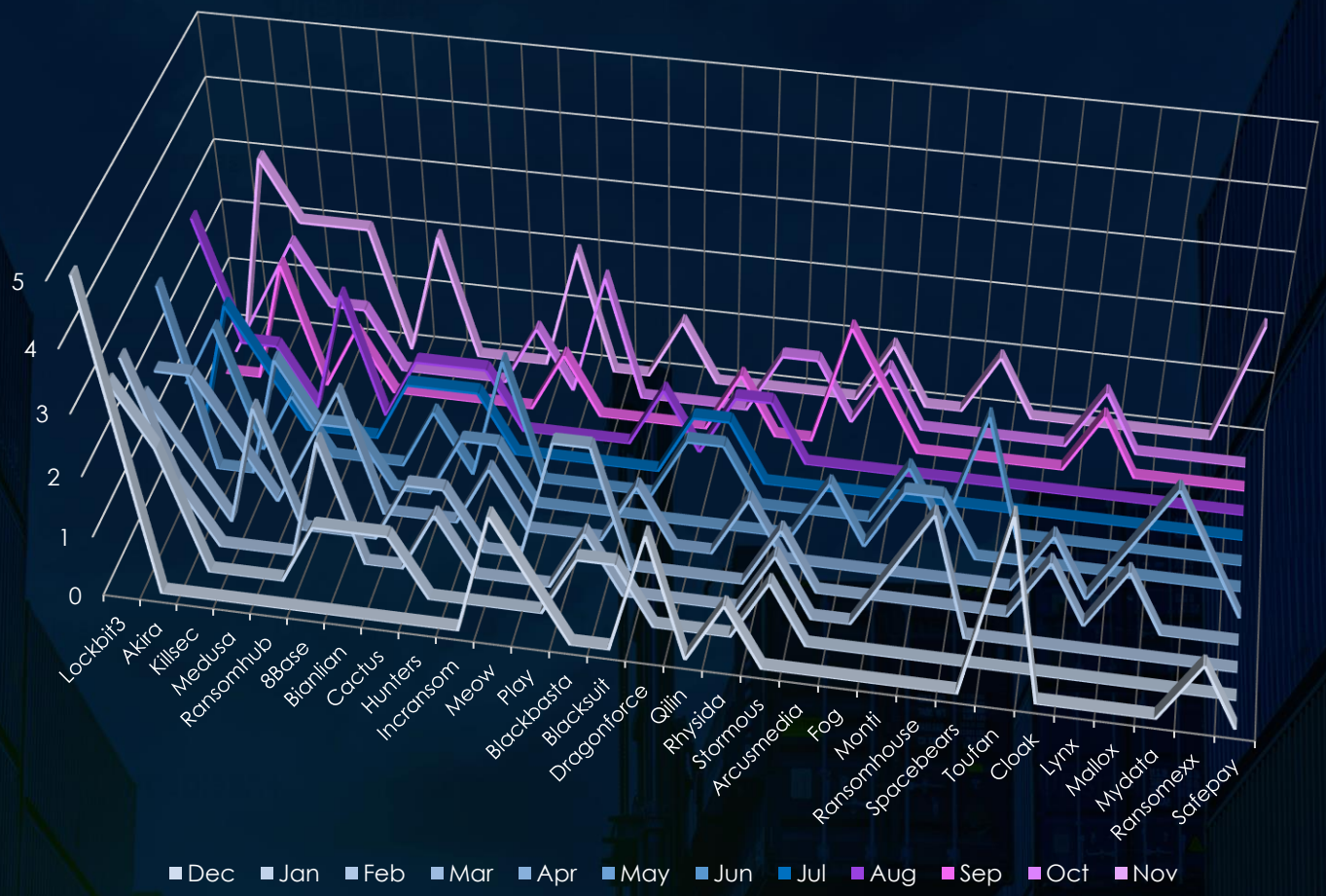
INDUSTRY MONTHLY ACTIVITY CHART



Monthly activity mostly follows the scaled down global trendline. However, starts falling off from May, where Logistics industry did not experience the global spike and have been the average line for the rest of the year. Though October and November recorded significant growth and imply uptick into 2025.

CYFIRMA
DECODING THREATS

BREAKDOWN OF ACTIVITY PER GANG



In total 49 out of 97 gangs recorded victims in logistics industry, 51% participation.

A breakdown of top 30 gang's monthly activity provides insights into which gangs were active each month.

Lockbit3 led ransomware activity, targeting 22 victims. Akira followed with 15 victims, showing concentrated activity in January, June, July, and a spike in November (3 victims).

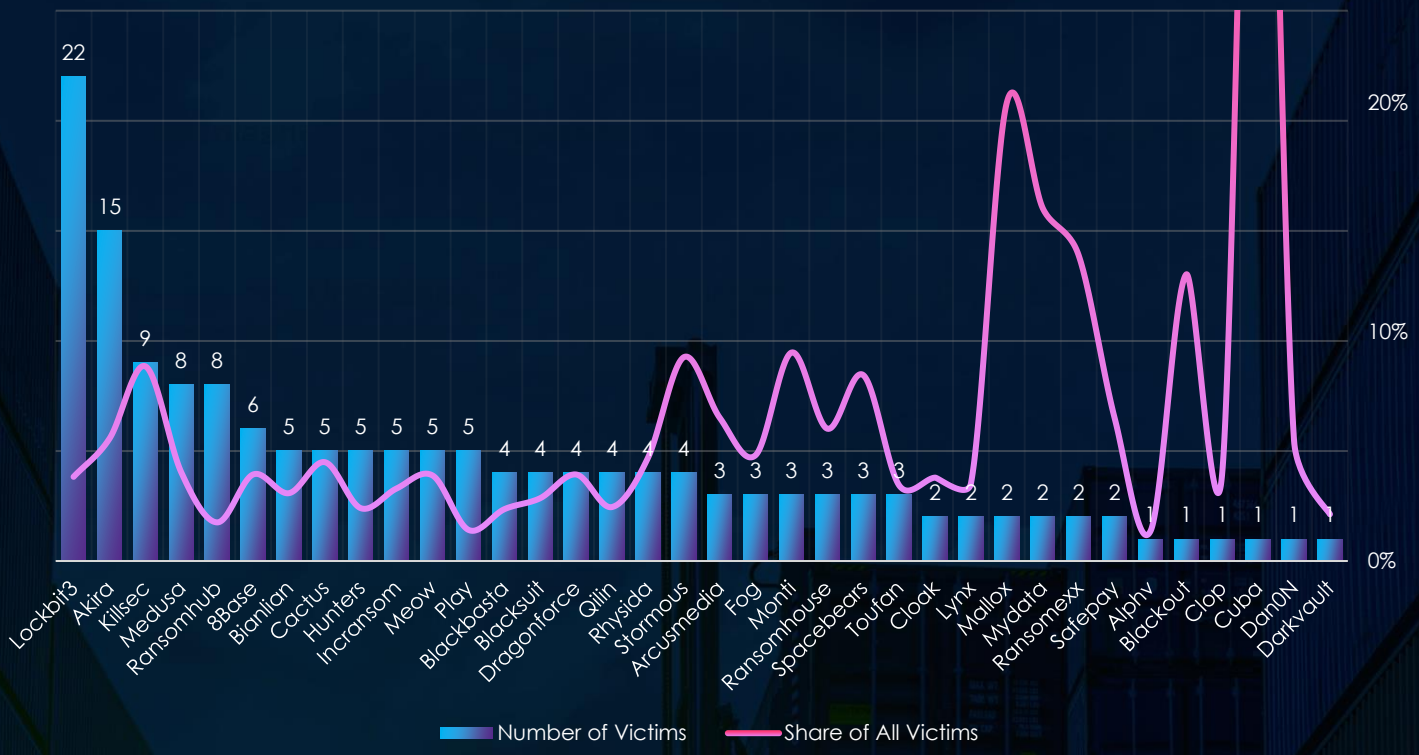
Killsec and Medusa each targeted 9 and 8 victims, respectively, with Killsec peaking in September and October, and Medusa active in March, May, and November. Ransomhub also impacted 8 victims, focusing primarily on later months like August, October, and November.

8Base targeted 6 victims, with most activity in February and April. Several groups, including Bianlian, Cactus, Hunters, Incransom, Meow, and Play, each impacted 5 victims, with scattered campaigns throughout the year. Notably, Meow peaked in December with two attacks, and Play surged in October.

Smaller groups like Blackbasta, Blacksuit, Dragonforce, Qilin, and Rhysida each targeted 4 victims, with Qilin showing steady activity from July to October and Dragonforce active early in the year. Stormous also targeted 4 victims, focusing on early and mid-year months.

Emerging gangs such as Arcusmedia, Fog, Monti, Spacebears, and Toufan had minimal activity, each targeting 3 victims or fewer. Groups like Mydata, Ransomexx, and Safepay were the least active, with isolated campaigns primarily in the first half of the year.

INDUSTRY RANSOMWARE VICTIMS PER GANG



Reviewing top 35 active gangs, Lockbit3 is the most active gang targeting logistics, with 22 victims (3.67%), demonstrating broad activity but not a specific focus on this sector. Akira, with 15 victims (5.34%), and Killsec, with 9 victims (8.49%), show moderate activity and a more concentrated effort within logistics. Other active gangs include Medusa (8 victims, 3.86%) and Ransomhub (8 victims, 1.68%), both with modest targeting of the logistics industry.

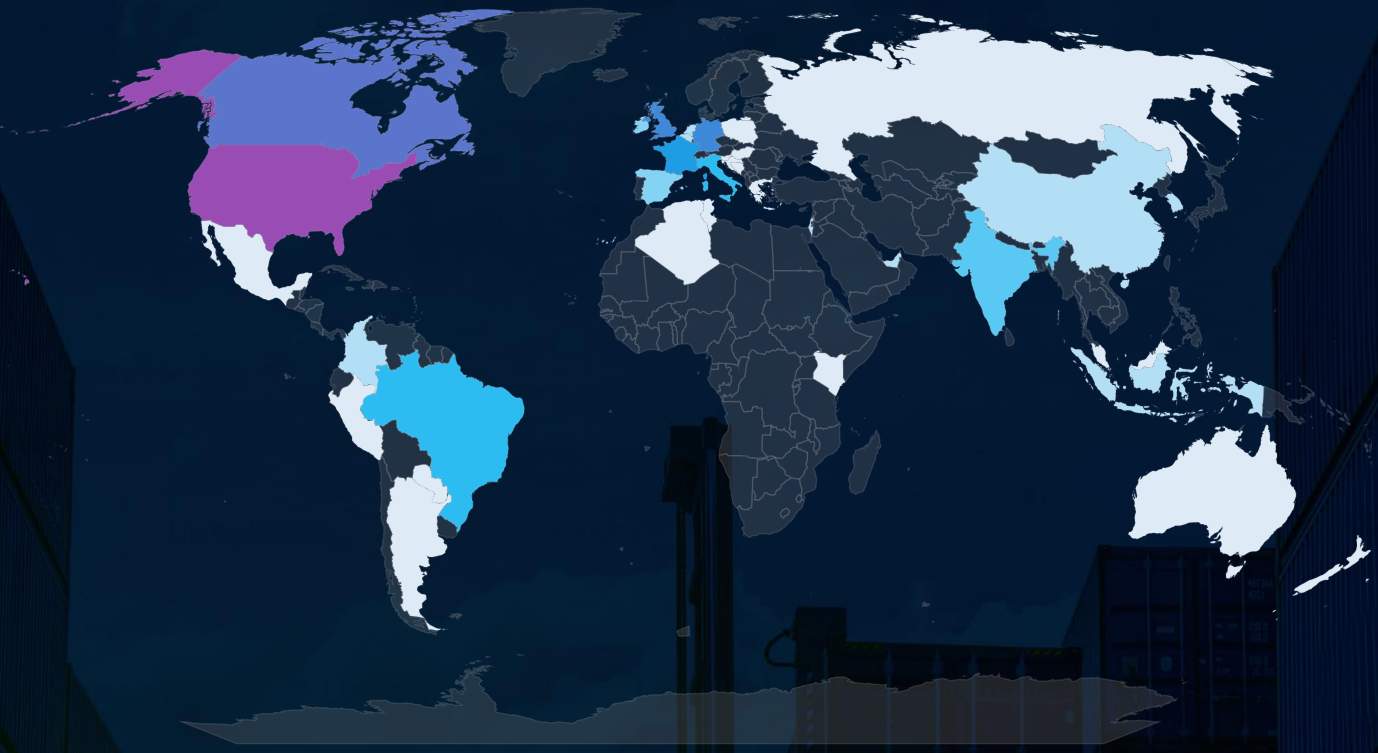
Several gangs display significant focus on logistics, though with varying victim counts:

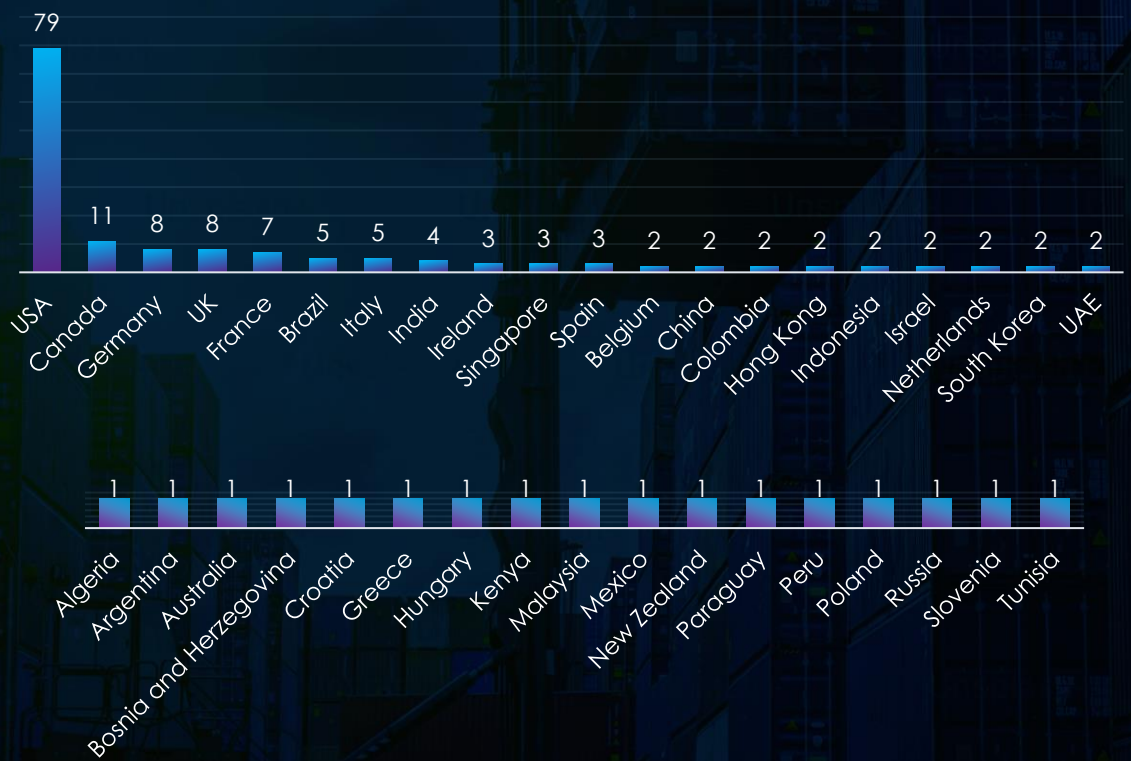
- Killsec (9 victims, 8.49%), Stormous (4 victims, 8.89%), and Monti (3 victims, 9.09%) demonstrate notable targeting efforts relative to their overall activity.
- Arcusmedia (3 victims, 6.25%), Ransomhouse (3 victims, 5.77%), and Spacebears (3 victims, 8.11%) reflect moderate levels of targeting with meaningful focus.

Some gangs show disproportionately high percentages due to low victim counts:

- Cuba (1 victim, 50.00%) is an extreme outlier, as the high percentage reflects a single incident rather than sustained activity.
- Mallox (2 victims, 20.00%), Mydata (2 victims, 15.38%), and Ransomexx (2 victims, 13.33%) also display exaggerated focus due to their minimal numbers of victims.
- Blackout (1 victim, 12.50%) represents a similar case, where a single incident skews the percentage.

GEOGRAPHIC DISTRIBUTION OF VICTIMS





The USA accounts for 46.2% of ransomware victims in the Logistics industry in 2024. The next most affected countries are Canada with 11 victims, the UK with 8, Germany with 8, and France with 7.

A total of 37 countries reported victims, with 17 of them having only one victim each.

CYFIRMA
DECODING THREATS

LOGISTICS INDUSTRY EXTERNAL THREAT LANDSCAPE MANAGEMENT (ETLM) OVERVIEW

Risk Level Indicator: Moderate

APT Campaigns

The logistics industry recorded a 24% incidence rate across observed APT campaigns, driven by nation-state espionage and financially motivated attacks. Groups like Stone Panda and Mustang Panda (China) target supply chain intelligence, while Cozy Bear and Fancy Bear (Russia) pursue strategic disruption. Lazarus (North Korea) and TA505 blend financial motives with state-sponsored agendas. Key targets include Asia-Pacific logistics hubs and advanced economies.

Actors: Stone Panda, Mustang Panda, Cozy Bear, Fancy Bear, Lazarus, TA505.

Geographic Focus: Japan, India, U.S.; activity in Vietnam, South Korea, Taiwan, and emerging markets like Thailand and the Philippines.

Targets: Web applications, operating systems, and IaaS solutions critical to logistics.

Malware: Winnti, Crimson RAT, PlugX, NukeSped RAT, Lodeinfo, MiniDuke.

Ransomware

The logistics sector accounted for 171 ransomware victims (3.28% of global total), with a -19.34% year-over-year decrease. Activity was consistent across quarters, except for a slight Q3 dip. October and November showed significant growth, indicating potential escalation into 2025. Lockbit3 led in volume, but smaller gangs like Killsec and Cuba also demonstrated significant focus.

Victim Trends: Stable activity; growth in October/November.

Key Actors: LockBit 3, Akira, Killsec (8.49% of victims), RansomHub, Cuba (50% of its victims in logistics).

Geography: U.S. accounted for 46% of victims; activity recorded in 37 countries.

Ranking: Logistics ranks 11th globally for ransomware targeting.

CYFIRMA
DECODING THREATS

MANUFACTURING INDUSTRY IN 2024

ADVANCED PERSISTENT THREATS

Over the past 12 months, manufacturing organizations recorded victims across 16 of the 34 Advanced Persistent Threat (APT) campaigns observed - an incidence rate of 47%.

These victims spanned multiple segments within the manufacturing industry as per below:

OBSERVED CAMPAIGNS PER MONTH

CYFIRMA
DECODING THREATS

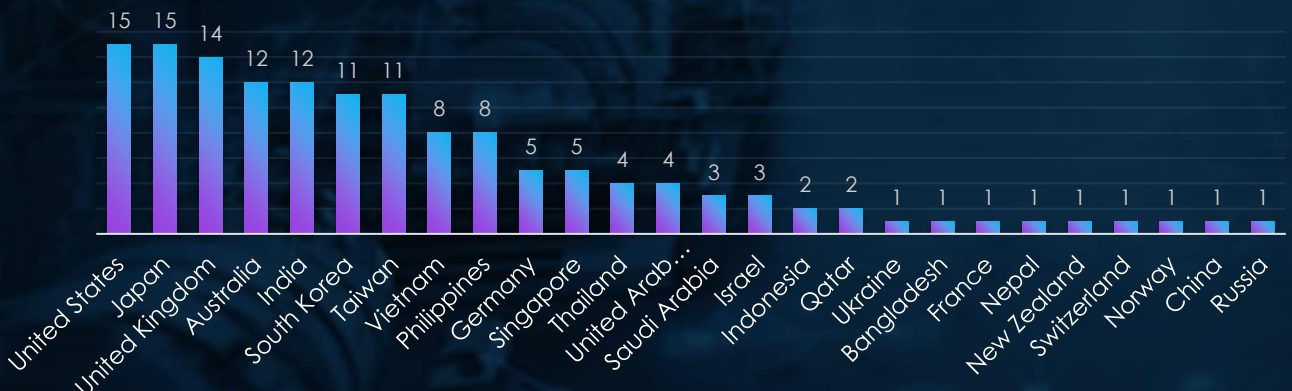
APT CAMPAIGNS - MANUFACTURING

SUSPECTED THREAT ACTORS

The manufacturing industry faces a mix of nation-state espionage and financially motivated threats. Groups like Lazarus Group (North Korea) and FIN7 target the sector for resource acquisition, focusing on financial gain. Nation-state actors such as MISSION2025, Mustang Panda, and Stone Panda (China) prioritize espionage and intellectual property theft, aiming to exploit advanced manufacturing technologies. Cozy Bear (Russia) and Transparent Tribe (Pakistan) align with broader geopolitical interests, incorporating manufacturing into larger intelligence-gathering efforts.

Meanwhile, emerging groups—like Unknown English-Speaking TA and Unknown Vietnamese TA—highlight the sector's growing appeal, underscoring its critical importance and vulnerability to a wide array of attackers.

GEOGRAPHICAL DISTRIBUTION

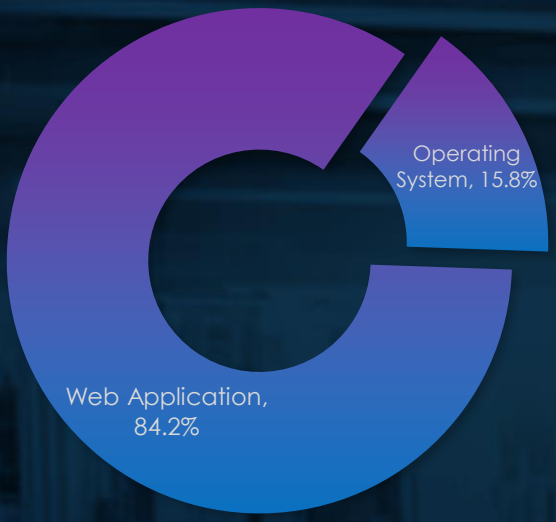


The manufacturing sector faces global APT activity, with a strong focus on industrialized nations like the United States, Japan, and the United Kingdom. Asia-Pacific countries, including India, South Korea, Taiwan, and Vietnam, are heavily targeted due to their significance in global supply chains.

Emerging economies like the Philippines and Indonesia are also increasingly targeted, while smaller nations such as Bangladesh and Nepal reflect the widening scope of attacks across both established and developing manufacturing hubs.

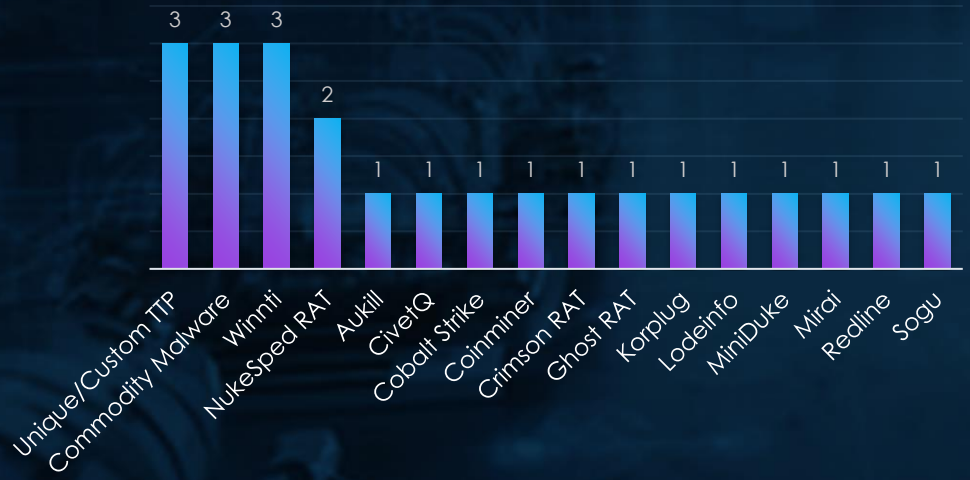
APT CAMPAIGNS - MANUFACTURING

TOP ATTACKED TECHNOLOGY



The manufacturing sector's most targeted technologies highlight attackers' focus on foundational systems. Web applications dominate, reflecting their critical role in manufacturing operations and vulnerability as internet-facing systems. Operating systems also see significant targeting, emphasizing the attackers' interest in exploiting core infrastructure to disrupt operations or gain deeper access to networks.

TOP MALWARE



The malware targeting the manufacturing sector reflects a blend of custom tools, commodity malware, and well-known strains. Unique/Custom TTPs and Commodity Malware lead, highlighting both tailored approaches and the use of readily available tools.

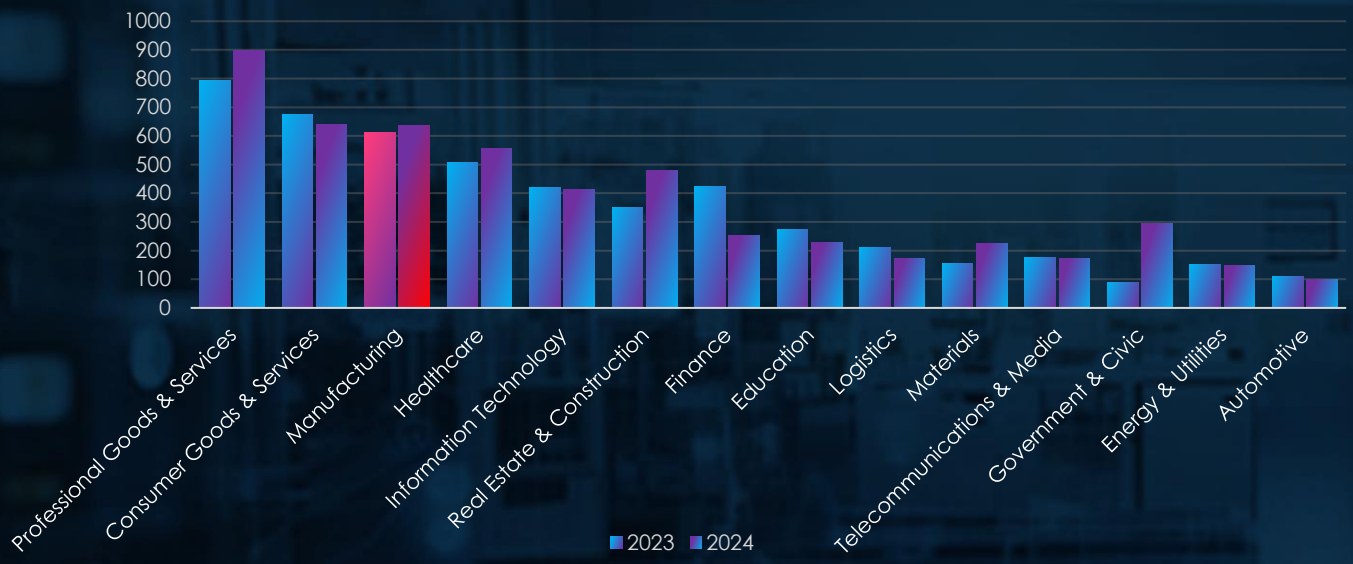
Winnti and NukeSped RAT stand out for their focus on long-term infiltration and data theft, aligning with espionage goals. Other tools, such as Cobalt Strike, Coinminer, and Korplug, demonstrate attackers' versatility in exploiting systems for both financial gain and operational disruption.

CYFIRMA
DECODING THREATS

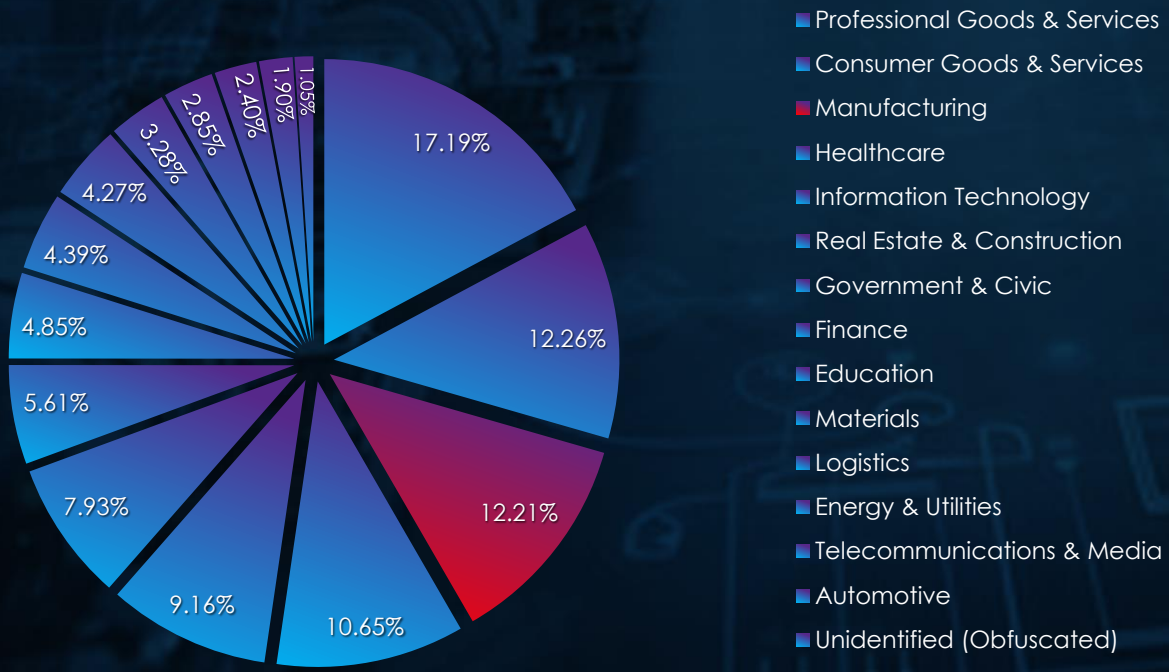
RANSOMWARE VICTIMOLOGY MANUFACTURING

In the past 12 months, CYFIRMA has identified 637 verified manufacturing industry ransomware victims. This accounts for 12.21% of the overall total of 5,219 ransomware victims during the same period.

GLOBAL DISTRIBUTION BY INDUSTRY

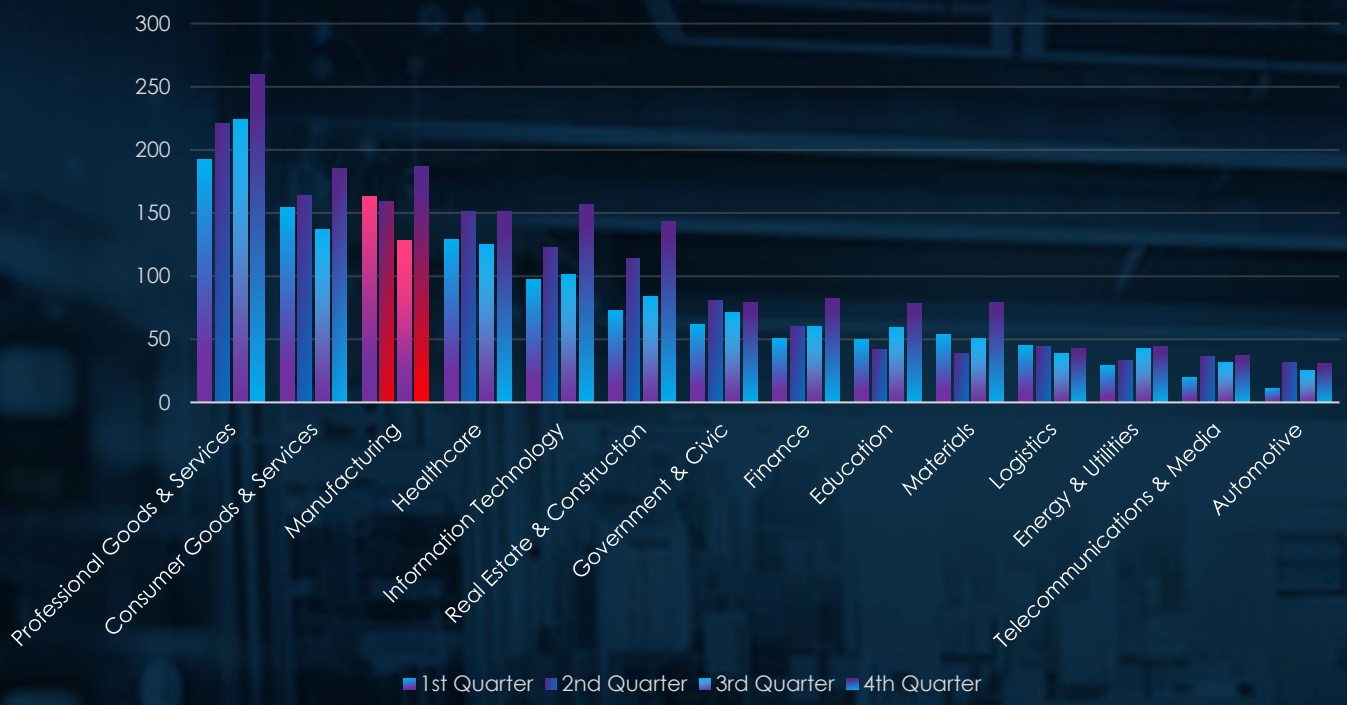


The industry recorded a mild increase of 4.08% in recorded victims from previous year. And ranked at 3rd place for combined victims in both years as well as retained 3rd place in both respective years. Underlying the continued and sustained risk.



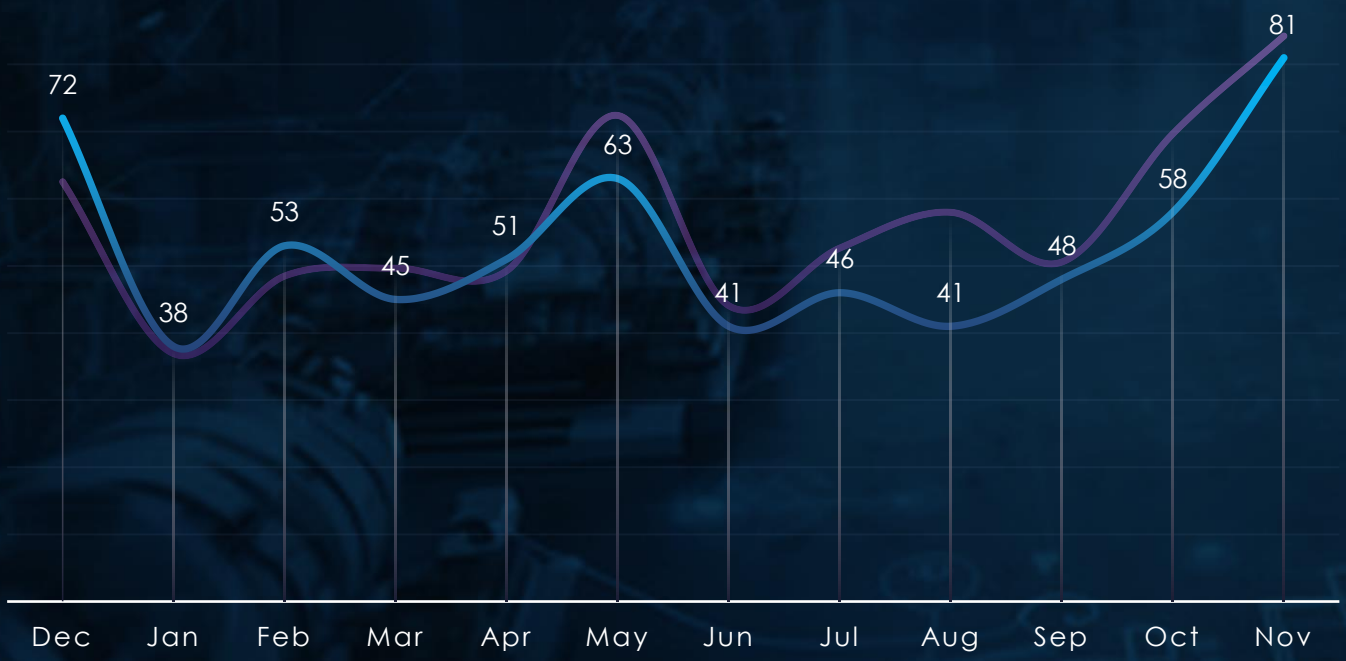
CYFIRMA
DECODING THREATS

QUARTERLY CHANGES DURING 2024



Manufacturing industry shows sustained numbers of victims across all four quarters. Notable dip occurred during 3rd quarter, however was followed with an uptick during 4th quarter.

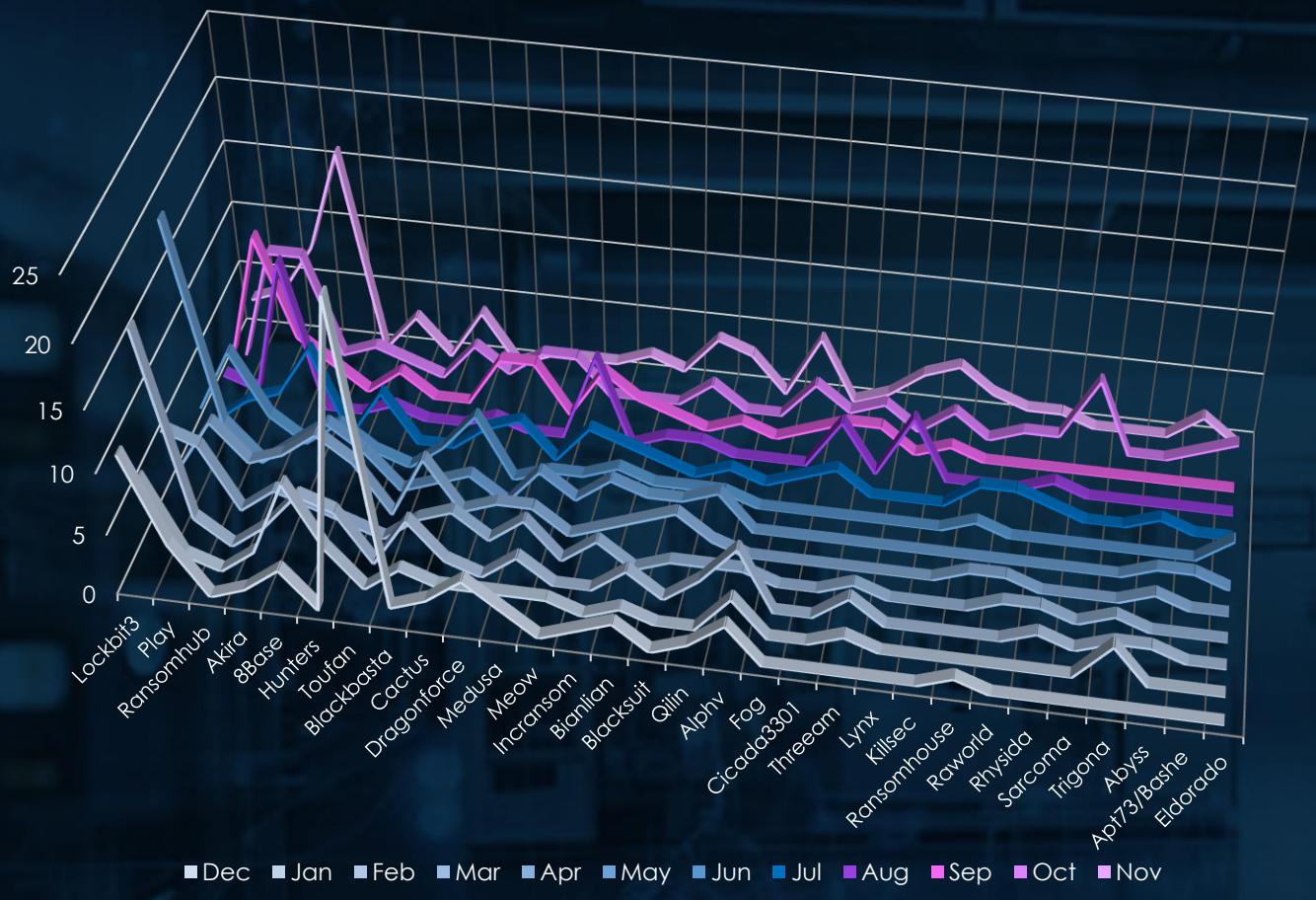
INDUSTRY MONTHLY ACTIVITY CHART



Monthly activity closely follows the scaled down global trendline. Only minor divergence was during August where industry contrary to global trend recorded minor dip. October and November recorded significant growth and imply uptick into 2025.

CYFIRMA
DECODING THREATS

BREAKDOWN OF ACTIVITY PER GANG



In total, 69 out of 97 gangs recorded victims in the manufacturing industry, with a 71% participation rate.

A breakdown of the top 30 gangs' monthly activity provides insights into which gangs were active each month.

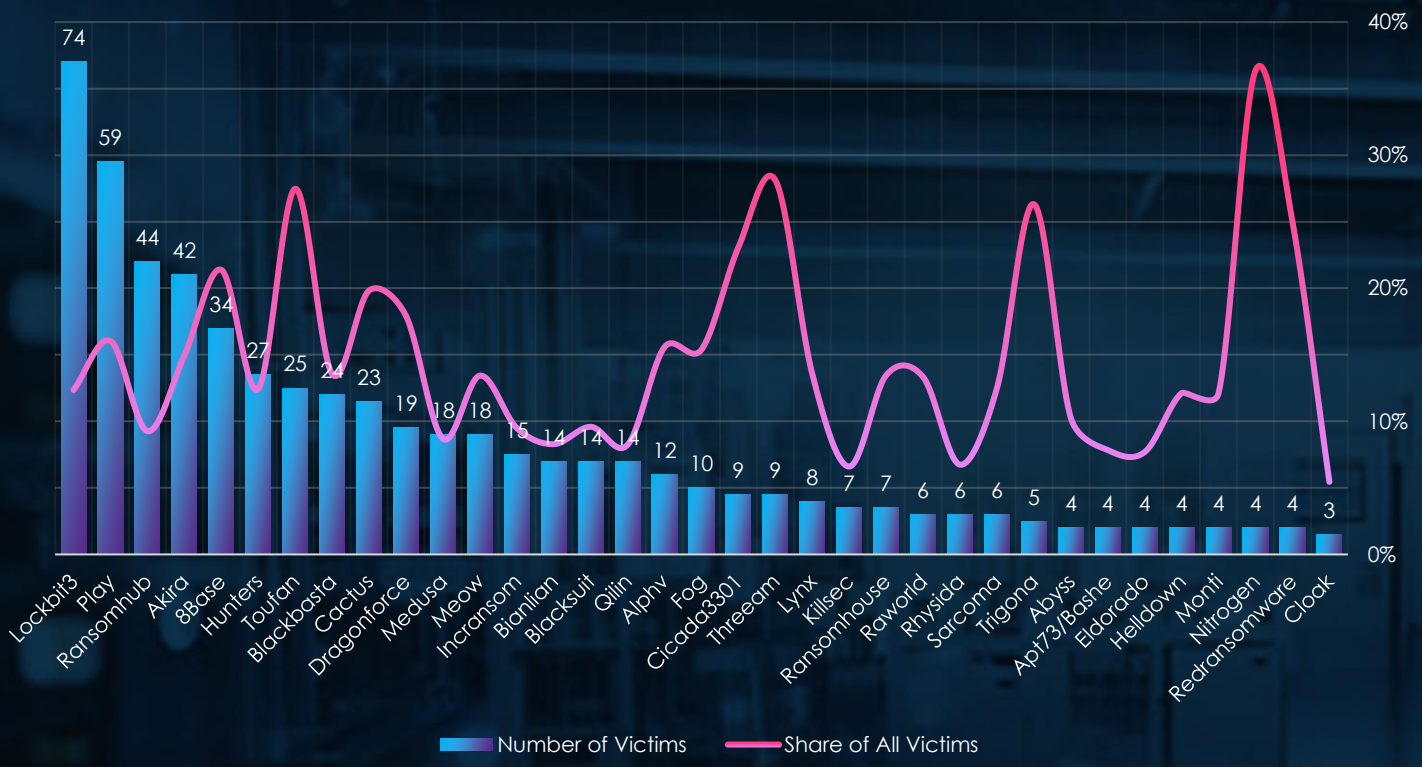
Lockbit3 led ransomware activity with 74 victims, peaking in February (17 victims) and May (20 victims). Play followed with 59 victims, spiking in September (12 victims) and October (9 victims). Ransomhub (44 victims) was most active in August, October, and November, while Akira (42 victims) peaked in July and November.

8Base (34 victims) focused on early-year campaigns, while Hunters (27 victims) maintained steady activity. Toufan published 25 victims in December and disappeared. Blackbasta (24 victims) and Cactus (23 victims) showed moderate but steady operations, with occasional peaks.

Dragonforce, Medusa, and Meow (18-19 victims each) focused on mid-to-late-year activity. Smaller groups like Incransom, Bianlian, Blacksuit, and Qilin (14-15 victims each) had scattered campaigns. Emerging actors like Fog (10 victims) and Cicada3301 (9 victims) were sporadically active, mostly late in the year.

Lockbit3 and Play drove sustained activity, while others like Ransomhub and Akira showed concentrated spikes.

INDUSTRY RANSOMWARE VICTIMS PER GANG



Analyzing top 35 active gangs, Lockbit3 leads in activity within the manufacturing sector, with 74 victims (12.35%), showing a strong focus on this industry. Play follows closely, with 59 victims (16.03%), reflecting substantial targeting. Ransomhub (44 victims, 9.26%) and Akira (42 victims, 14.95%) also show notable activity and focus in this sector. These gangs collectively dominate ransomware activity in manufacturing.

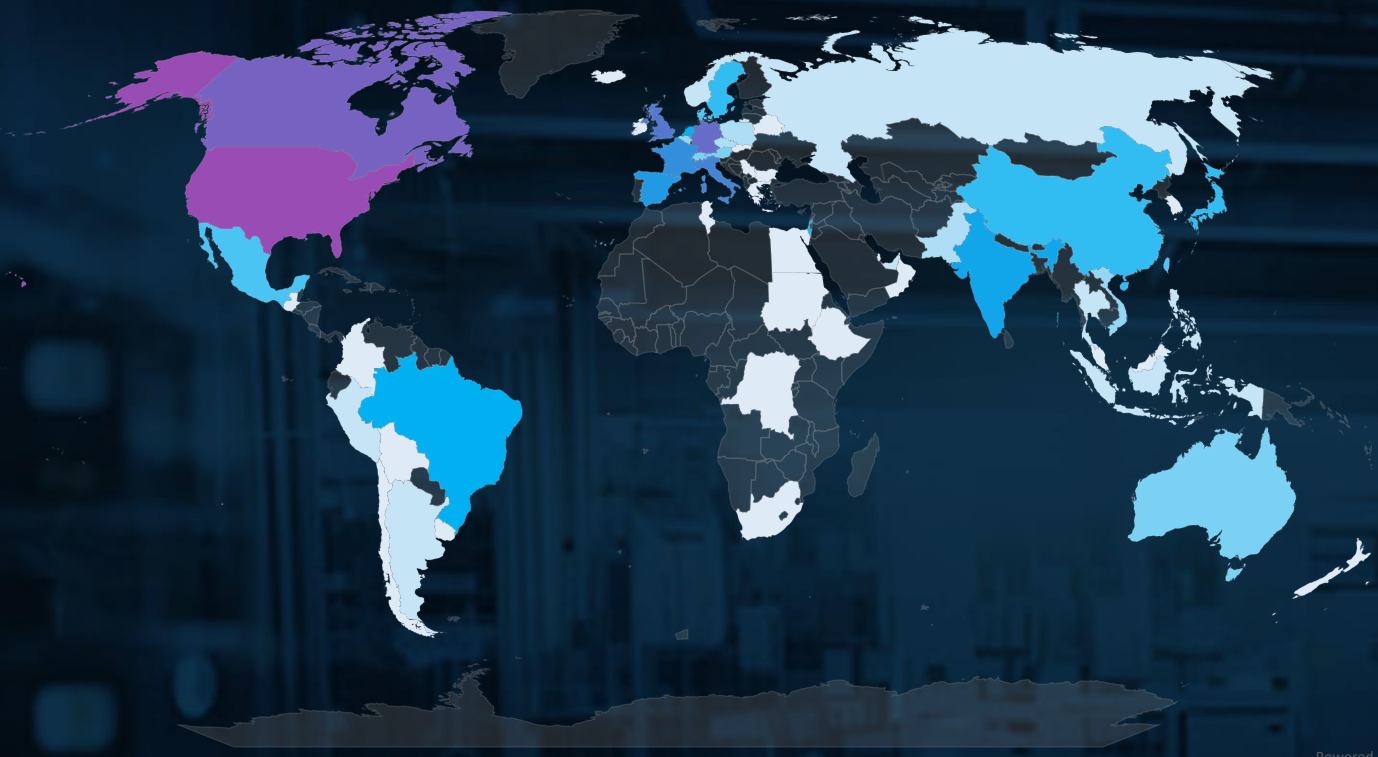
Several gangs exhibit strong focus on the manufacturing sector:

- Toufan (25 victims, 27.47%), Cactus (23 victims, 19.83%), Dragonforce (19 victims, 17.92%), and Alphv (12 victims, 15.58%) demonstrate significant activity and concentrated targeting.
- Other gangs like Fog (10 victims, 15.38%) and Blackbasta (24 victims, 13.56%) further emphasize the sector's vulnerability to ransomware attacks.
- Meow (18 victims, 13.43%), Lynx (8 victims, 13.56%), and Ransomhouse (7 victims, 13.46%) also show meaningful focus on manufacturing.

Some gangs show disproportionately high percentages due to low victim counts:

- Nitrogen (4 victims, 36.36%), Trigona (5 victims, 26.32%), and Threeam (9 victims, 28.13%) demonstrate extremely high percentages driven by relatively few victims.
- Redransomware (4 victims, 25.00%) and Cicada3301 (9 victims, 23.08%) also reflect skewed focus due to their low absolute numbers of victims.
- Toufan, despite its 25 victims (27.47%), has a similarly high percentage that indicates concentrated effort but warrants careful interpretation relative to its total activity.

GEOGRAPHIC DISTRIBUTION OF VICTIMS

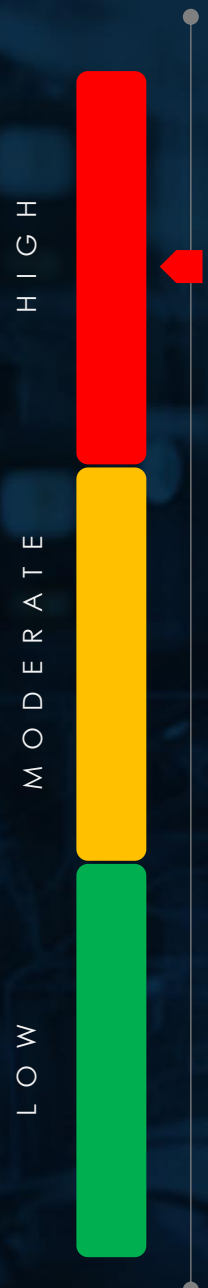


The USA accounts for 63.1% of ransomware victims in the Manufacturing industry in 2024. The next most affected countries are Canada with 36 victims, Germany with 32, the UK with 26, and Italy with 23.

A total of 61 countries reported victims, with 26 of them having only one victim each.

CYFIRMA
DECODING THREATS

MANUFACTURING INDUSTRY EXTERNAL THREAT LANDSCAPE MANAGEMENT (ETLM) OVERVIEW



Risk Level Indicator: High

APT Campaigns

The manufacturing sector recorded a high 47% incidence rate across observed APT campaigns, driven by a mix of espionage and financially motivated attacks. Groups like Lazarus and FIN7 target resources for financial gain, while nation-state actors such as MISSION2025, Mustang Panda, and Stone Panda focus on intellectual property theft and technological advancements. Emerging threats from less-defined groups highlight the growing global appeal of targeting this sector.

Actors: Lazarus, FIN7, Stone Panda, Mustang Panda, Cozy Bear, Transparent Tribe.

Geographic Focus: U.S., Japan, U.K.; Asia-Pacific nations (India, South Korea, Taiwan); emerging markets like Indonesia, Philippines.

Targets: Web applications, operating systems, and core infrastructure.

Malware: Winnti, NukeSped RAT, Cobalt Strike, Coinminer, Korplug.

Ransomware

Manufacturing accounted for 637 ransomware victims (12.21% of global total), showing a 4.08% increase year-over-year and ranking as the 3rd most targeted sector. Sustained activity across the year included a Q3 dip followed by significant growth in Q4, particularly in October and November, signaling a potential upward trend into 2025.

Victim Trends: Stable activity; spikes in October and November.

Key Actors: LockBit 3, Toufan (27% of its victims in manufacturing), Akira, 8Base, Cactus.

Geography: U.S. accounted for 63% of victims; activity recorded in 61 countries.

Insight: Manufacturing remains a top target due to its critical role in global supply chains and technological innovation.

Ranking: Manufacturing ranked 3rd globally for ransomware targeting.

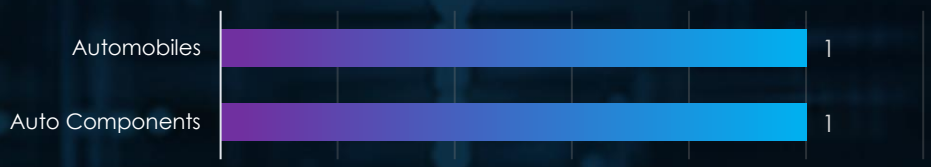
CYFIRMA
DECODING THREATS

AUTOMOTIVE INDUSTRY IN 2024

ADVANCED PERSISTENT THREATS

Over the past 12 months, automotive organizations recorded victims in 1 of the 34 Advanced Persistent Threat (APT) campaigns observed - an incidence rate of 3%.

These victims spanned 2 segments within the automotive industry as per below:



OBSERVED CAMPAIGNS PER MONTH

DEC

0

JAN

0

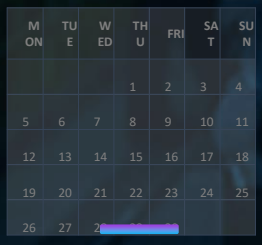
FEB

0

MAR

0

APR

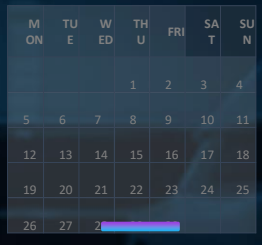


0

MAY

0

JUN

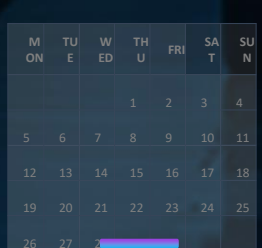


0

JUL

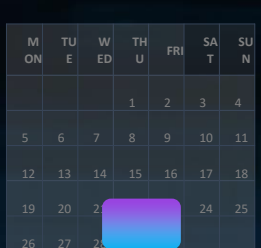
0

AUG



0

SEP

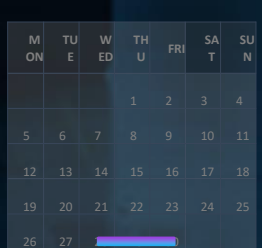


1

OCT

0

NOV

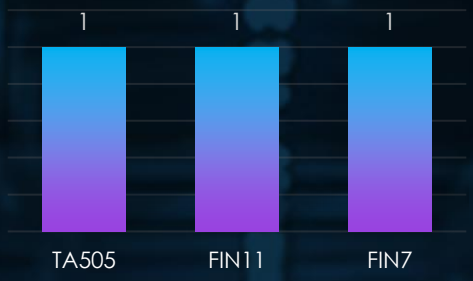


0

CYFIRMA
DECODING THREATS

APT CAMPAIGNS - AUTOMOTIVE

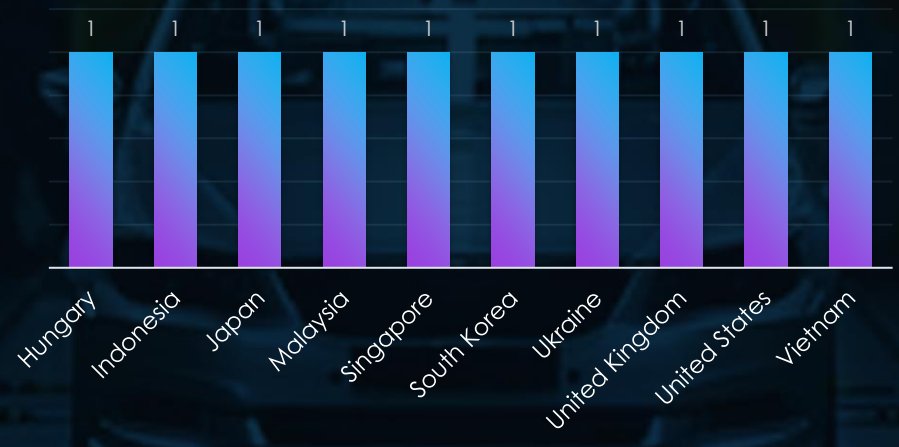
SUSPECTED THREAT ACTORS



The single observed campaign came from financially motivated cybercriminals. Due to overlapping TTPs we have murky attribution to all three TA505, FIN11, and FIN7, which are known for their focus on data theft, ransomware, and financial extortion.

The low presence of only profit-driven actors represents a significant departure from the previously prominent state-sponsored cyber activities associated with China. This shift suggests that China has aimed its cyber capabilities towards different objectives.

GEOGRAPHICAL DISTRIBUTION

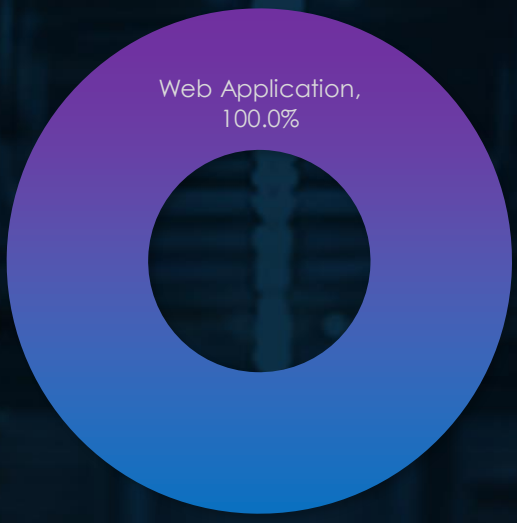


The geographic distribution of APT activity in the automotive industry highlights a global reach, with incidents spread across countries like the United States, Japan, and the United Kingdom, reflecting their prominence in automotive innovation and production.

Activity in South Korea, Vietnam, and Indonesia underscores the importance of the Asia-Pacific region as a growing hub for automotive manufacturing.

APT CAMPAIGNS - AUTOMOTIVE

TOP ATTACKED TECHNOLOGY



The automotive industry's sole targeted technology is web applications, highlighting their critical role in modern automotive operations and their vulnerability as internet-facing systems.

TOP MALWARE

The automotive industry was targeted with unique/custom TTPs, reflecting a tailored approach by attackers to exploit specific vulnerabilities.

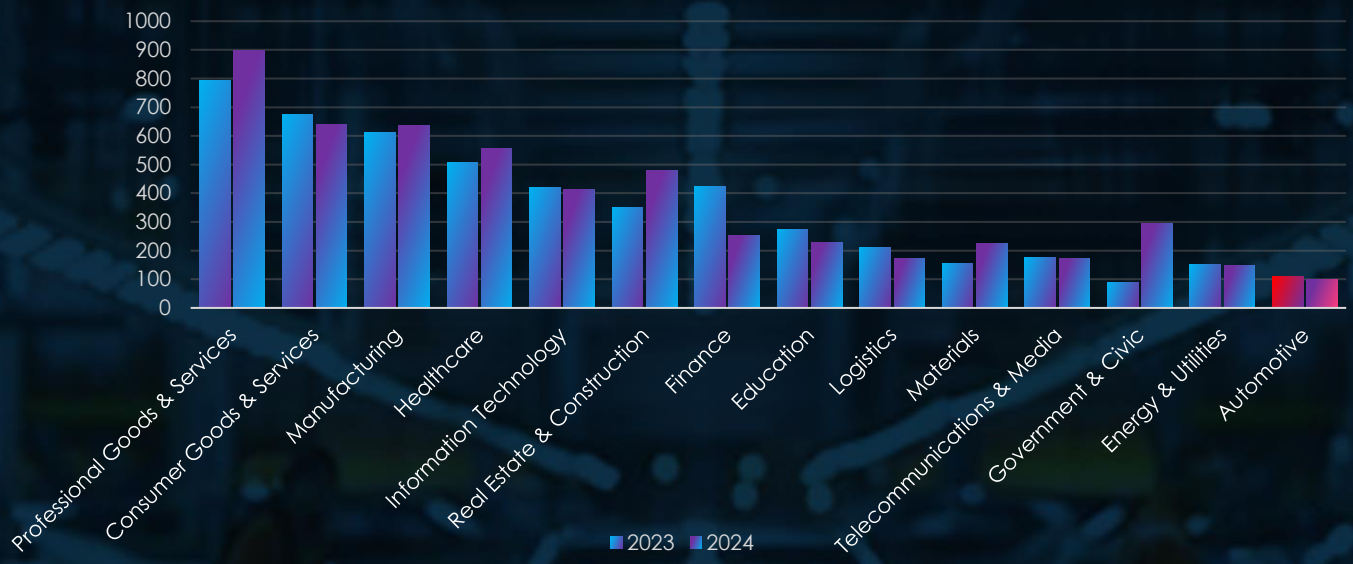
This highlights the industry's exposure to sophisticated and highly targeted threats.

CYFIRMA
DECODING THREATS

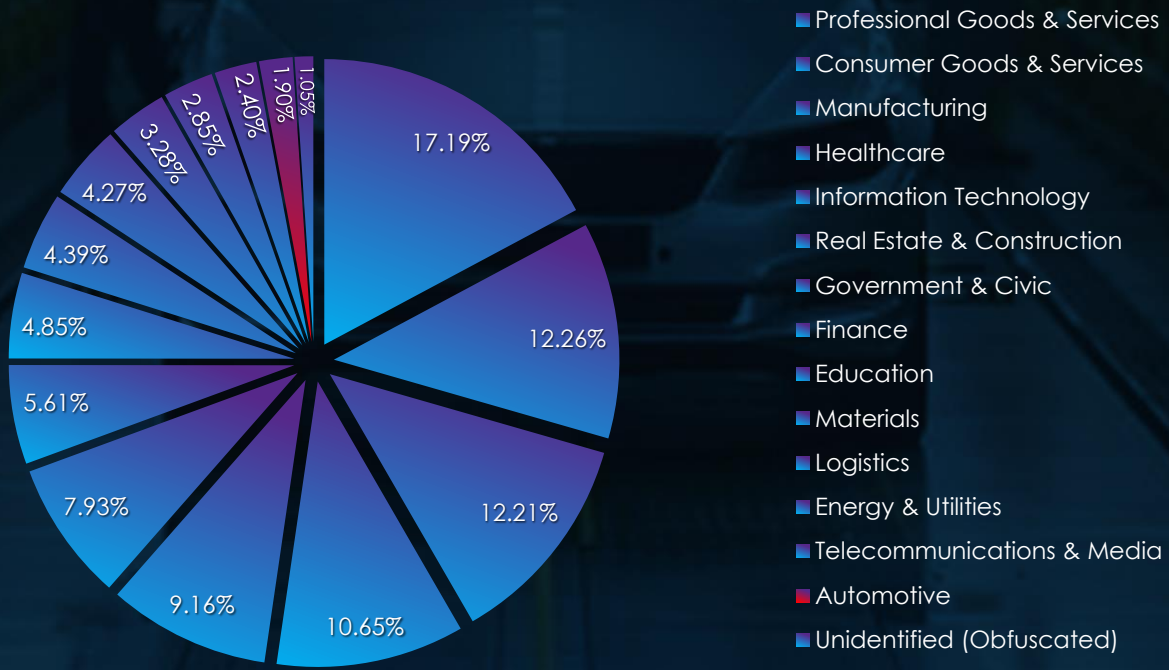
RANSOMWARE VICTIMOLOGY AUTOMOTIVE

In the past 12 months, CYFIRMA has identified 99 verified automotive industry ransomware victims. This accounts for 1.90% of the overall total of 5,219 ransomware victims during the same period.

GLOBAL DISTRIBUTION BY INDUSTRY

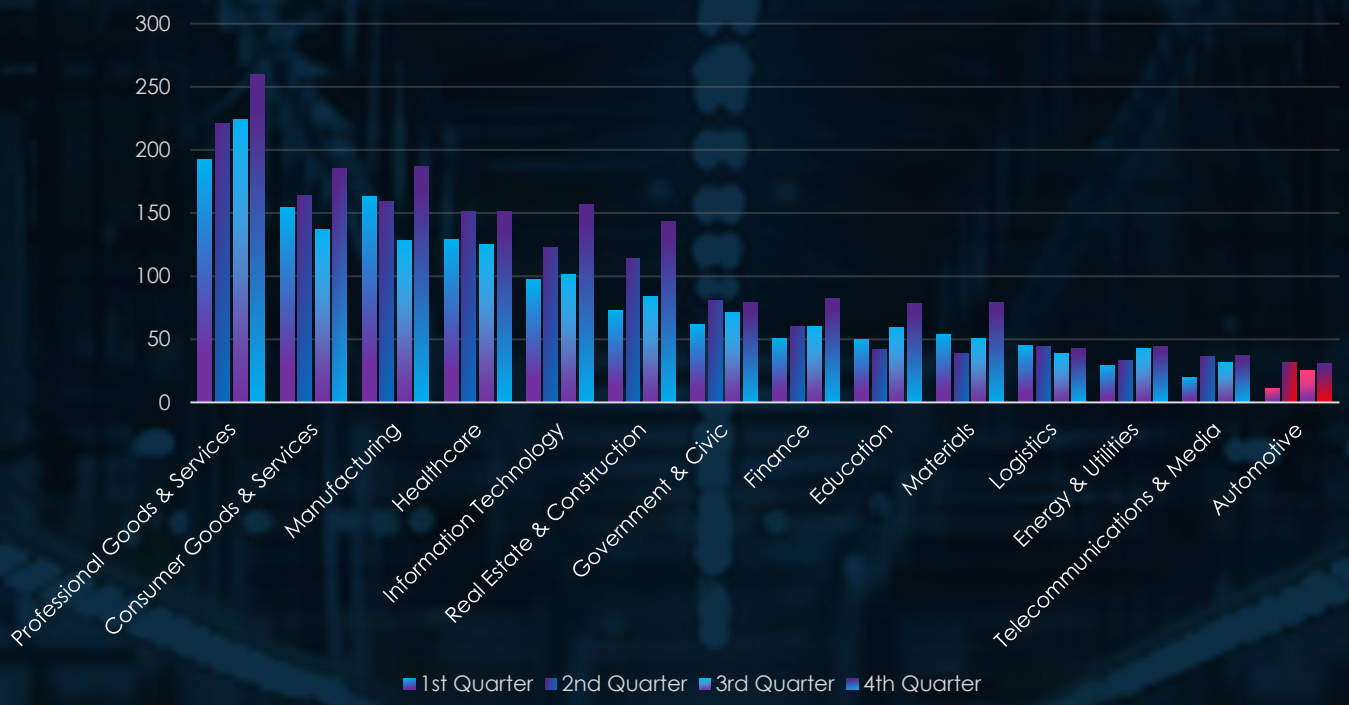


The industry recorded a significant decrease of 10.81% in recorded victims from previous year. And ranked at last at 14th place for combined victims in both years. Even though it dropped down from 13th to 14th during 2024 as the least frequent victim, it is important to note the narrow scope of just automotive industry.



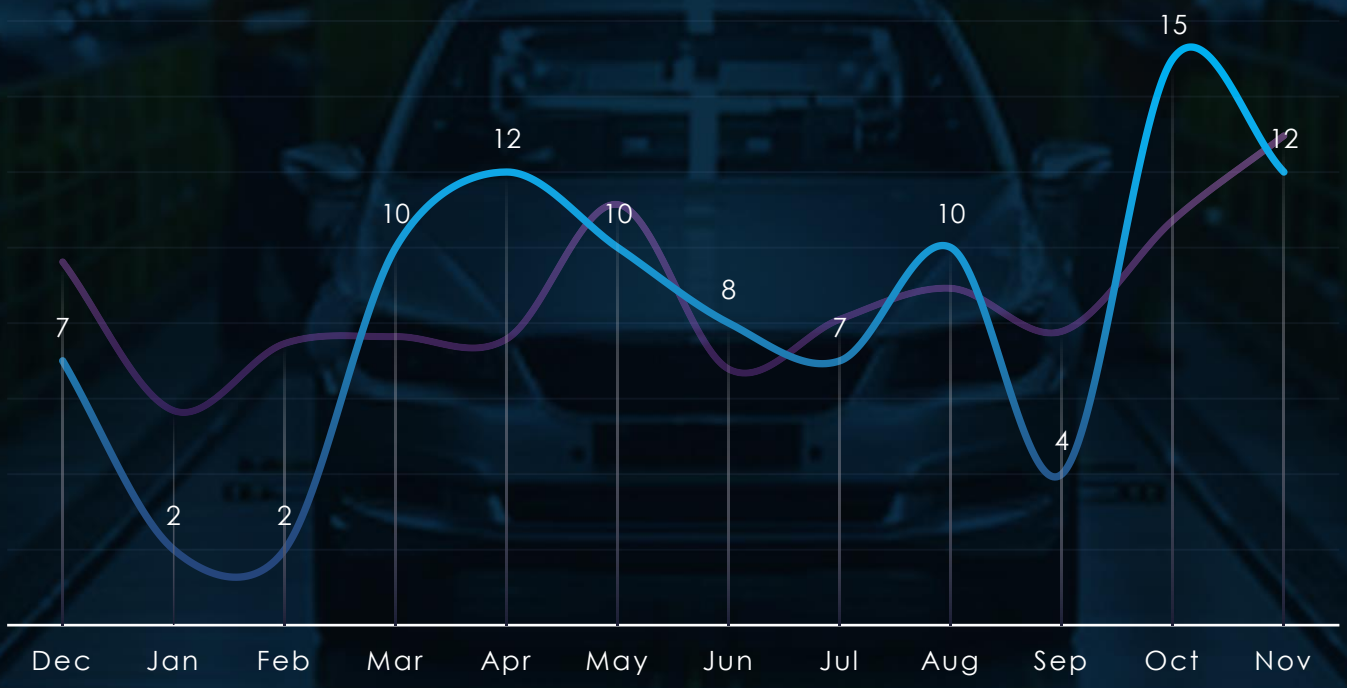
CYFIRMA
DECODING THREATS

QUARTERLY CHANGES DURING 2024



Automotive industry had calm first quarter of the year, unfortunately the rest of the year picked up the numbers. Especially in second and fourth quarter.

INDUSTRY MONTHLY ACTIVITY CHART



Monthly activity only roughly follows the scaled down global trendline. January and February we significantly calmer months, offset by above average months of March and April. Another dip came in September, but year ended with all year high, signalling elevated risk into 2025.

CYFIRMA
DECODING THREATS

BREAKDOWN OF ACTIVITY PER GANG

In total, 35 out of 97 gangs recorded victims in the automotive industry, with a 36% participation rate.

A breakdown of the top 30 gangs' monthly activity provides insights into which gangs were active each month.

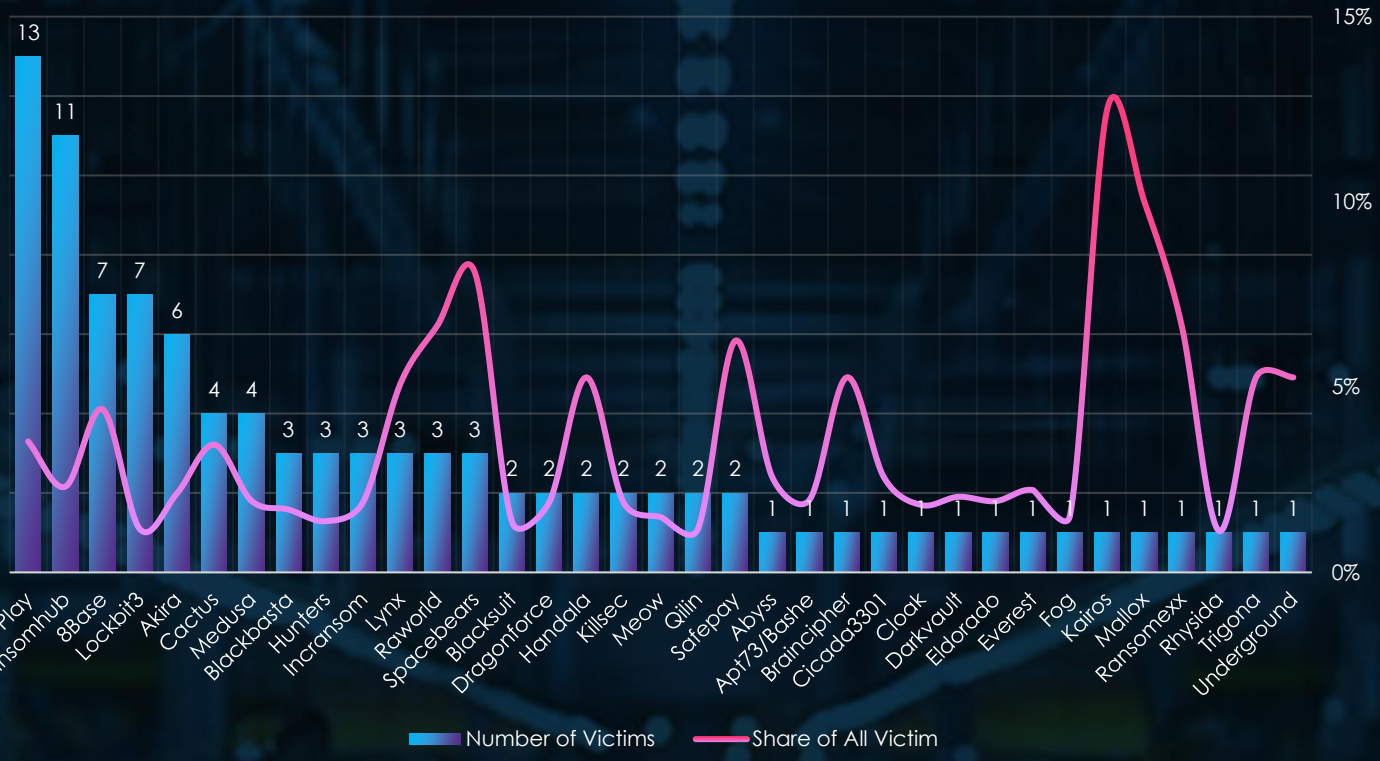
Play led ransomware activity, targeting 13 victims, with peaks in March, May, and October. Ransomhub followed with 11 victims, primarily active in August and November. 8Base and Lockbit3 each accounted for 7 victims, with 8Base peaking in February and March.

Akira targeted 6 victims, with notable activity in July and November. Cactus and Medusa (4 victims each) were active sporadically, with Cactus peaking early in the year and Medusa showing scattered campaigns. Smaller groups like Blackbasta, Hunters, and Incransom targeted 3 victims each, with activity concentrated in specific months such as April, September, and November.

Emerging actors like Lynx, Raworld, and Spacebears (3 victims each) demonstrated isolated campaigns, while groups such as Blacksuit, Dragonforce, and Qilin (2 victims each) had limited activity. Minor actors like Safepay, Abyss, and Kairos targeted only 1 or 2 victims, with their campaigns appearing late in the year.

Overall, activity was dominated by Play and Ransomhub, with smaller and emerging groups contributing sporadically to a fragmented threat landscape.

INDUSTRY RANSOMWARE VICTIMS PER GANG



Looking at all 35 active gangs, Play is the most active gang in the automotive sector, with 13 victims (3.53%), suggesting moderate activity but no specific focus on this industry. Ransomhub follows with 11 victims (2.32%), reflecting similar trends of moderate activity across industries. Lockbit3 and 8Base each have 7 victims (1.17% and 4.40%, respectively), with 8Base showing a slightly stronger focus.

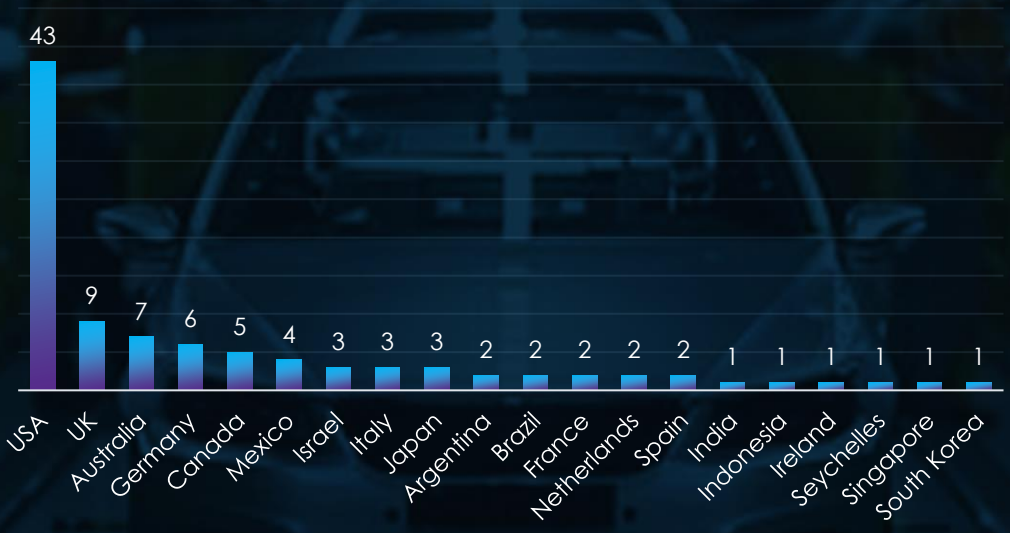
Several gangs demonstrate notable focus within the automotive sector, albeit with varying victim counts:

- Spacebears (3 victims, 8.11%) and Raworld (3 victims, 6.67%) display meaningful targeting relative to their total activity.
- Safepay (2 victims, 6.25%) also indicates some level of specific focus despite its small victim count.
- Lynx (3 victims, 5.08%) and Handala (2 victims, 5.26%) show similar trends, though their impact is limited by the low number of victims.

Certain gangs show disproportionately high percentages due to very low victim counts:

- Kairos (1 victim, 12.50%) and Mallox (1 victim, 10.00%) exhibit extremely high percentages driven by single incidents.
- Ransomexx (1 victim, 6.67%), Underground (1 victim, 5.26%), and Trigona (1 victim, 5.26%) similarly reflect skewed focus due to their small victim counts.
- Braincipher (1 victim, 5.26%) and Abyss (1 victim, 2.56%) also display percentages that require cautious interpretation due to minimal activity.

GEOGRAPHIC DISTRIBUTION OF VICTIMS



The USA accounts for 43.4% of ransomware victims in the Automotive industry in 2024. The next most affected countries are the UK with 9 victims, Australia with 7, Germany with 6, and Canada with 5.

A total of 20 countries reported victims, with 6 of them having only one victim each.

CYFIRMA
DECODING THREATS

AUTOMOTIVE INDUSTRY EXTERNAL THREAT LANDSCAPE MANAGEMENT (ETLM) OVERVIEW

Risk Level Indicator: Low/Moderate

APT Campaigns

The automotive sector had a low 3% incidence rate across observed APT campaigns, driven solely by financially motivated groups such as TA505, FIN11, and FIN7, targeting data theft, ransomware, and extortion. Notably, Chinese state-sponsored activity, previously prominent in this sector, has significantly declined.

Actors: TA505, FIN11, FIN7.

Geographic Focus: U.S., Japan, U.K.; emerging hubs in South Korea, Vietnam, and Indonesia.

Targets: Solely web applications, reflecting their vulnerability as critical internet-facing systems.

Tactics: Custom TTPs tailored to exploit specific vulnerabilities.

Ransomware

The automotive industry accounted for 99 ransomware victims (1.90% of global total), marking a 10.81% year-over-year decrease and ranking as the least targeted sector. Activity was calm in Q1 but increased in Q2 and Q4, with a year-high in December indicating potential elevated risk into 2025.

Victim Trends: Steady increase after Q1; peaks in March, April, and December.

Key Actors: Play (most active), 8Base, Lynx (5.0% share), Raworld (6.7%), Spacebears (8.1%).

Geography: U.S. accounted for 43% of victims; activity recorded in 20 countries.

Insight: The lack of a concentrated focus by ransomware groups reflects the sector's lower priority compared to others.

Ranking: Automotive industry ranked 13th as the least frequent target of ransomware.

CYFIRMA
DECODING THREATS

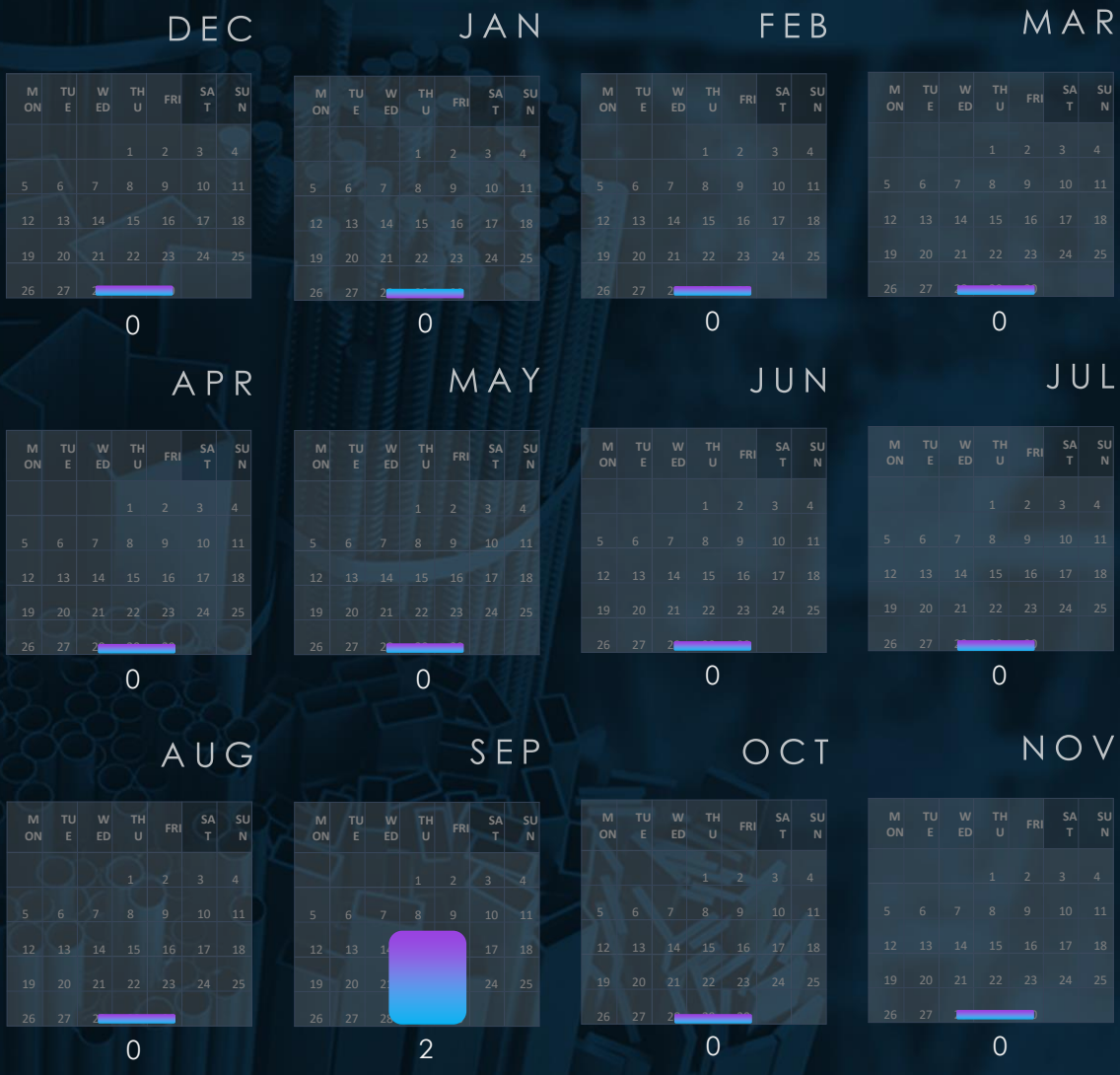
MATERIALS INDUSTRY IN 2024

ADVANCED PERSISTENT THREATS

Over the past 12 months, materials organizations recorded victims across 2 of the 34 Advanced Persistent Threat (APT) campaigns observed - an incidence rate of 6%.

These victims spanned multiple segments within the materials industry as per below:

OBSERVED CAMPAIGNS PER MONTH



CYFIRMA
DECODING THREATS

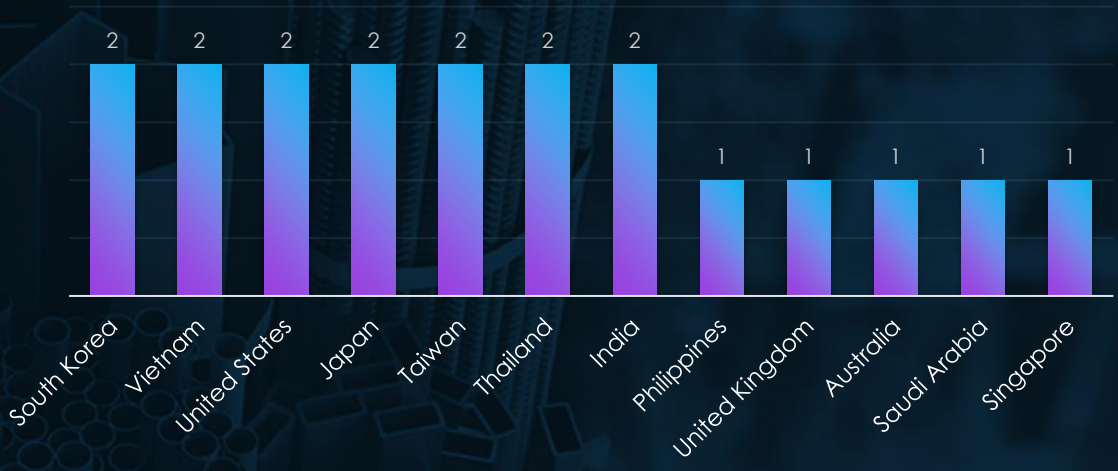
APT CAMPAIGNS - MATERIALS

SUSPECTED THREAT ACTORS

The materials industry faces threats from a mix of nation-state and financially motivated actors. Cozy Bear and Fancy Bear (Russia) focus on espionage, likely targeting sensitive data and intellectual property related to critical materials. Meanwhile, TA505 represents profit-driven motives, targeting the sector for financial extortion and data theft.

MISSION2025 (China) emphasizes geopolitical interests, aiming to exploit technological advancements and trade secrets. This combination of threats underscores the materials industry's strategic importance in both economic and geopolitical contexts.

GEOGRAPHICAL DISTRIBUTION



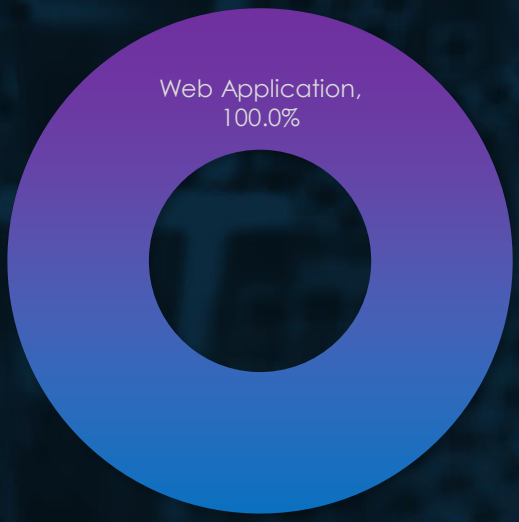
The materials industry faces geographically diverse targeting, with a strong focus on Asia-Pacific nations like South Korea, Vietnam, Japan, Taiwan, and India, reflecting the region's role as a hub for critical material production and innovation.

The United States also features prominently, underscoring its strategic importance in the global supply chain.

Other countries, including the Philippines, United Kingdom, and Saudi Arabia, illustrate the expanding reach of attacks, targeting both established and emerging players in the materials sector.

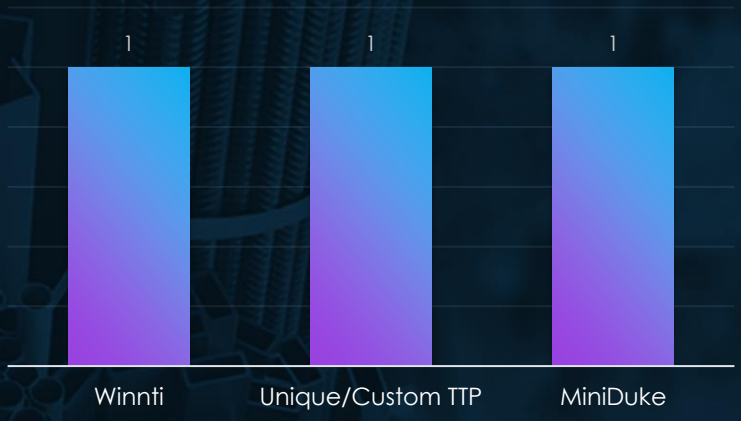
APT CAMPAIGNS - MATERIALS

TOP ATTACKED TECHNOLOGY



The materials industry's targeted technology is web applications, emphasizing their vulnerability as internet-facing systems essential for operations. This highlights the critical need for securing these interfaces to prevent exploitation and protect sensitive industry data.

TOP MALWARE

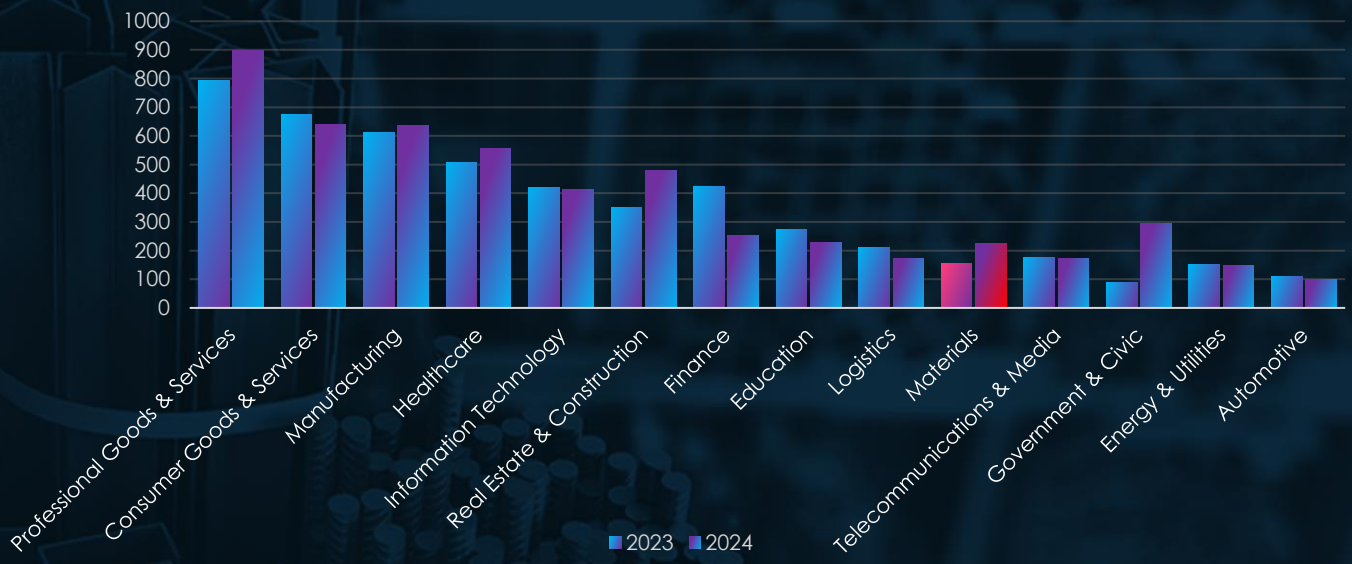


The materials industry is targeted by a mix of custom and well-known malware. Winnti is notable for its long-term infiltration and data theft capabilities, commonly used in espionage operations. Unique/Custom TTPs highlight attackers' tailored approaches to exploiting specific vulnerabilities. MiniDuke, known for its espionage focus, further underscores the strategic importance of the materials sector to nation-state actors.

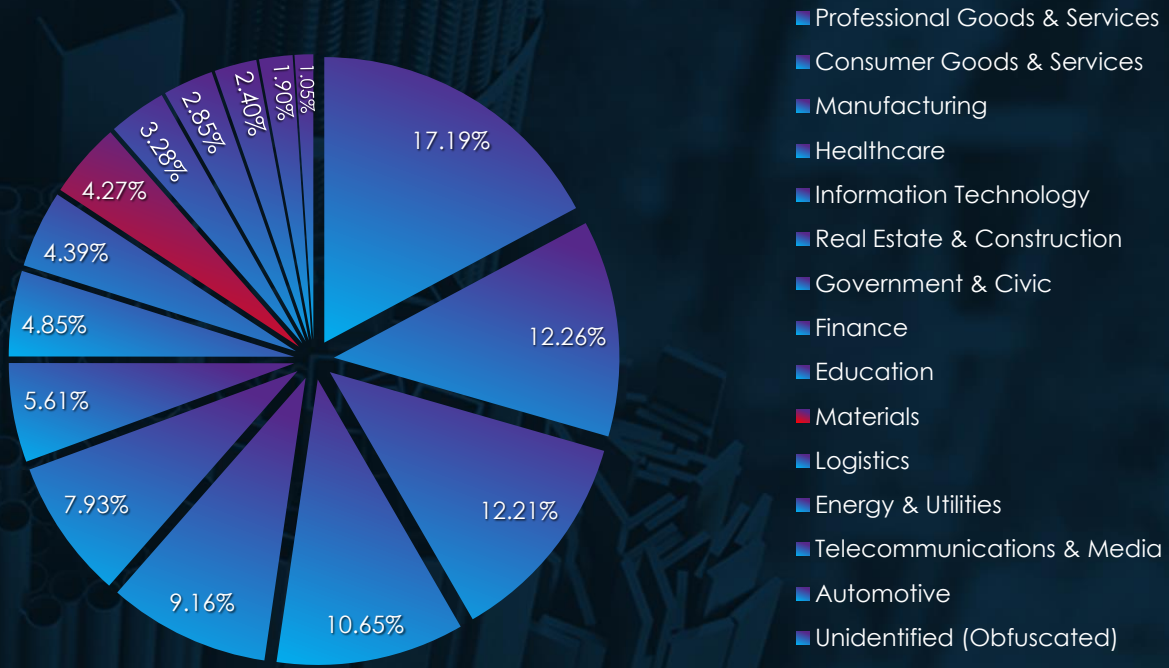
RANSOMWARE VICTIMOLOGY MATERIALS

In the past 12 months, CYFIRMA has identified 223 verified materials industry ransomware victims. This accounts for 4.27% of the overall total of 5,219 ransomware victims during the same period.

GLOBAL DISTRIBUTION BY INDUSTRY

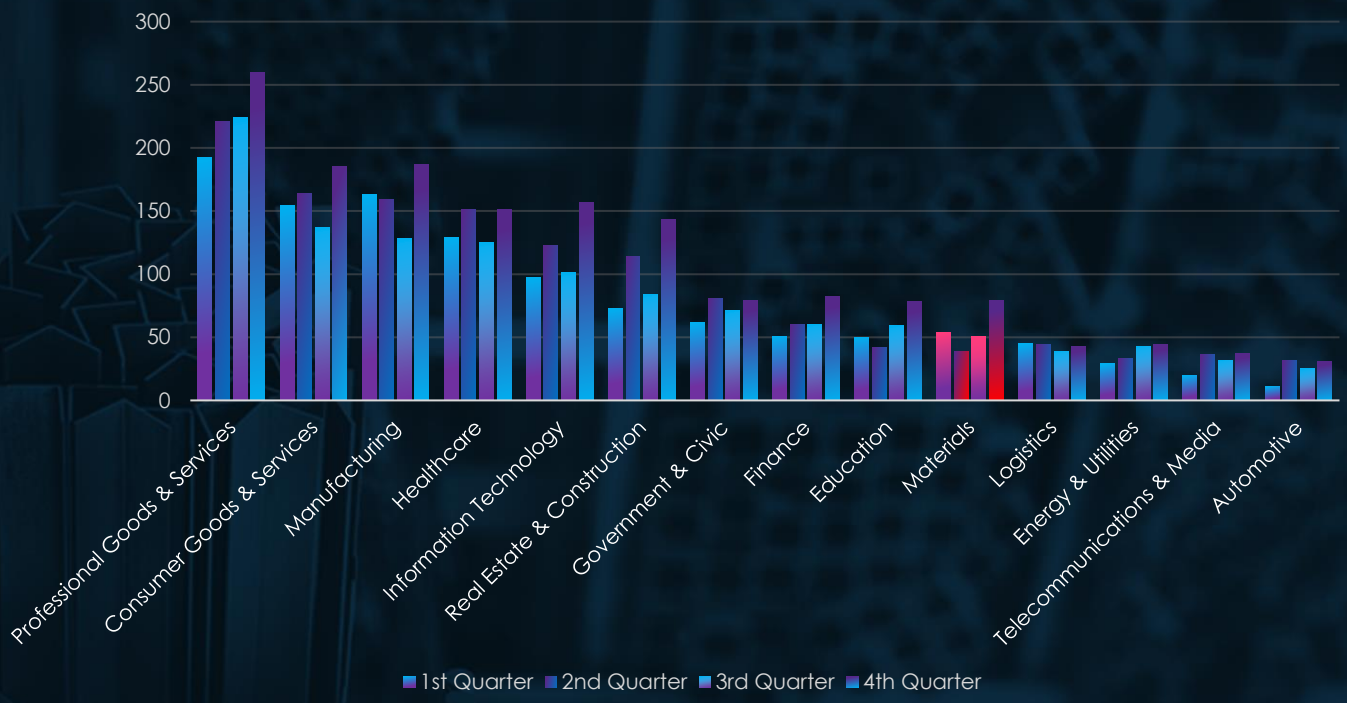


The industry recorded a major increase of 30.49% in recorded victims from previous year. And ranked at 10th place for victims in both years combined. Industry moved up from 11th to 10th during 2024 as tenth most frequent victim.



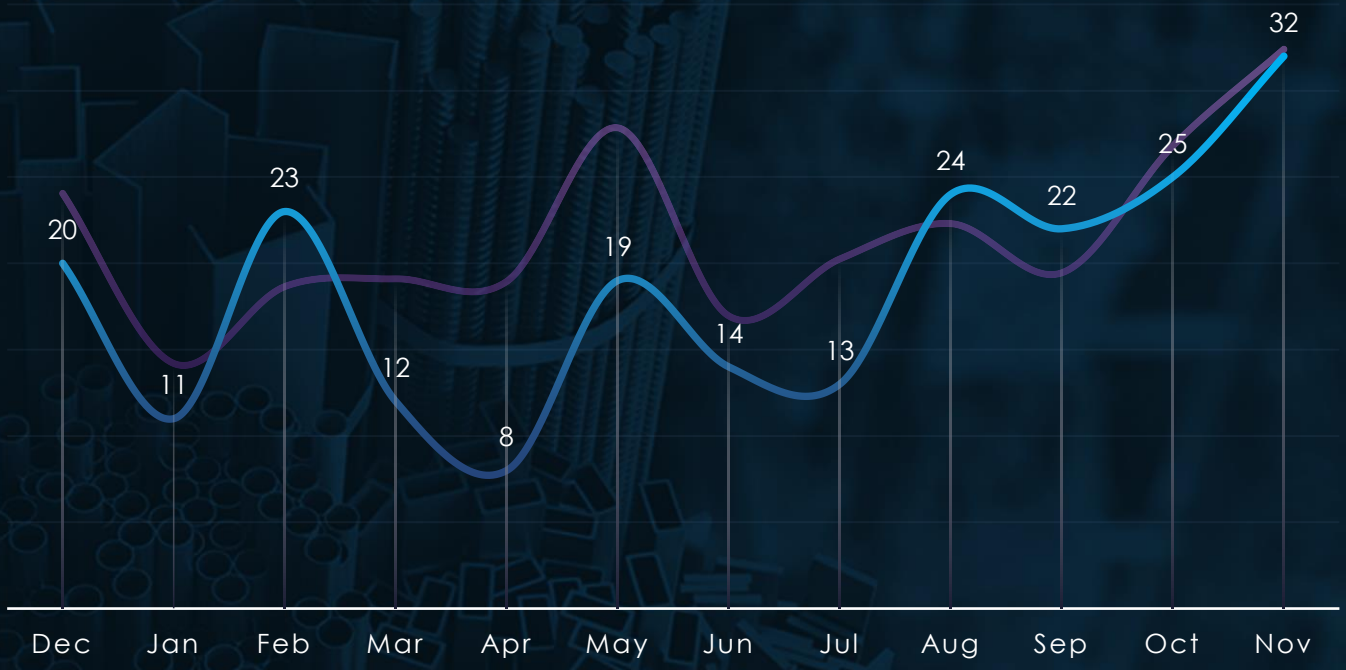
CYFIRMA
DECODING THREATS

QUARTERLY CHANGES DURING 2024



Materials industry experienced sustained activity in first three quarters, with minor dip during the second. However, in line with global trend number of victims spiked in fourth quarter.

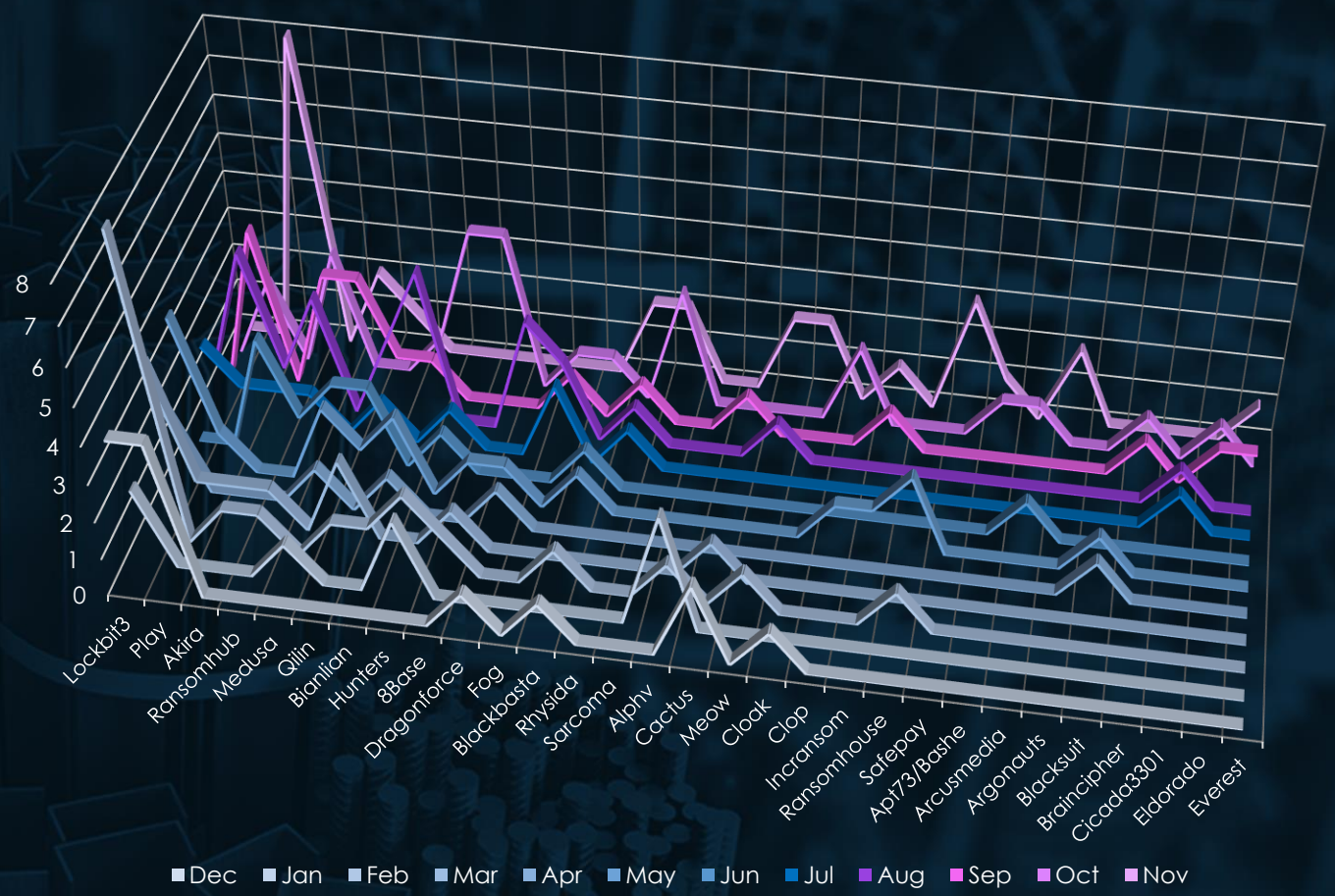
INDUSTRY MONTHLY ACTIVITY CHART



Monthly activity only follows the scaled down global trendline at the start and end of the year. In March and April industry recorded dip in activity and diverged from global trendline. In May activity picked up again and towards the end of the year caught up with global trendline, which suggest higher activity at the start of 2025.

CYFIRMA
DECODING THREATS

BREAKDOWN OF ACTIVITY PER GANG



In total 54 out of 97 gangs recorded victims in materials industry, 56% participation.

A breakdown of top 30 gang's monthly activity provides insights into which gangs were active each month.

Lockbit3 dominated ransomware activity with 27 victims, peaking in February (8 victims). Play followed with 17 victims, with notable spikes in August and September. Akira targeted 15 victims, with activity concentrated in the latter half of the year, particularly in November (8 victims).

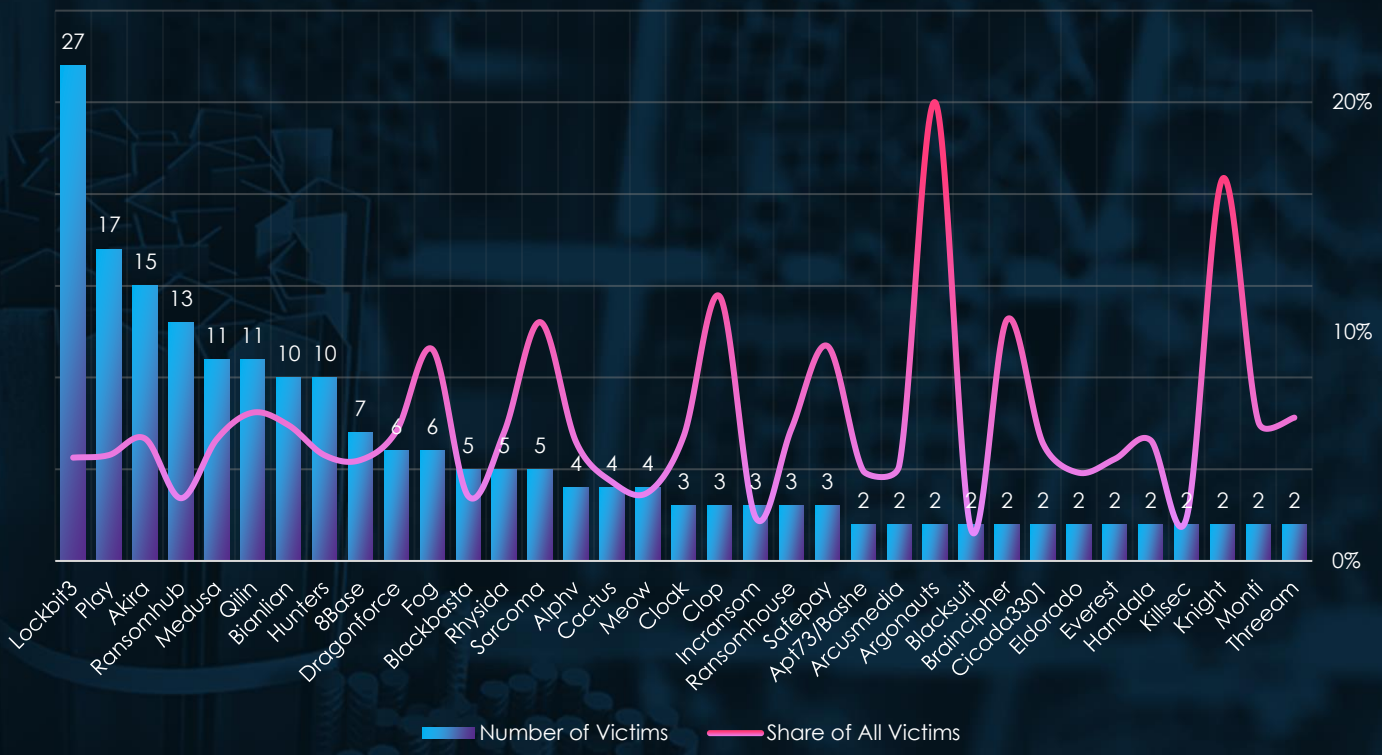
Ransomhub recorded 13 victims, with steady activity in August through October. Medusa and Qilin each accounted for 11 victims, with Medusa peaking in May and October, while Qilin maintained consistent activity across multiple months. Bianlian and Hunters (10 victims each) focused their campaigns on August and October.

Smaller actors included 8Base (7 victims), Dragonforce, and Fog (6 each), with Dragonforce peaking in August and Fog active later in the year. Blackbasta and Rhysida targeted 5 victims each, with Rhysida showing late-year spikes in October and November. Sarcoma also reached 5 victims, with its activity exclusively in October and November.

Emerging groups such as Alphv, Cactus, and Meow (4 victims each) showed limited but sporadic operations. Minor actors like Cloak, Clop, and Incransom (3 victims each) contributed with isolated campaigns, primarily in mid-to-late months.

Overall, Lockbit3 and Play led the ransomware landscape, while groups like Akira, Ransomhub, and Medusa demonstrated seasonal peaks.

INDUSTRY RANSOMWARE VICTIMS PER GANG



Analysis of the top 35 gangs, Lockbit3 is the most active gang in the materials sector, with 27 victims (4.51%), followed by Play, with 17 victims (4.62%). Both demonstrate moderate activity but no specific focus on the materials industry. Akira (15 victims, 5.34%) and Ransomhub (13 victims, 2.74%) also show some presence in this sector, though their focus appears distributed across multiple industries.

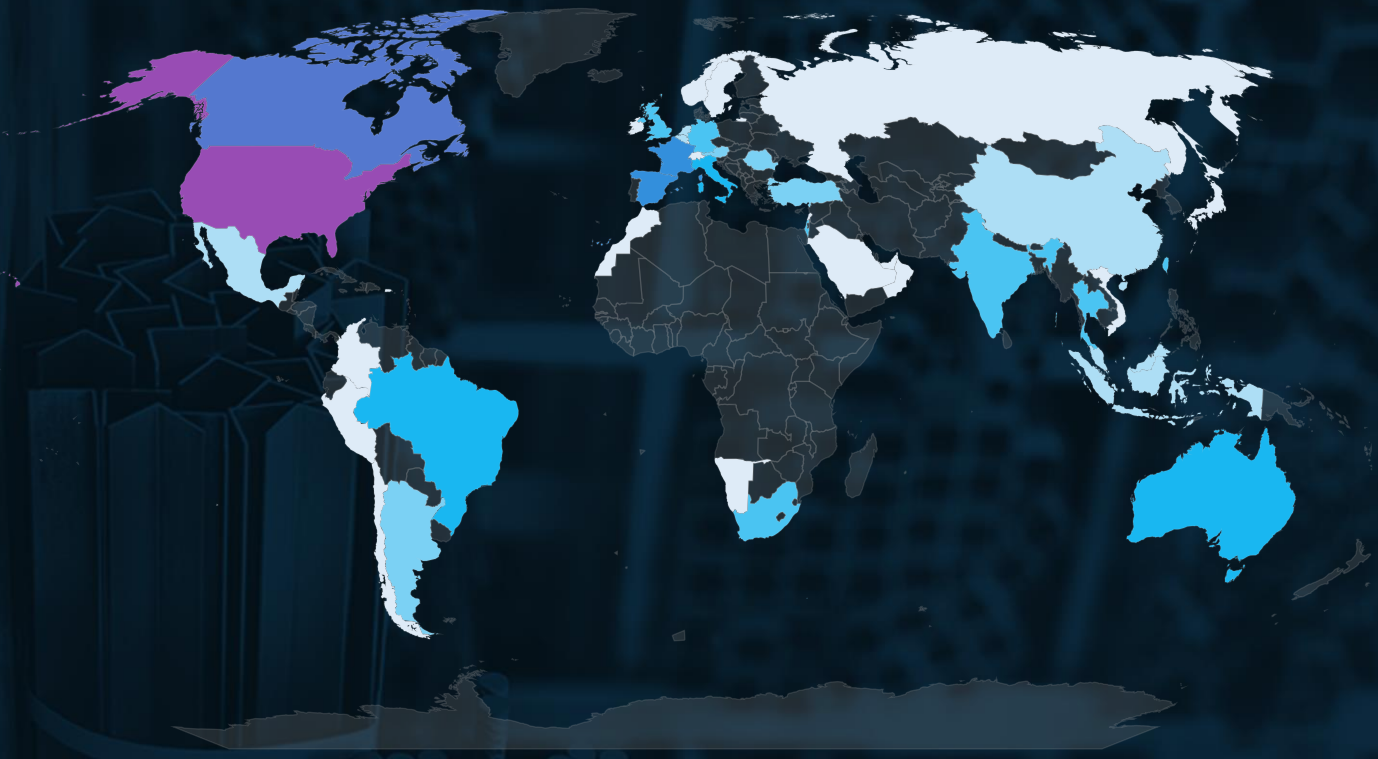
Several gangs exhibit significant focus within the materials sector:

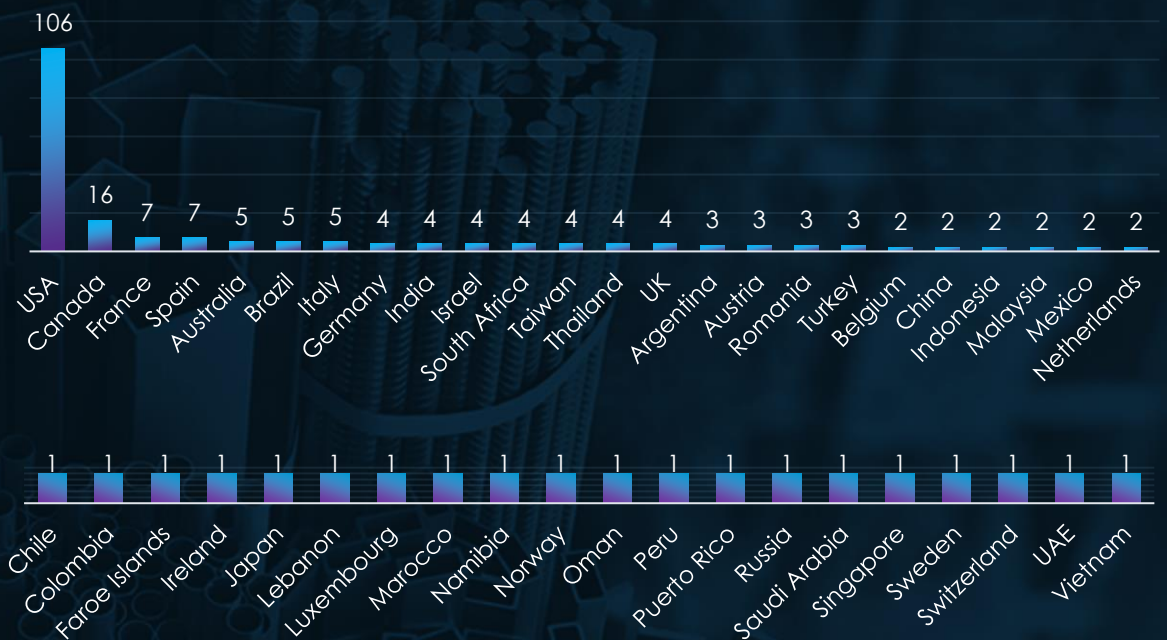
- Qilin (11 victims, 6.47%) and Fog (6 victims, 9.23%) show concentrated targeting efforts.
- Sarcoma (5 victims, 10.42%) and Rhysida (5 victims, 5.62%) further reflect notable focus.
- Smaller gangs like Clop (3 victims, 11.54%) and Safepay (3 victims, 9.38%) also demonstrate a meaningful focus on the materials industry despite lower victim counts.

Certain gangs show disproportionately high percentages due to low victim counts:

- Argonauts (2 victims, 20.00%) and Knight (2 victims, 16.67%) display very high percentages driven by minimal activity.
- Braincipher (2 victims, 10.53%) and Threeam (2 victims, 6.25%) similarly reflect skewed focus due to their low number of victims.
- Monti (2 victims, 6.06%) and Handala (2 victims, 5.26%) also exhibit percentages that require cautious interpretation given their small absolute numbers.

GEOGRAPHIC DISTRIBUTION OF VICTIMS





The USA accounts for 47.5% of ransomware victims in the Materials industry in 2024. The next most affected countries are Canada with 16 victims, France with 7, Spain with 7, and Italy with 5.

A total of 44 countries reported victims, with 20 of them having only one victim each.

CYFIRMA
DECODING THREATS

MATERIALS INDUSTRY EXTERNAL THREAT LANDSCAPE MANAGEMENT (ETLM) OVERVIEW

Risk Level Indicator: Moderate

APT Campaigns

The materials sector experienced a low 6% incidence rate across observed APT campaigns, driven by nation-state and financially motivated actors. Cozy Bear and MISSION2025 target intellectual property and trade secrets, while TA505 focuses on financial extortion. The sector's strategic importance to global supply chains and innovation makes it a key target for espionage and economic disruption.

Actors: Cozy Bear, Fancy Bear, MISSION2025, TA505.

Geographic Focus: U.S., South Korea, Vietnam, Japan, India; emerging targets in the Philippines, U.K., Saudi Arabia.

Targets: Web applications, reflecting their critical role in operations and vulnerability as internet-facing systems.

Malware: Winnti, MiniDuke; custom TTPs for tailored exploitation.

Ransomware

The materials industry accounted for 223 ransomware victims (4.27% of global total), with a significant 30.49% year-over-year increase, ranking 10th among targeted sectors in 2024. Activity remained steady across most quarters, with a Q4 spike indicating higher risks moving into 2025.

Victim Trends: Stable across Q1-Q3; spikes in Q4.

Key Actors: LockBit 3 (27 victims, peak in February), Play (17 victims, peaks in August/September), Akira (15 victims, peak in November).

Geography: U.S. accounted for 48% of victims; activity recorded in 44 countries.

Ranking: Materials industry ranked 10th as the tenth most frequent victim of ransomware.

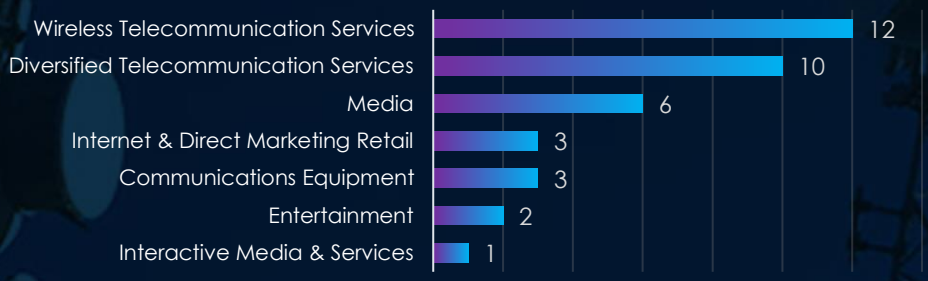
CYFIRMA
DECODING THREATS

TELECOMMUNICATIONS & MEDIA INDUSTRY IN 2024

ADVANCED PERSISTENT THREATS

Over the past 12 months, telecommunications & media organizations recorded victims across 16 of the 34 Advanced Persistent Threat (APT) campaigns observed - an incidence rate of 47%.

These victims spanned multiple segments within the telecommunications & media industry as per below:

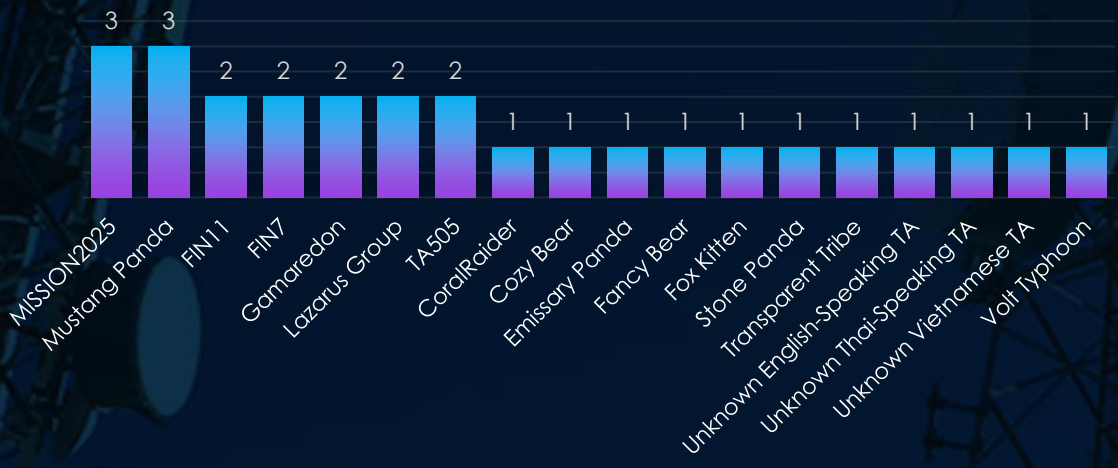


OBSERVED CAMPAIGNS PER MONTH

CYFIRMA
DECODING THREATS

APT CAMPAIGNS TELECOMMUNICATIONS & MEDIA

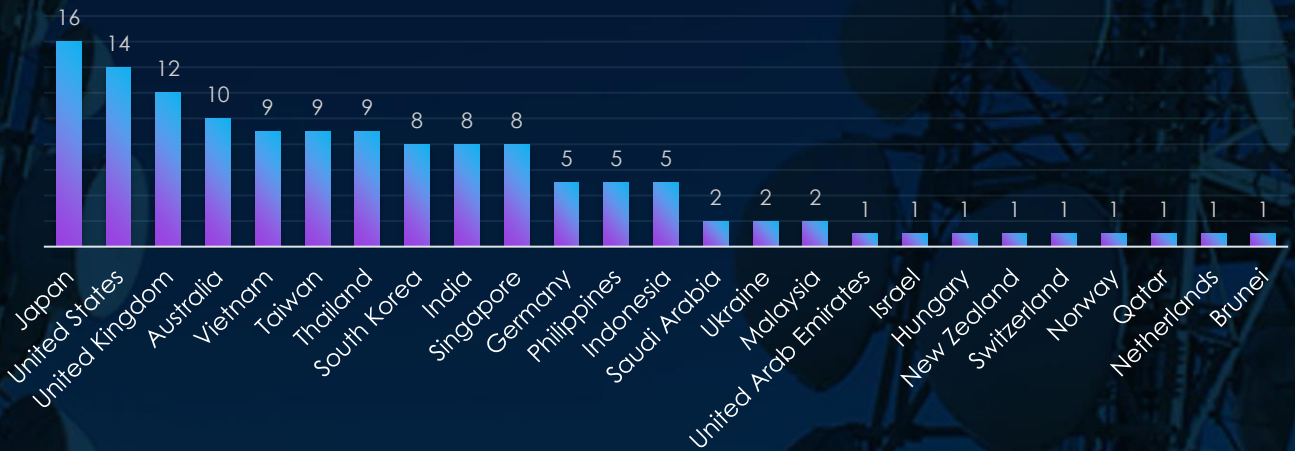
SUSPECTED THREAT ACTORS



The industry faces threats from both nation-state and financially motivated actors. MISSION2025 and Mustang Panda (China) lead, focusing on espionage and infrastructure exploitation, while Lazarus Group, FIN11, and FIN7 target the sector for financial gain.

Russian groups like Gamaredon, Cozy Bear, and Fancy Bear prioritize intelligence gathering and geopolitical objectives. Emerging actors, including Unknown Thai- and Vietnamese-Speaking TAs, reflect an expanding threat landscape, underscoring the sector's critical role in global communications and information control.

GEOGRAPHICAL DISTRIBUTION



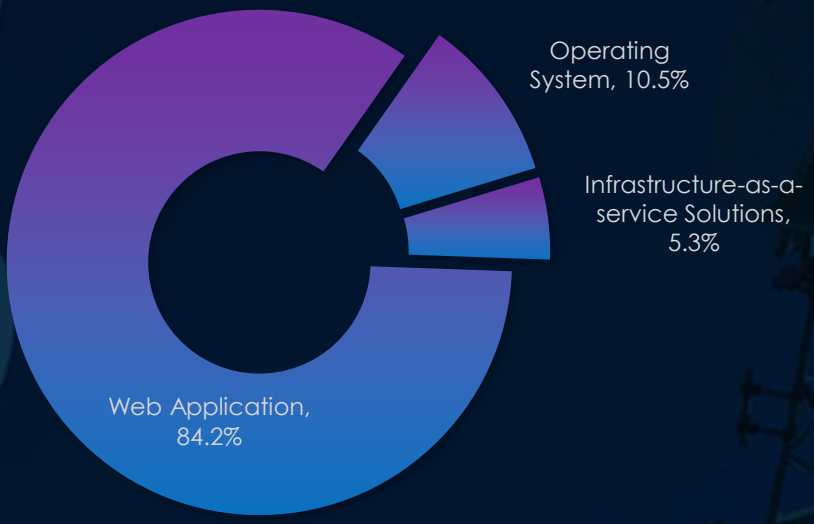
The telecommunications and media industry is targeted globally, with a strong focus on advanced economies and key hubs. Countries like Japan, United States, and United Kingdom lead, reflecting their prominence in global communications infrastructure. Asia-Pacific nations, including Vietnam, Taiwan, and Thailand, are heavily targeted, underscoring the region's strategic importance.

Emerging markets such as Philippines, Indonesia, and Malaysia also feature, highlighting attackers' expanding reach. The inclusion of smaller nations like Brunei, Norway, and Qatar illustrates the diverse scope of threats to this critical sector.

CYFIRMA
DECODING THREATS

APT CAMPAIGNS
TELECOMMUNICATIONS & MEDIA

TOP ATTACKED TECHNOLOGY



Web applications dominate, reflecting their vulnerability as internet-facing systems integral to communication platforms. Operating systems also see significant targeting, emphasizing their foundational role in infrastructure. Additionally, infrastructure-as-a-service solutions appear as a target.

TOP MALWARE

The telecommunications and media industry faces a diverse array of malware threats, with Unique/Custom TTPs and Commodity Malware leading in usage, reflecting both tailored attacks and the accessibility of widely available tools.

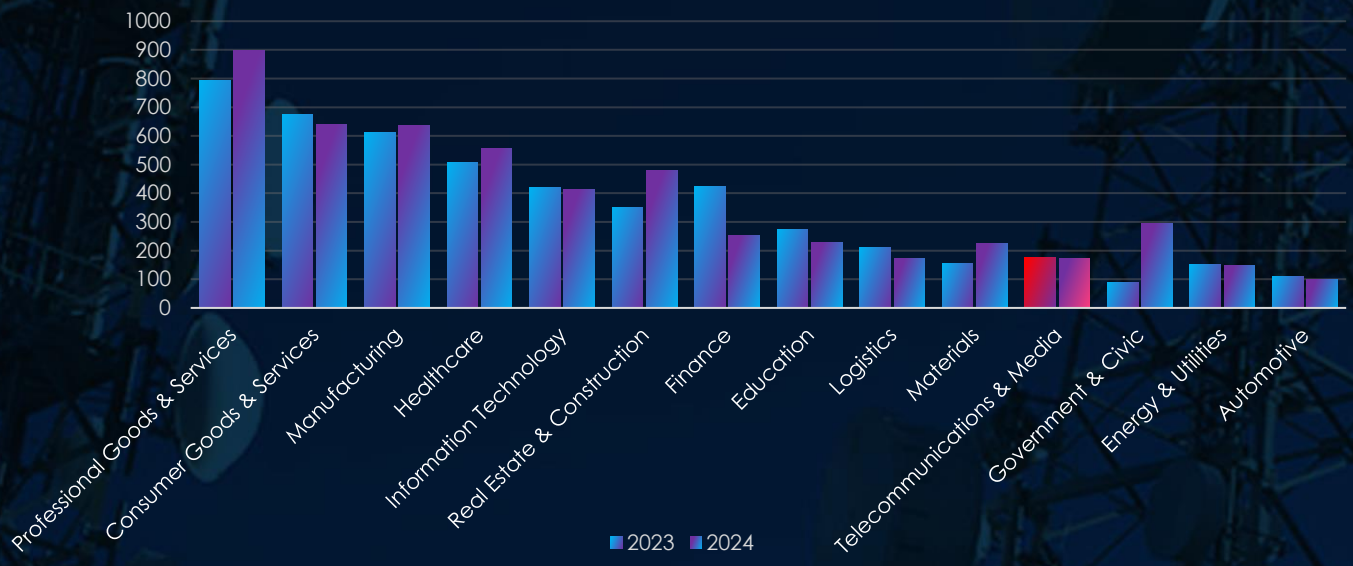
Winnti highlights its role in long-term infiltration and data theft, aligning with espionage objectives. Other notable tools like ransomware, Cobalt Strike, and PlugX emphasize versatility, supporting operations ranging from financial extortion to system exploitation.

CYFIRMA
DECODING THREATS

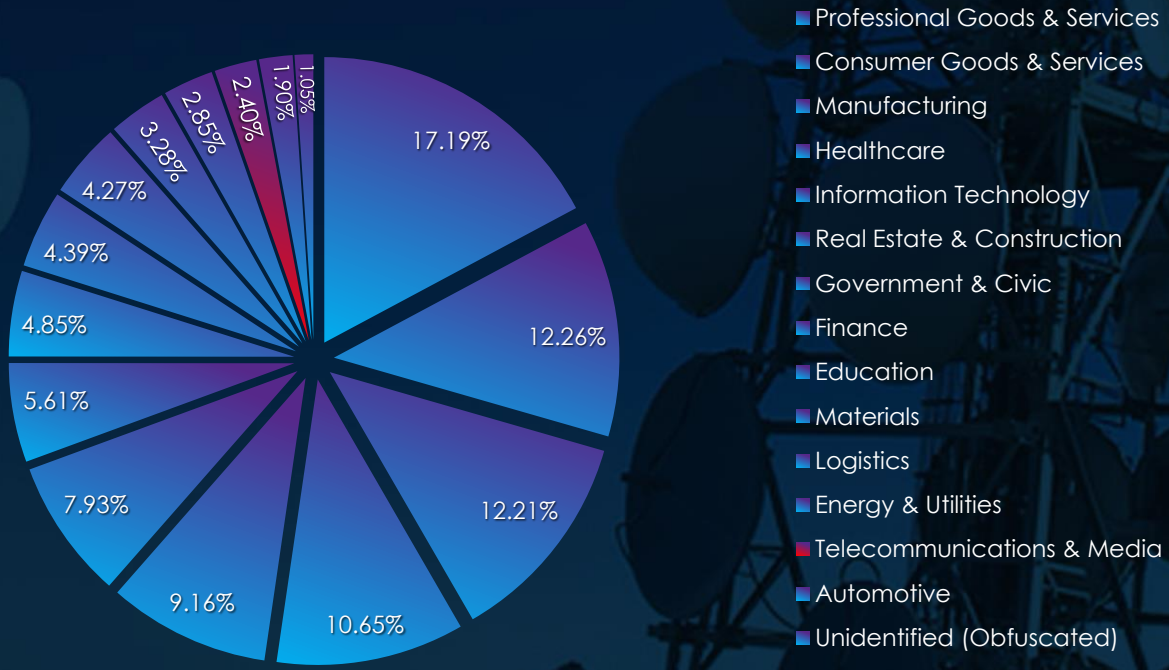
RANSOMWARE VICTIMOLOGY TELECOMMUNICATION & MEDIA

In the past 12 months, CYFIRMA has identified 125 verified telecommunications & media industry ransomware victims. This accounts for 2.40% of the overall total of 5,219 ransomware victims during the same period.

GLOBAL DISTRIBUTION BY INDUSTRY

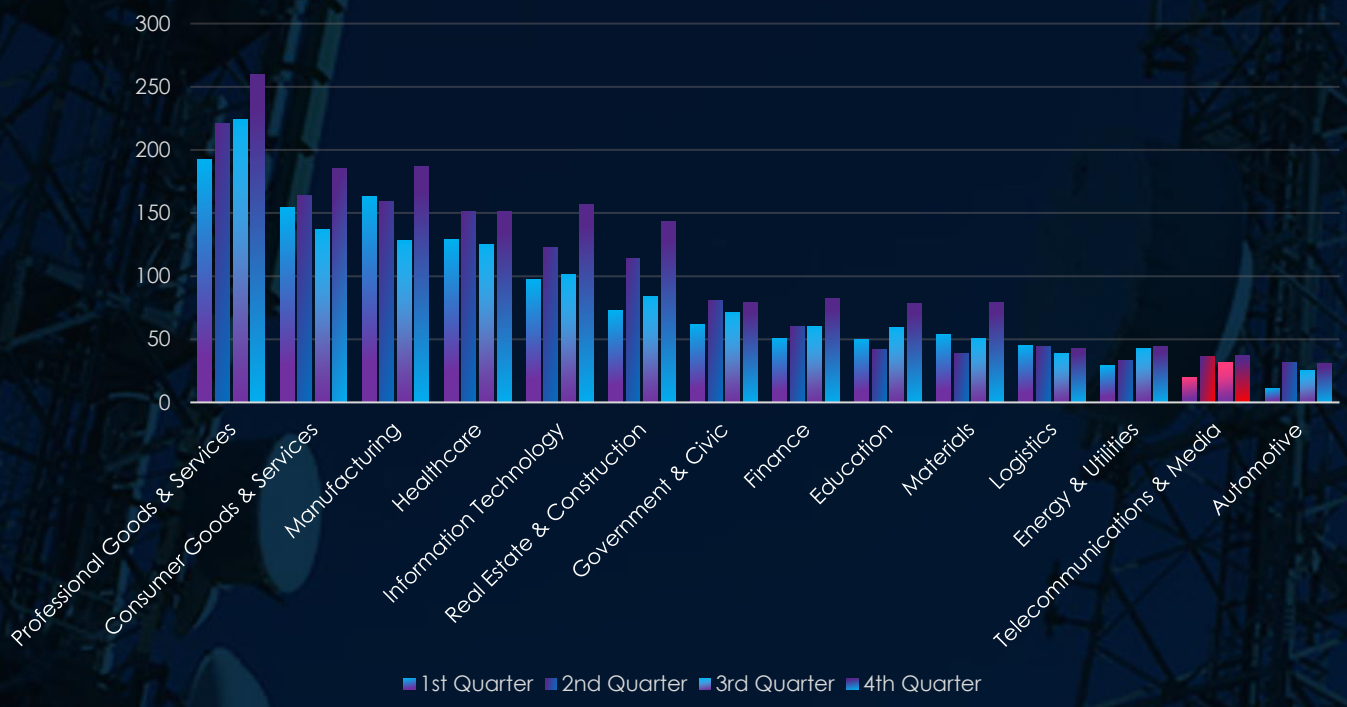


The industry recorded remarkably consistent number of recorded victims, just very minor 2.29%% decrease from previous year. And ranked at 10th place for both years combined. Industry moved down from 9th to 12th place during 2024 as second least frequent victim.



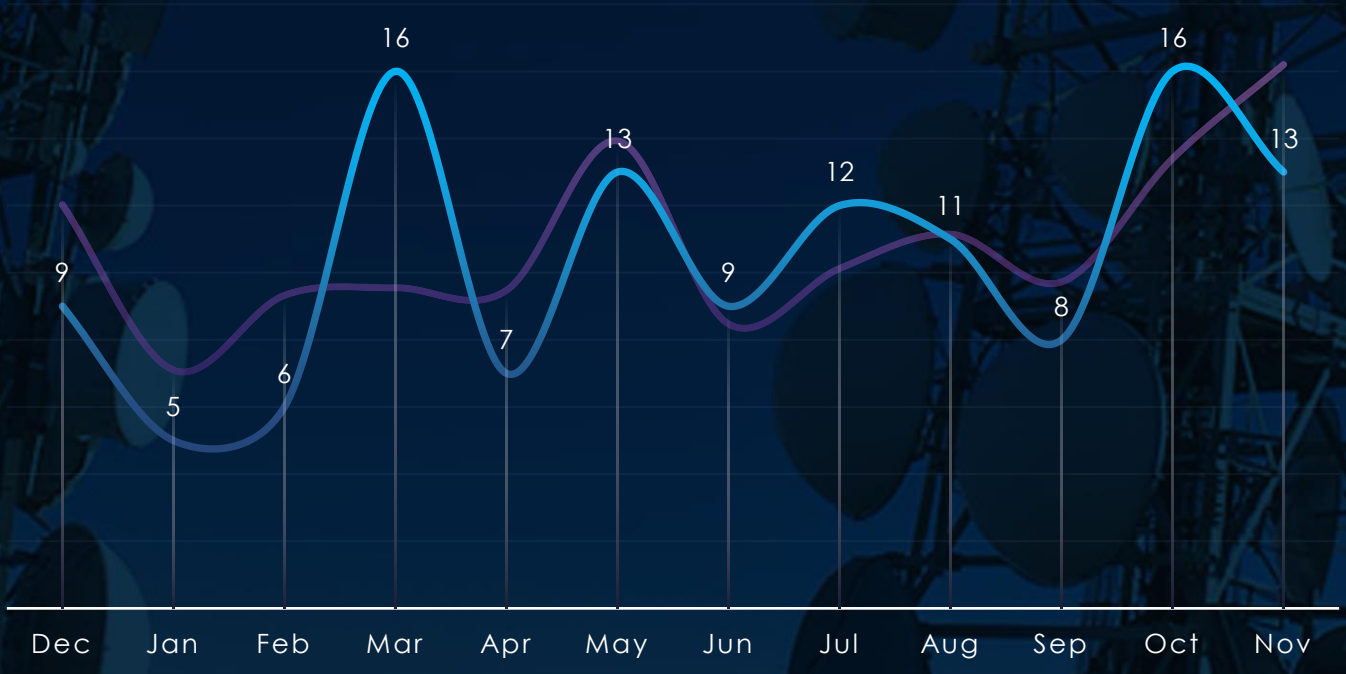
CYFIRMA
DECODING THREATS

QUARTERLY CHANGES DURING 2024



Telecommunication & media industry had very calm start of the year in first quarter. Then from second quarter onwards recorded sustained elevation until the end of the year.

INDUSTRY MONTHLY ACTIVITY CHART

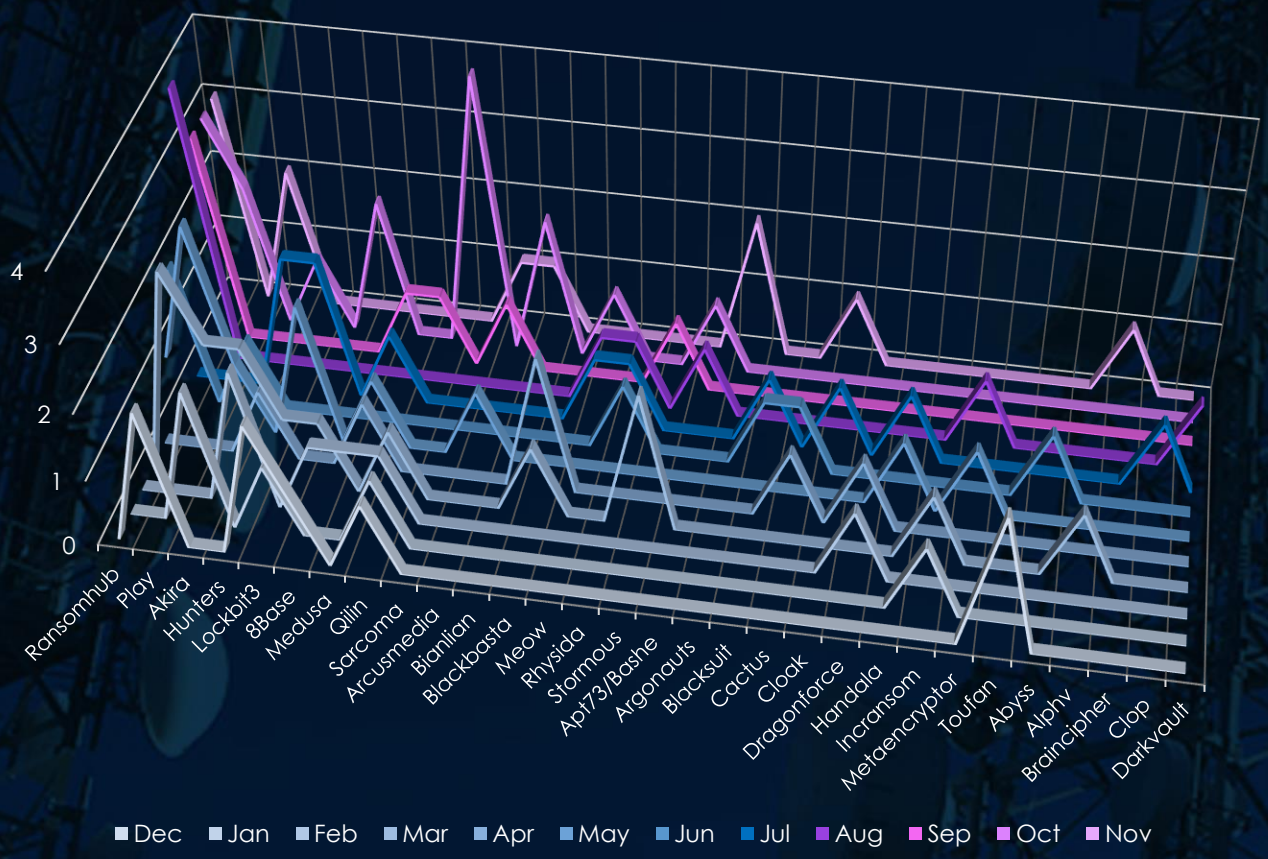


Monthly activity at large follows the scaled down global trendline. Start of the year was mildly below average, then during March this industry experience major spike in activity.

During October industry followed the global elevation, however in November it diverged and experienced tapering off.

CYFIRMA
DECODING THREATS

BREAKDOWN OF ACTIVITY PER GANG



In total 43 out of 97 gangs recorded victims in telecommunications & media technology industry, 44% participation.

A breakdown of top 30 gang's monthly activity provides insights into which gangs were active each month.

Ransomhub led activity with 16 victims, focusing on late-year operations, particularly in August through November. Play followed with 10 victims, peaking in March and May. Akira, Hunters, and Lockbit3 each accounted for 8 victims. Akira and Hunters showed consistent activity in early months, while Lockbit3 had scattered campaigns throughout the year.

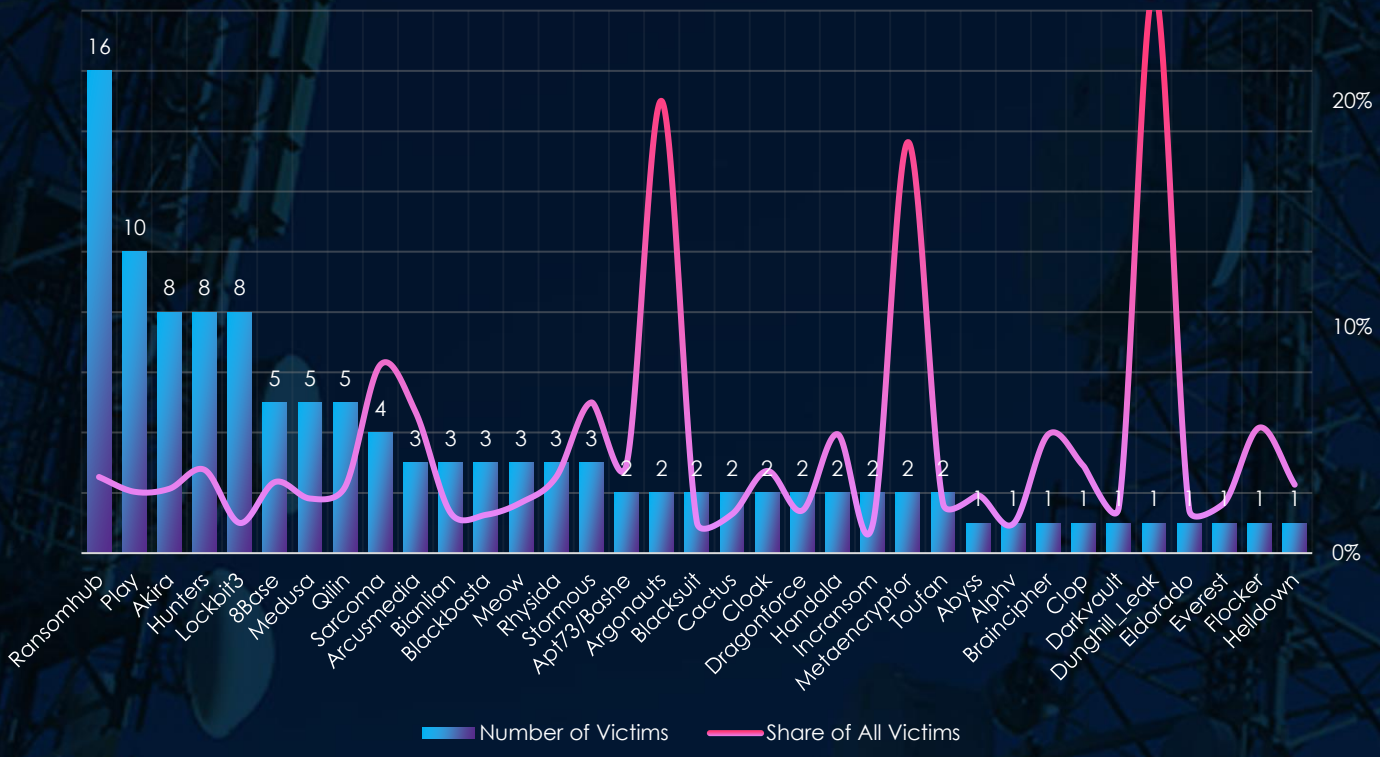
8Base, Medusa, and Qilin each targeted 5 victims, with 8Base and Medusa showing early-year activity and Qilin spreading attacks more evenly. Sarcoma targeted 4 victims exclusively in October, reflecting a late-year focus.

Smaller actors such as Arcusmedia, Bianlian, Blackbasta, and Meow (3 victims each) had isolated campaigns, with Bianlian and Blackbasta active mid-year and Meow showing late-year spikes. Emerging groups like Rhysida and Stormous also targeted 3 victims, concentrated in mid-to-late months.

Lesser groups, including Apt73/Bashe, Argonauts, and Blacksuit (2 victims each), displayed minimal activity. Single-incident actors like Abyss, Alphv, and Braincipher (1 victim each) had isolated operations, primarily late in the year.

Overall, Ransomhub dominated with a late-year surge, while Play and Akira showed consistent mid-year activity.

INDUSTRY RANSOMWARE VICTIMS PER GANG



Breaking down the top 35 gangs' victimology, the trendline of share of all victims for the most active gangs is low, implying no targeted focus on this industry.

Ransomhub leads in activity within the telecommunications and media sector, with 16 victims (3.37%), showing moderate activity but a distributed targeting strategy. Play follows with 10 victims (2.72%), while Akira and Hunters each have 8 victims (2.85% and 3.69%, respectively). Lockbit3 (8 victims, 1.34%) also shows some presence in this sector, although its focus appears broader.

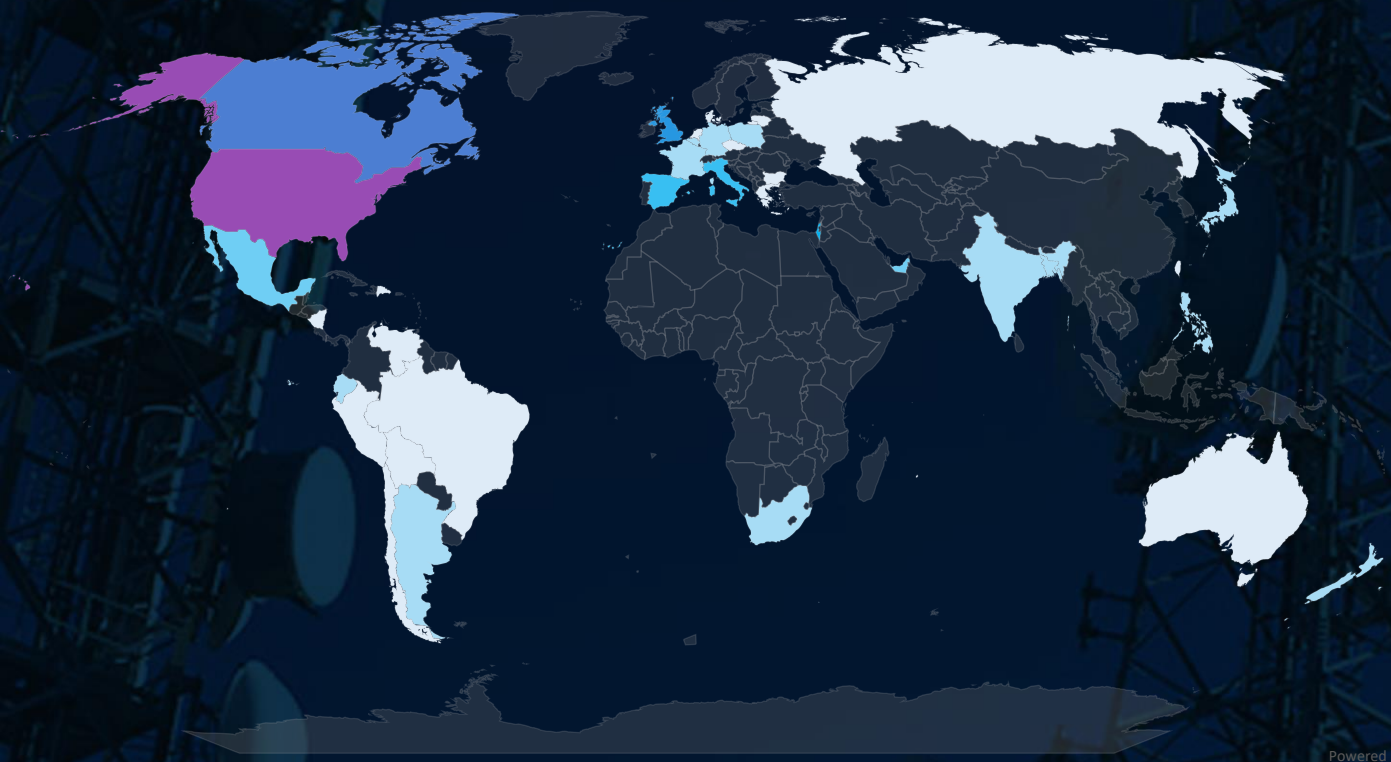
Several gangs demonstrate meaningful focus within telecommunications and media:

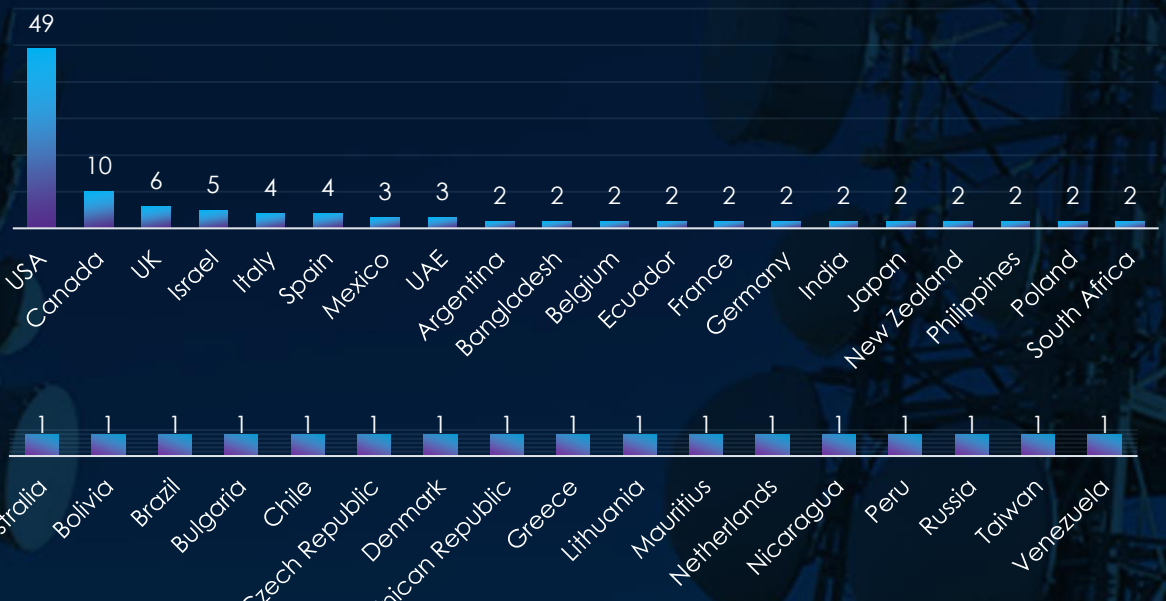
- Sarcoma (4 victims, 8.33%) shows notable targeting relative to its total activity.
- Stormous (3 victims, 6.67%) and Arcusmedia (3 victims, 6.25%) reflect similar trends of focused efforts.
- Smaller gangs like Handala (2 victims, 5.26%) and Cloak (2 victims, 3.64%) also demonstrate some level of targeting in this industry.

Certain gangs exhibit disproportionately high percentages due to low victim counts:

- Dunghill_Leak (1 victim, 25.00%) and Argonauts (2 victims, 20.00%) reflect extremely high percentages, driven by minimal activity.
- Metaencryptor (2 victims, 18.18%) shows a similarly skewed focus.
- Flocker (1 victim, 5.56%) and Braincipher (1 victim, 5.26%) also display percentages that require cautious interpretation due to their low number of victims.

GEOGRAPHIC DISTRIBUTION OF VICTIMS





The USA accounts for 39.2% of ransomware victims in the Telecommunication & Media industry in 2024. The next most affected countries are Canada with 10 victims, the UK with 6, Israel with 5, and Italy with 4.

A total of 37 countries reported victims, with 17 of them having only one victim each.

CYFIRMA
DECODING THREATS

TELECOMMUNICATIONS & MEDIA INDUSTRY EXTERNAL THREAT LANDSCAPE MANAGEMENT (ETLM) OVERVIEW

Risk Level Indicator: High/Low

APT Campaigns

The telecommunications and media industry experienced a 47% incidence rate across observed APT campaigns, driven by nation-state and financially motivated actors. Groups like MISSION2025 and Mustang Panda target espionage and infrastructure, while FIN7 and FIN11 pursue financial gain. Emerging threats from Southeast Asian actors highlight the sector's critical role in global communications and information control.

Actors: MISSION2025, Mustang Panda, Cozy Bear, FIN7, FIN11; emerging Thai- and Vietnamese-speaking TAs.

Geographic Focus: U.S., Japan, U.K.; heavy targeting in Asia-Pacific (Vietnam, Taiwan, Thailand); emerging economies like Indonesia, Philippines, Malaysia.

Targets: Web applications, operating systems, and infrastructure-as-a-service solutions.

Malware: Winnti, Cobalt Strike, PlugX; a mix of tailored and commodity malware.

Ransomware

The telecommunications and media sector accounted for 125 ransomware victims (2.40% of global total), showing a slight -2.29% year-over-year decrease. After a calm start in Q1, activity surged in March and remained elevated through Q4. Ransomhub led with late-year spikes, while other groups like Play, Akira, and LockBit3 maintained steady mid-year activity.

Victim Trends: Calm Q1; spikes in March and sustained activity through Q4, tapering in November.

Key Actors: Ransomhub (16 victims), Play (10 victims), Akira, Hunters, LockBit3 (8 each).

Geography: U.S. accounted for 39% of victims; activity recorded in 27 countries.

Insight: Ransomware activity was dispersed, with no group showing a sustained focus on this industry.

Ranking: Automotive ranked 12th as the second least frequent target of ransomware.

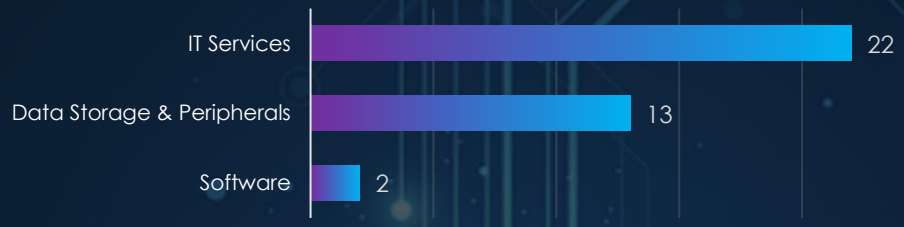
CYFIRMA
DECODING THREATS

INFORMATION TECHNOLOGY INDUSTRY IN 2024

ADVANCED PERSISTENT THREATS

Over the past 12 months, information technology organizations recorded victims across 26 of the 34 Advanced Persistent Threat (APT) campaigns observed - an incidence rate of 76%.

These victims spanned multiple segments within the information technology industry as per below:

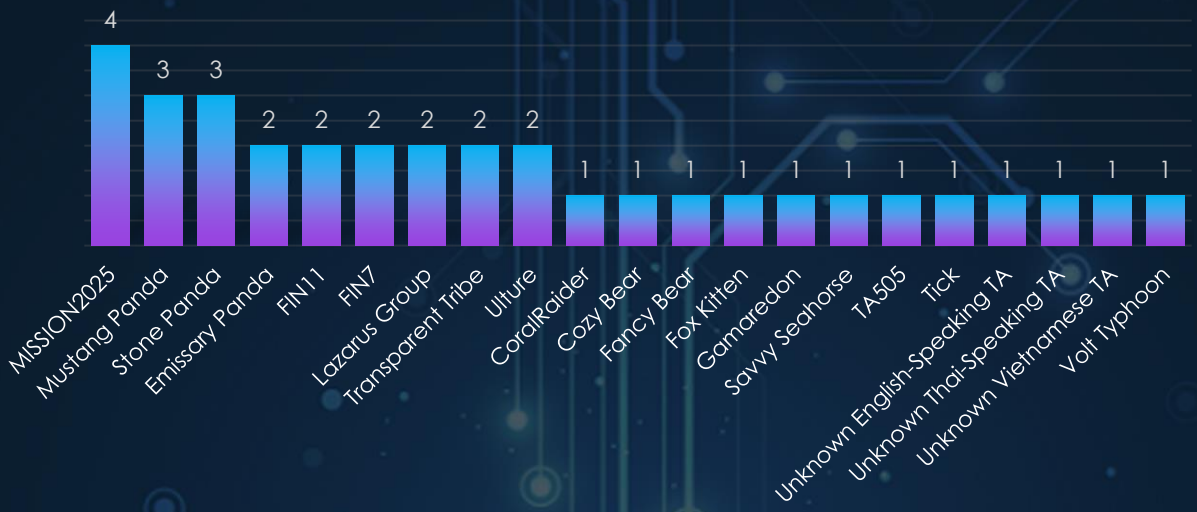


OBSERVED CAMPAIGNS PER MONTH

CYFIRMA
DECODING THREATS

APT CAMPAIGNS INFORMATION TECHNOLOGY

SUSPECTED THREAT ACTORS



The information technology industry is heavily targeted by both nation-state and financially motivated actors. MISSION2025, Mustang Panda, and Stone Panda (China) lead, focusing on espionage and intellectual property theft to support geopolitical goals.

Financially driven groups such as FIN11, FIN7, and Lazarus Group exploit the industry for ransomware and data extortion. Russian groups, including Cozy Bear, Fancy Bear, and Gamaredon, prioritize intelligence gathering and strategic disruption. Emerging actors, such as Unknown Thai and Vietnamese-Speaking TAs, and Ulture, highlight the industry's expanding threat landscape.

GEOGRAPHICAL DISTRIBUTION

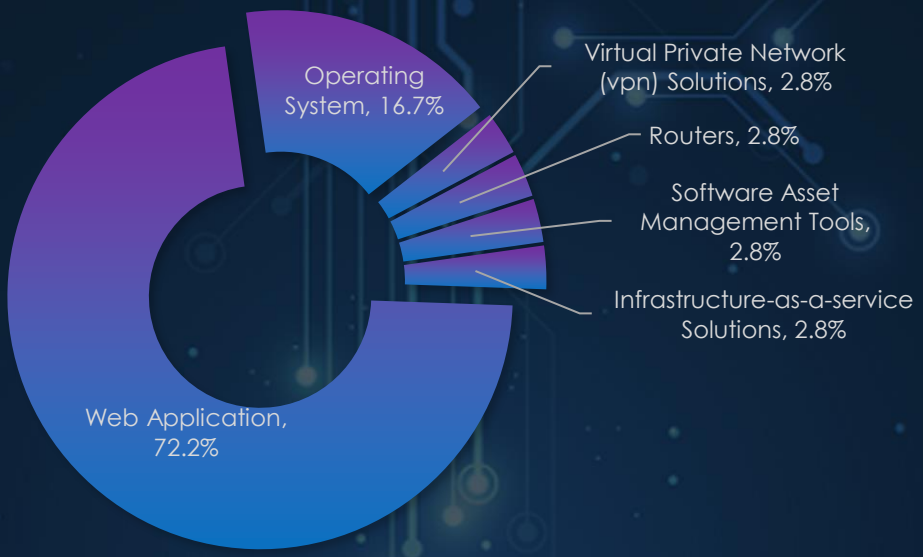
The information technology industry faces global targeting, with Japan, United States, and United Kingdom leading due to their prominence in innovation. Asia-Pacific nations like India, Taiwan, and South Korea are also heavily targeted, reflecting the region's growing IT significance.

Emerging markets such as Bangladesh and Indonesia, alongside smaller nations like Brunei and Nepal, illustrate the sector's expanding threat landscape across both established and developing regions.

CYFIRMA
DECODING THREATS

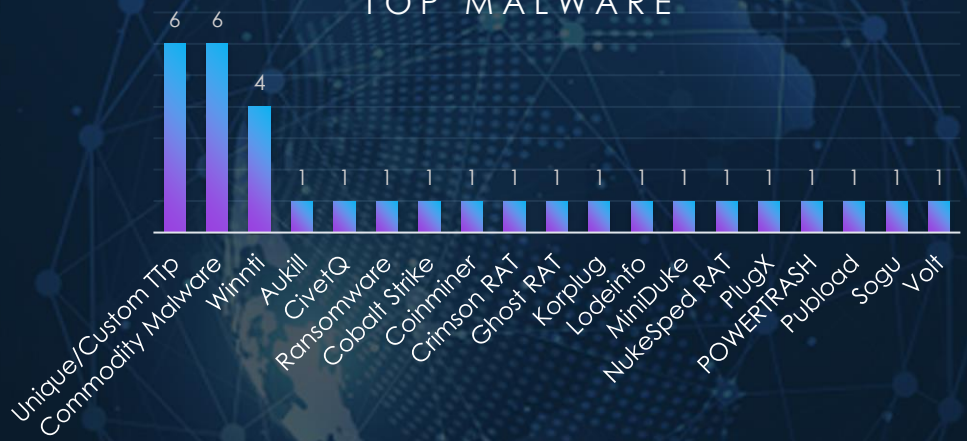
APT CAMPAIGNS
INFORMATION TECHNOLOGY

TOP ATTACKED TECHNOLOGY



The information technology industry's most targeted technologies highlight attackers' focus on foundational and internet-facing systems. Web applications dominate, emphasizing their critical role and vulnerability. Operating systems also see significant targeting due to their centrality in IT infrastructure. Additional technologies like VPN solutions, routers, and infrastructure-as-a-service solutions reflect attackers' interest in exploiting essential tools that support modern IT environments.

TOP MALWARE



The malware targeting the information technology industry reflects a blend of tailored and widely available tools. Unique/Custom TTPs and Commodity Malware lead, emphasizing the balance between targeted sophistication and accessibility.

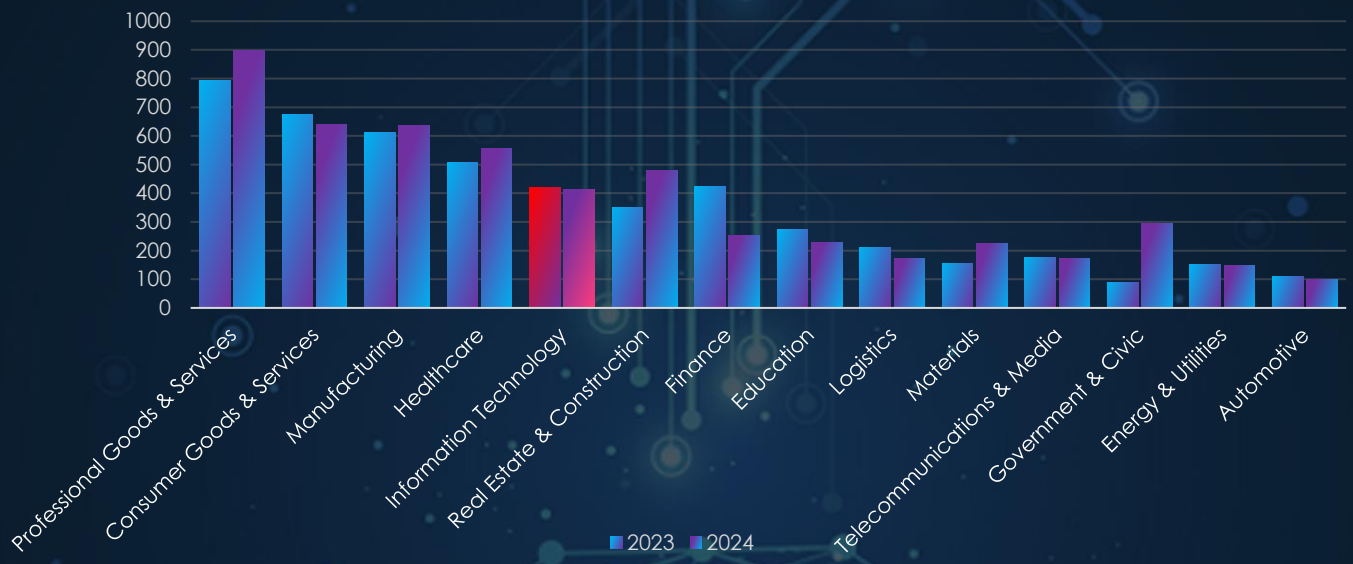
Winnti highlights its persistent use for espionage and data theft, while tools like Cobalt Strike, Ransomware, and PlugX showcase versatility for financial extortion and infiltration. Lesser-used malware such as Coinminer and Crimson RAT indicate niche but impactful operations, underscoring the sector's exposure to both advanced and opportunistic threats.

CYFIRMA
DECODING THREATS

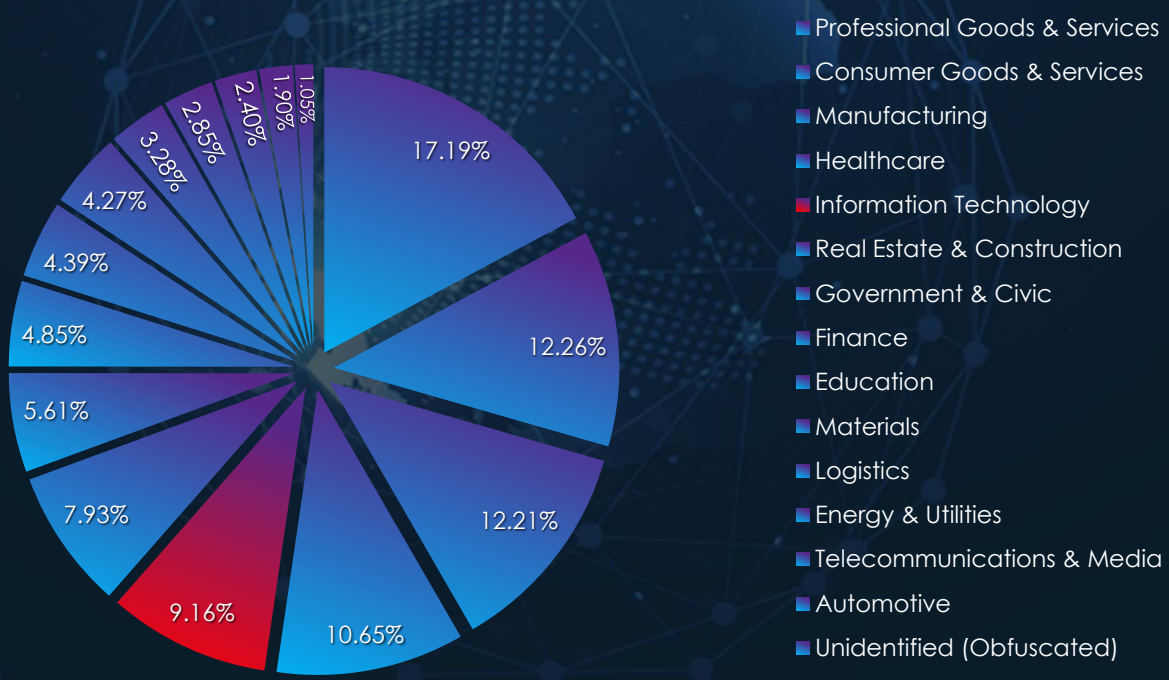
RANSOMWARE VICTIMOLOGY INFORMATION TECHNOLOGY

In the past 12 months, CYFIRMA has identified 478 verified information technology industry ransomware victims. This accounts for 9.16% of the overall total of 5,219 ransomware victims during the same period.

GLOBAL DISTRIBUTION BY INDUSTRY

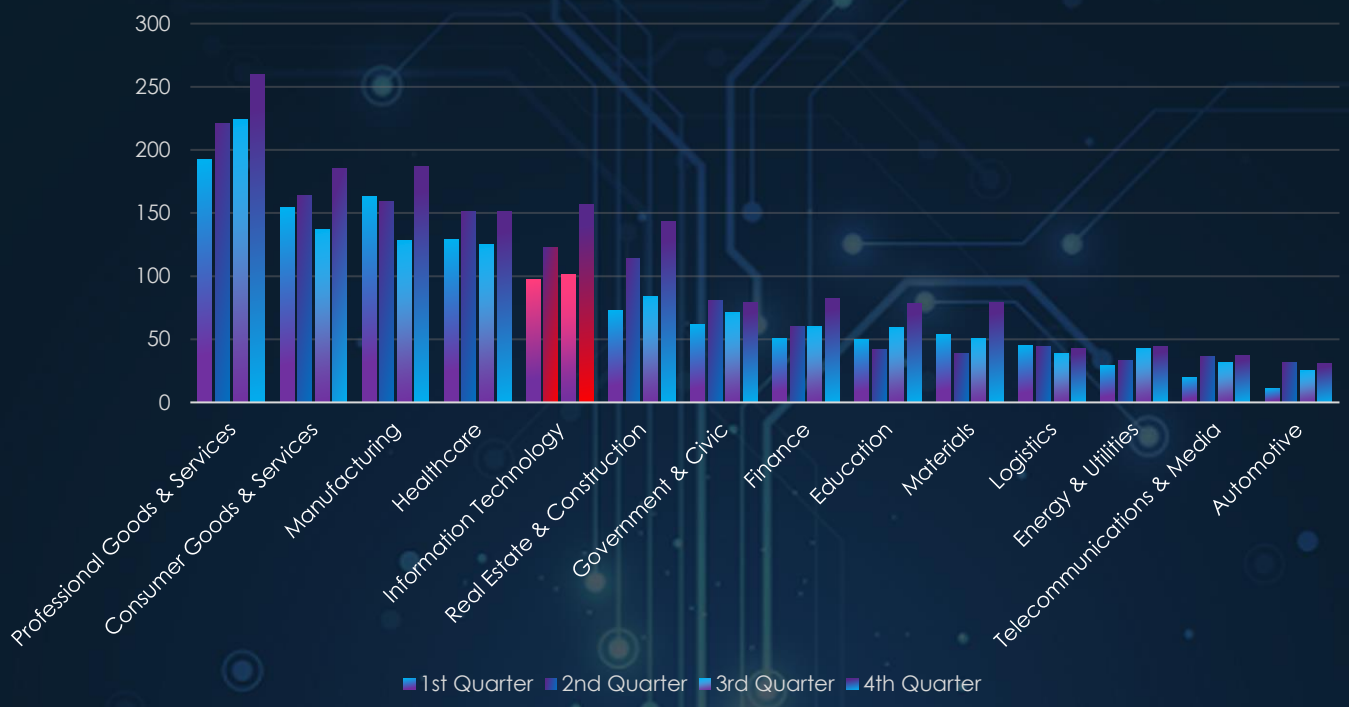


The industry recorded remarkably consistent number of recorded victims, just very minor 1.66% decrease from previous year. And ranked at 5th place for both years combined. Industry moved up from 6th to 5th place during 2024 as fifth most frequent victim.



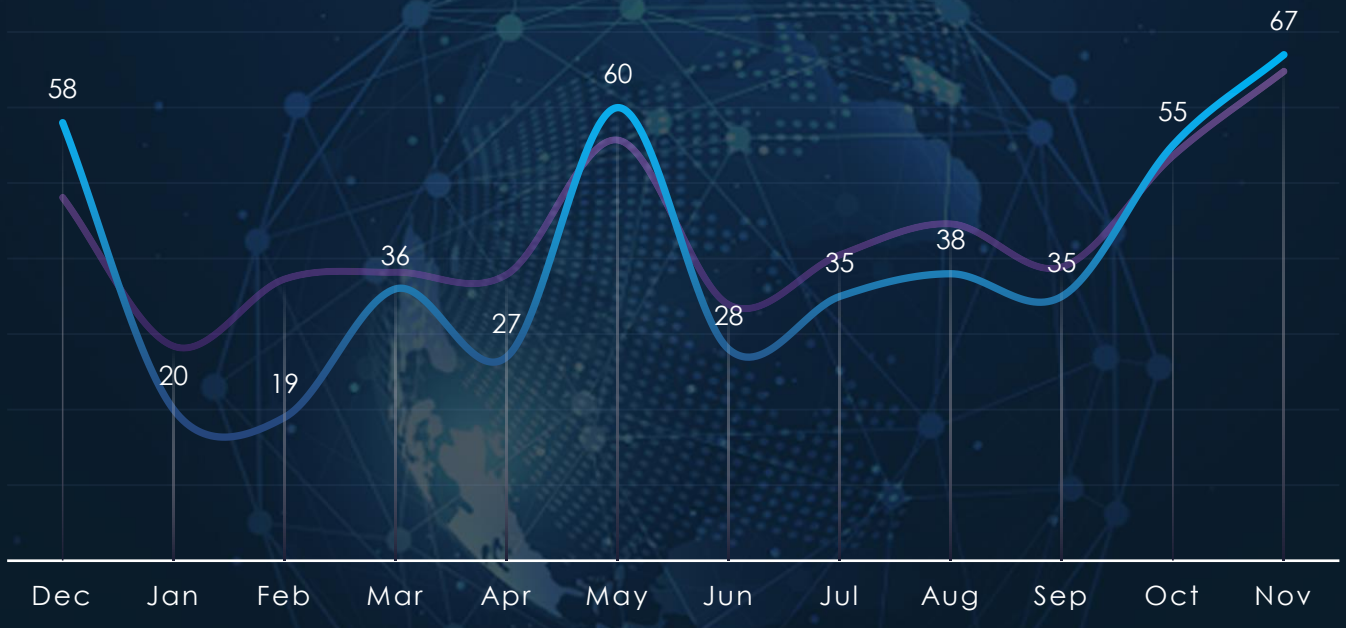
CYFIRMA
DECODING THREATS

QUARTERLY CHANGES DURING 2024



Information technology industry experienced alternating activity, first and second quarters were relatively calmer. Third and especially fourth quarters recorded elevated numbers.

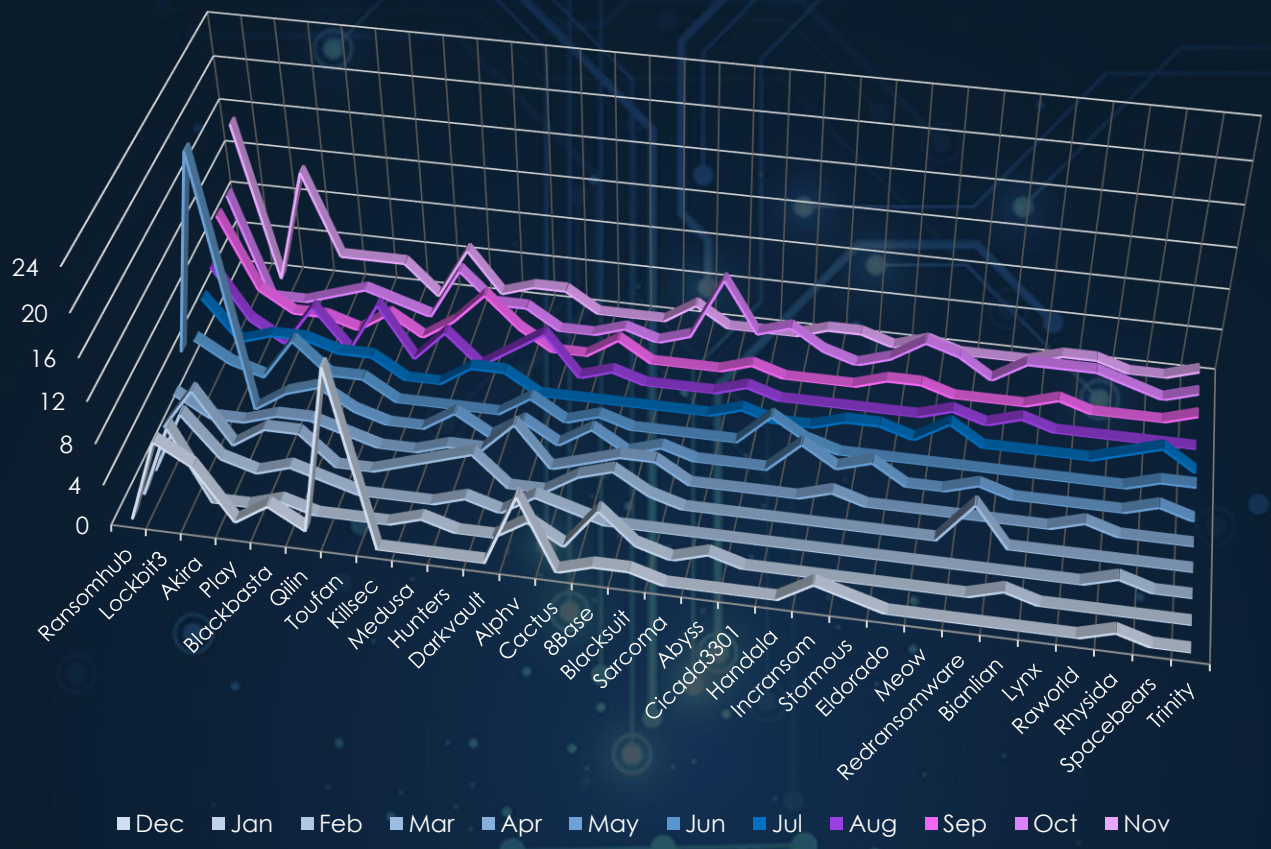
INDUSTRY MONTHLY ACTIVITY CHART



Monthly activity nearly perfectly follows the scaled down global trendline. There is only minor below average dip in January and February. By the end of the year during October and November number of victims sharply rose, which suggests elevation into 2025.

CYFIRMA
DECODING THREATS

BREAKDOWN OF ACTIVITY PER GANG



In total 67 out of 97 gangs recorded victims in information technology industry, 69% participation.

Ransomhub led ransomware activity with 62 victims, showing a sharp increase from August onward and peaking in November (15 victims). Lockbit3 closely followed with 61 victims, maintaining steady activity throughout the year, with a significant spike in May (24 victims).

Akira and Play each targeted 26 victims. Akira was most active in November (11 victims), while Play had consistent activity across the year, peaking in July (5 victims). Blackbasta (23 victims) demonstrated steady activity, with notable spikes in May and November.

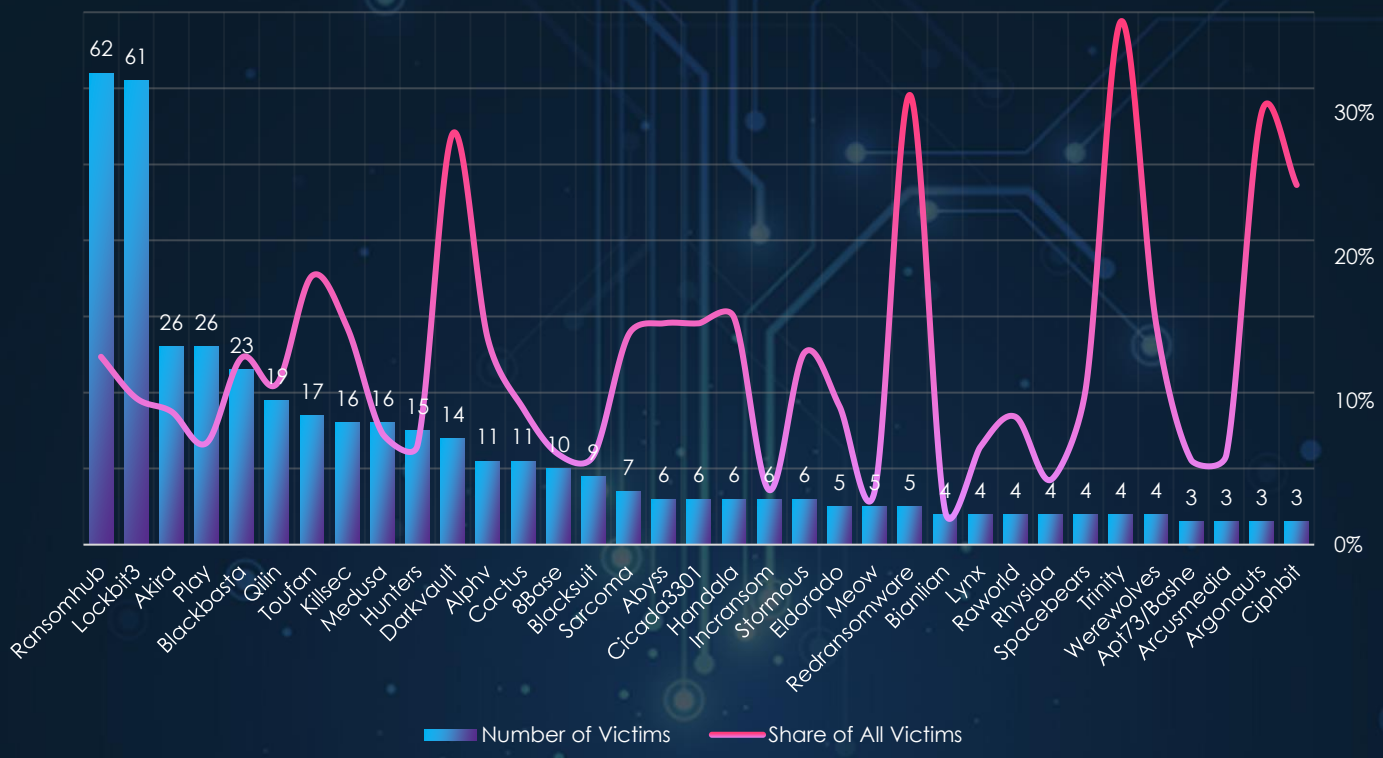
Qilin targeted 19 victims, with activity intensifying in August and November. Toufan published 17 victims in December. Killsec and Medusa each accounted for 16 victims, with Killsec peaking in September and October, while Medusa saw consistent activity late in the year.

Hunters and Darkvault (15 and 14 victims, respectively) maintained steady but lower activity, with Darkvault peaking in April and Hunters spreading its efforts across multiple months. Alphv and Cactus each targeted 11 victims, with Alphv active early in the year and Cactus peaking in May and September.

Large groups like 8Base (10 victims) and Blacksuit (9 victims) showed limited campaigns, with activity scattered throughout the year. Sarcoma (7 victims) conducted its operations exclusively in October. Other groups, such as Abyss, Cicada3301, and Handala (6 victims each), demonstrated sporadic, concentrated campaigns.

Emerging actors like Eldorado, Meow, and Redransomware targeted 5 victims each, while smaller gangs such as Lynx and Rhysida (4 victims each) had isolated operations.

INDUSTRY RANSOMWARE VICTIMS PER GANG



Reviewing the top 35 gangs, Ransomhub and Lockbit3 dominate ransomware activity within the IT sector, with 62 victims (13.05%) and 61 victims (10.18%), respectively. Their substantial victim counts highlight significant targeting efforts in this industry. Akira and Play, each with 26 victims (9.25% and 7.07%, respectively), also exhibit notable activity, though with less focus than the leading gangs.

Several gangs demonstrate concentrated targeting efforts within IT:

• Toufan (17 victims, 18.68%) and Killsec (16 victims, 15.09%) indicate strong focus within the IT sector.

• Darkvault (14 victims, 28.57%) and Redransomware (5 victims, 31.25%) show strikingly high percentages, reflecting a concentrated targeting strategy despite smaller victim counts.

• Other gangs such as Alphv (11 victims, 14.29%), Sarcoma (7 victims, 14.58%), and Werewolves (4 victims, 15.38%) also indicate strong focus.

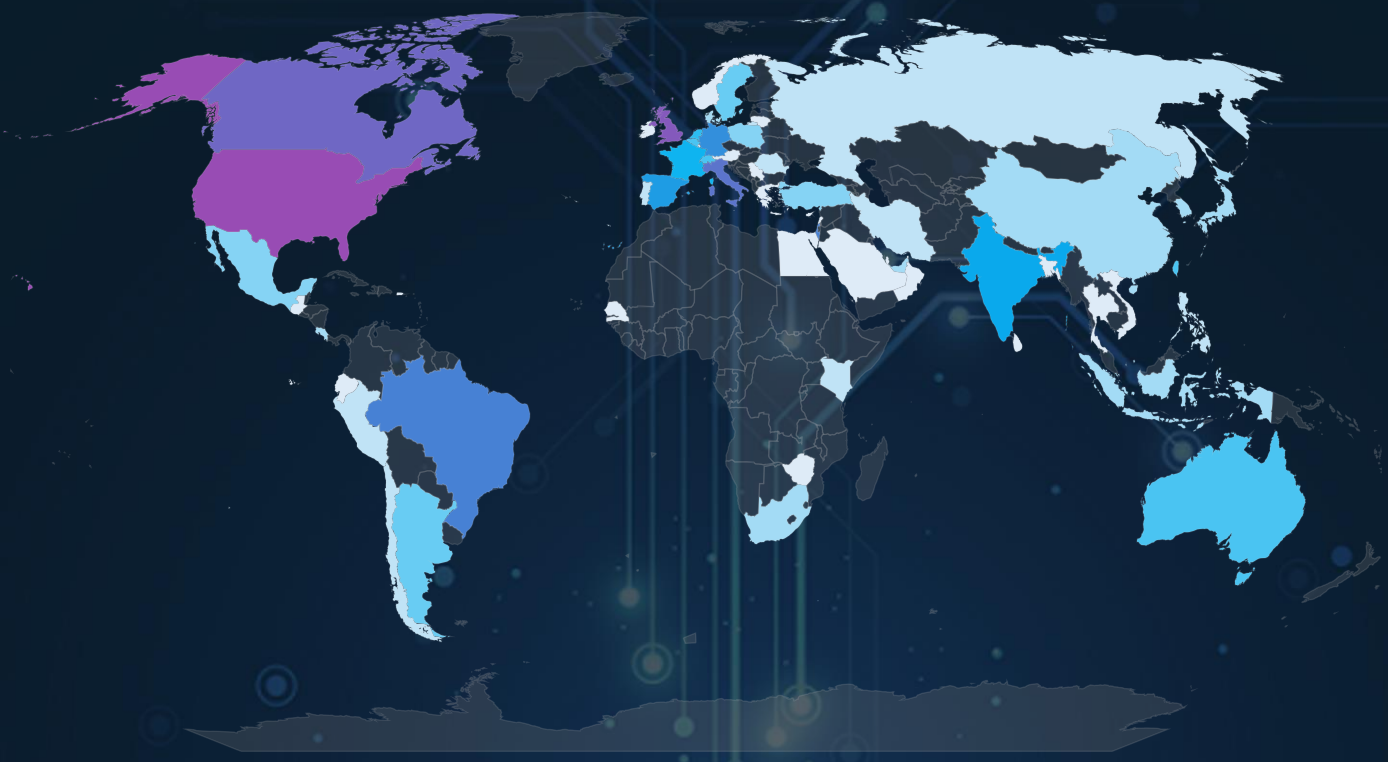
Some gangs exhibit disproportionately high percentages due to low victim counts:

• Trinity (4 victims, 36.36%) and Argonauts (3 victims, 30.00%) reflect extremely high percentages despite minimal activity.

• Ciphbit (3 victims, 25.00%) and Darkvault (14 victims, 28.57%) show similarly skewed focus due to their limited number of victims.

• Redransomware (5 victims, 31.25%) and Handala (6 victims, 15.79%) demonstrate elevated percentages that require careful interpretation given their low absolute numbers.

GEOGRAPHIC DISTRIBUTION OF VICTIMS



The USA accounts for 41% of ransomware victims in the Information Technology industry in 2024. The next most affected countries are the UK with 30 victims, Canada with 23, Italy with 20, and Brazil with 18.

A total of 63 countries reported victims, with 26 of them having only one victim each.

CYFIRMA
DECODING THREATS

INFORMATION TECHNOLOGY INDUSTRY EXTERNAL THREAT LANDSCAPE MANAGEMENT (ETLM) OVERVIEW

Risk Level Indicator: High

APT Campaigns

The information technology industry recorded a 76% incidence rate across observed APT campaigns, with threats driven by both nation-state and financially motivated actors. Groups like MISSION2025 and Stone Panda target intellectual property and geopolitical objectives, while FIN7 and FIN11 focus on ransomware and data extortion. Emerging threats from Southeast Asian actors highlight the industry's growing vulnerability.

Actors: MISSION2025, Mustang Panda, Stone Panda, FIN7, Cozy Bear, emerging Southeast Asian TAs.

Geographic Focus: U.S., Japan, U.K.; heavy targeting in Asia-Pacific (India, Taiwan, South Korea); emerging markets like Philippines and Indonesia.

Targets: Web applications, operating systems, VPN solutions, routers, IaaS.

Malware: Winnti, Cobalt Strike, PlugX, Coinminer, Crimson RAT.

Ransomware

The IT sector accounted for 478 ransomware victims (9.16% of global total), showing a slight -1.66% year-over-year decrease and ranking 5th in targeted industries. Activity intensified in Q3 and Q4, with October and November showing sharp increases, signaling continued risks into 2025.

Victim Trends: Calm Q1/Q2; spikes in Q3/Q4, peaking in November.

Key Actors: Most active were Ransomhub (62 victims, peak in November), LockBit 3 (61 victims, peak in May). Most consistent were Akira (26 victims, peak in November), Play (26 victims, peak in July).

Geography: U.S. accounted for 41% of victims; activity recorded in 63 countries.

Insights: Ransomhub and Blackbasta showed the highest share of victims in IT (13% each), with niche groups like Darkvault and Redransomware recording 28%-36% of their targets in IT.

Ranking: IT Industry ranked 5th most frequent target of ransomware.

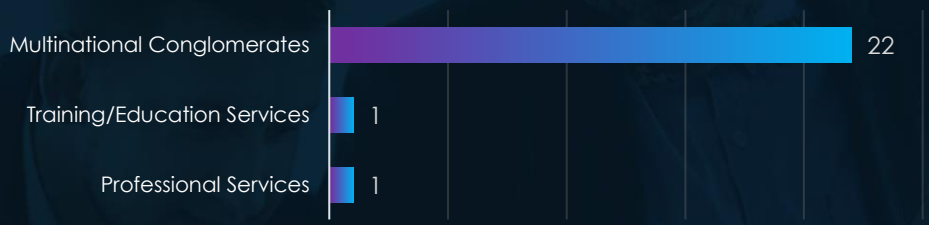
CYFIRMA
DECODING THREATS

PROFESSIONAL GOODS & SERVICES INDUSTRY IN 2024

ADVANCED PERSISTENT THREATS

Over the past 12 months, professional goods & services organizations recorded victims across 23 of the 34 Advanced Persistent Threat (APT) campaigns observed - an incidence rate of 68%.

These victims spanned multiple segments within the professional goods & services industry as per below:

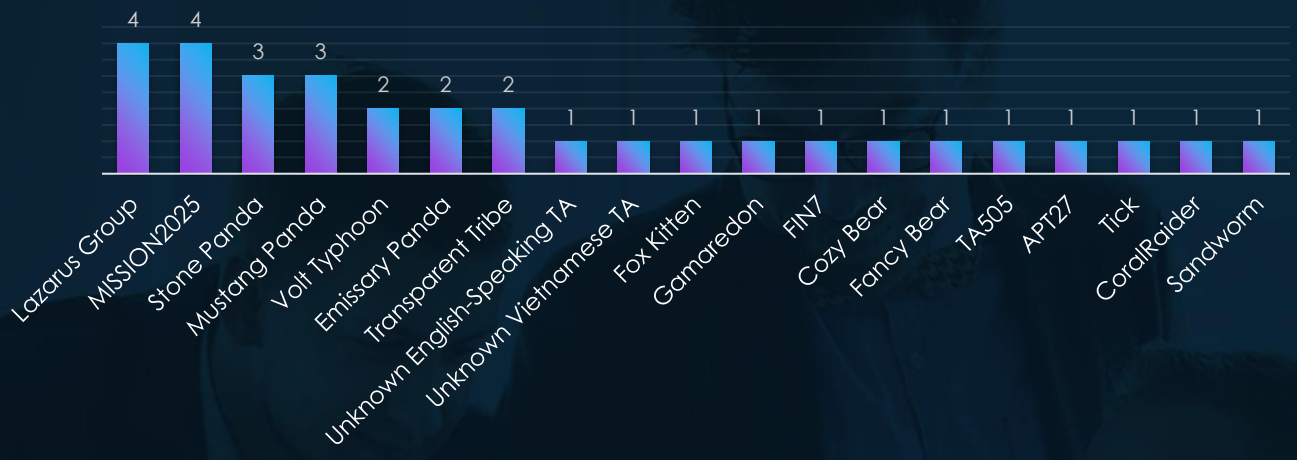


OBSERVED CAMPAIGNS PER MONTH

CYFIRMA
DECODING THREATS

APT CAMPAIGNS
PROFESSIONAL GOODS & SERVICES

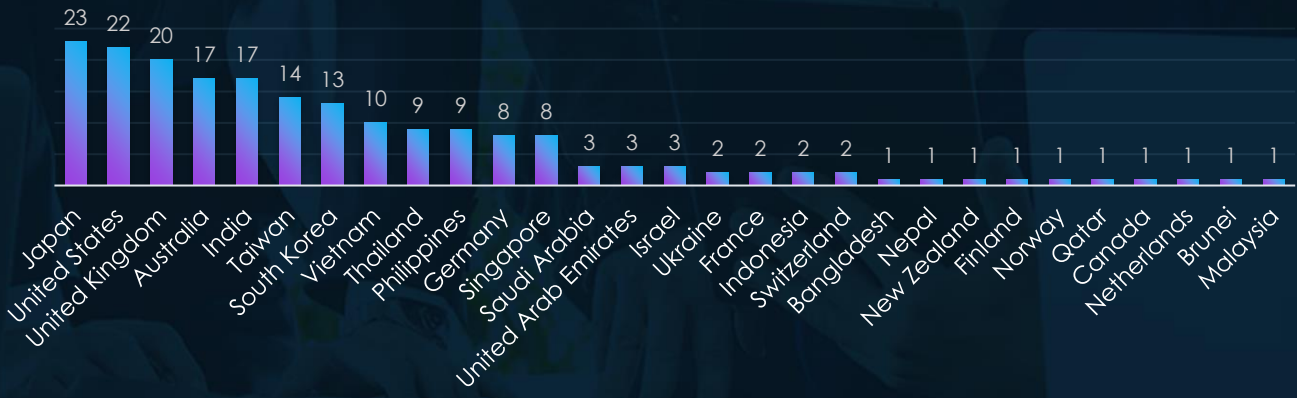
SUSPECTED THREAT ACTORS



The Professional Goods & Services industry is targeted by a mix of nation-state and financially motivated actors. Chinese groups, including Lazarus Group, MISSION2025, Stone Panda, and Mustang Panda, dominate, focusing on espionage and intellectual property theft. Russian actors such as Cozy Bear, Fancy Bear, and Gamaredon prioritize intelligence gathering and strategic disruption. F

Financially motivated groups like FIN7 and TA505 exploit the sector for data extortion and ransomware. Lesser-known or emerging actors, such as Unknown Vietnamese TA and Fox Kitten, reflect the industry's appeal to a growing range of adversaries.

GEOGRAPHICAL DISTRIBUTION



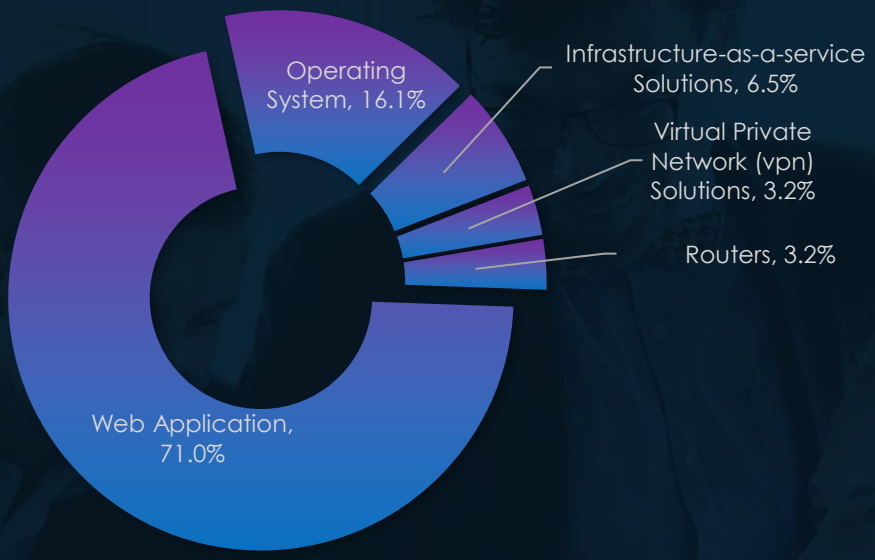
The Professional Goods & Services industry is globally targeted, with Japan, United States, and United Kingdom leading due to their prominence in the sector. Asia-Pacific nations, including India, Taiwan, and South Korea, also feature prominently, reflecting the region's growing professional goods & services industry.

Emerging markets such as Vietnam, Philippines, and Indonesia highlight the attackers' expanding interest in developing economies. The inclusion of smaller nations like Finland, Qatar, and Brunei demonstrates the broadening scope of threats, targeting both established and emerging markets across the globe.

CYFIRMA
DECODING THREATS

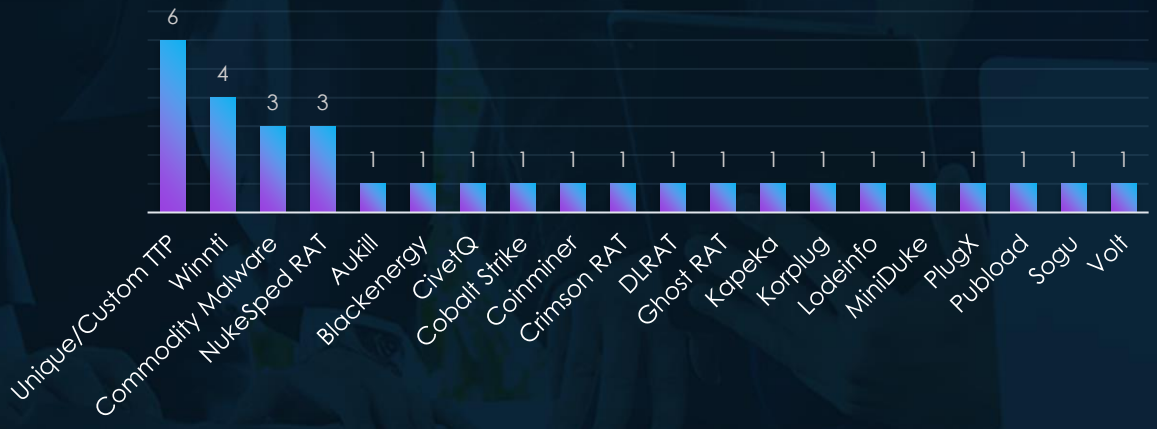
APT CAMPAIGNS
PROFESSIONAL GOODS & SERVICES

TOP ATTACKED TECHNOLOGY



Web applications dominate, reflecting their vulnerability as internet-facing systems integral to business operations. Operating systems are also heavily targeted, underscoring their foundational role in infrastructure. Additionally, infrastructure-as-a-service solutions, VPN solutions, and routers appear as key targets.

TOP MALWARE



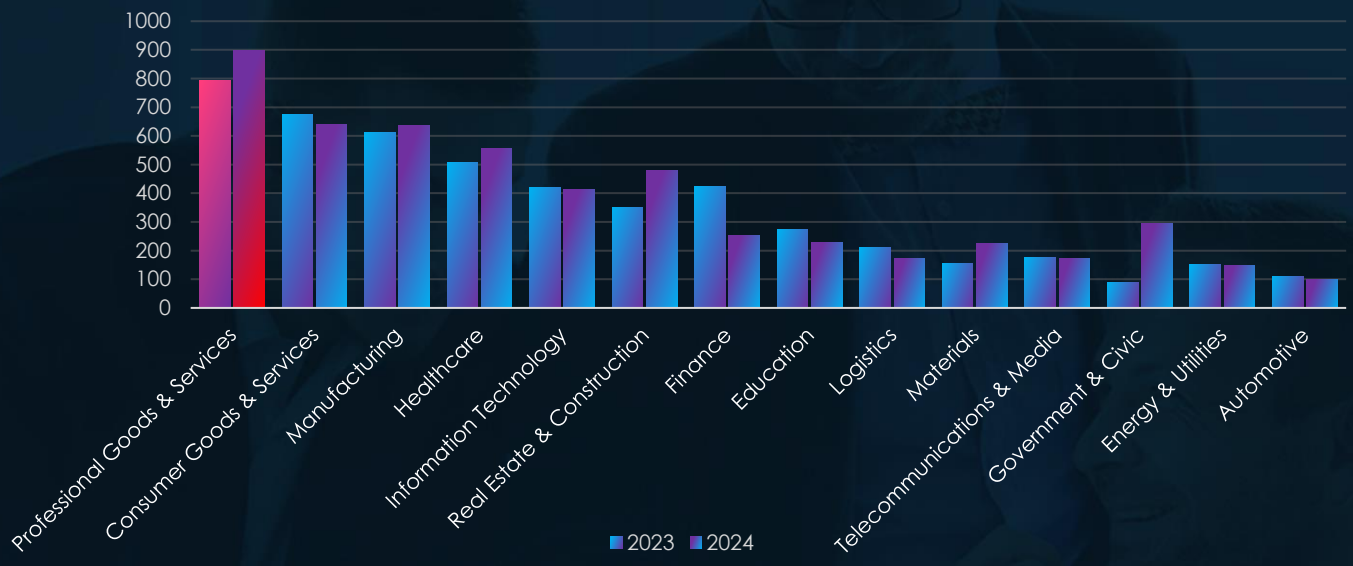
The industry faces a diverse range of malware threats, blending sophisticated custom tools with widely used strains. Unique/Custom TTPs lead, reflecting attackers' tailored approaches to exploit vulnerabilities. Winnti and NukeSped RAT highlight their persistent use for espionage and long-term infiltration.

Tools like Cobalt Strike and PlugX underscore versatility for data theft and system compromise, while niche malware such as Coinminer and Crimson RAT indicate opportunistic campaigns.

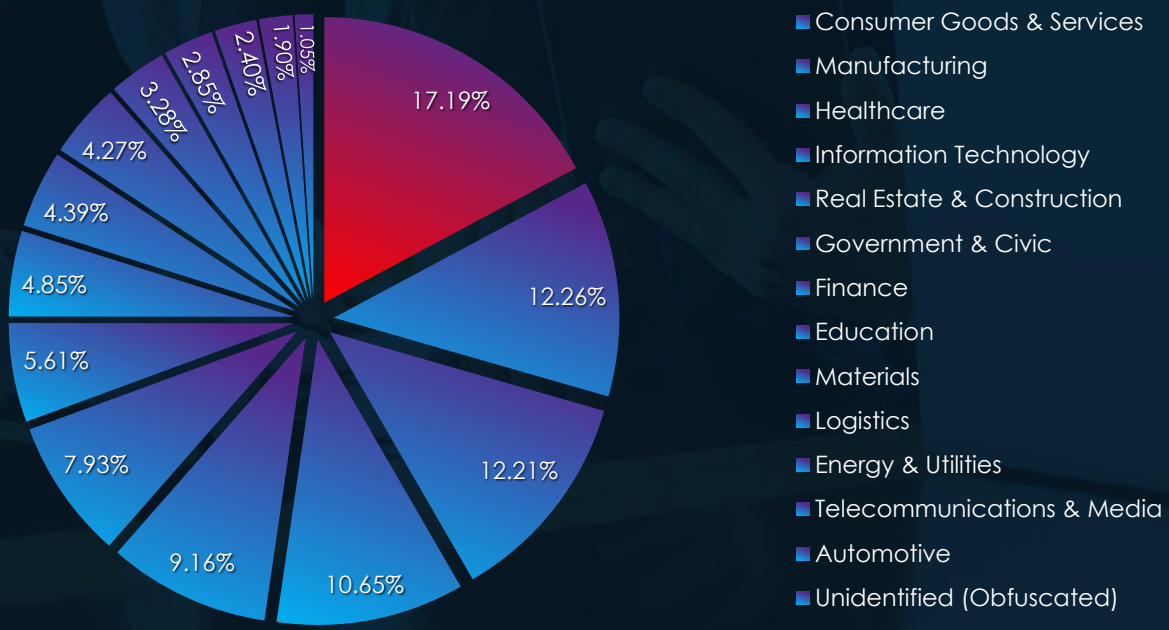
RANSOMWARE VICTIMOLOGY PROESSFIONAL GOODS & SERVICES

In the past 12 months, CYFIRMA has identified 897 verified professional goods & services industry ransomware victims. This accounts for 17.19% of the overall total of 5,219 ransomware victims during the same period.

GLOBAL DISTRIBUTION BY INDUSTRY

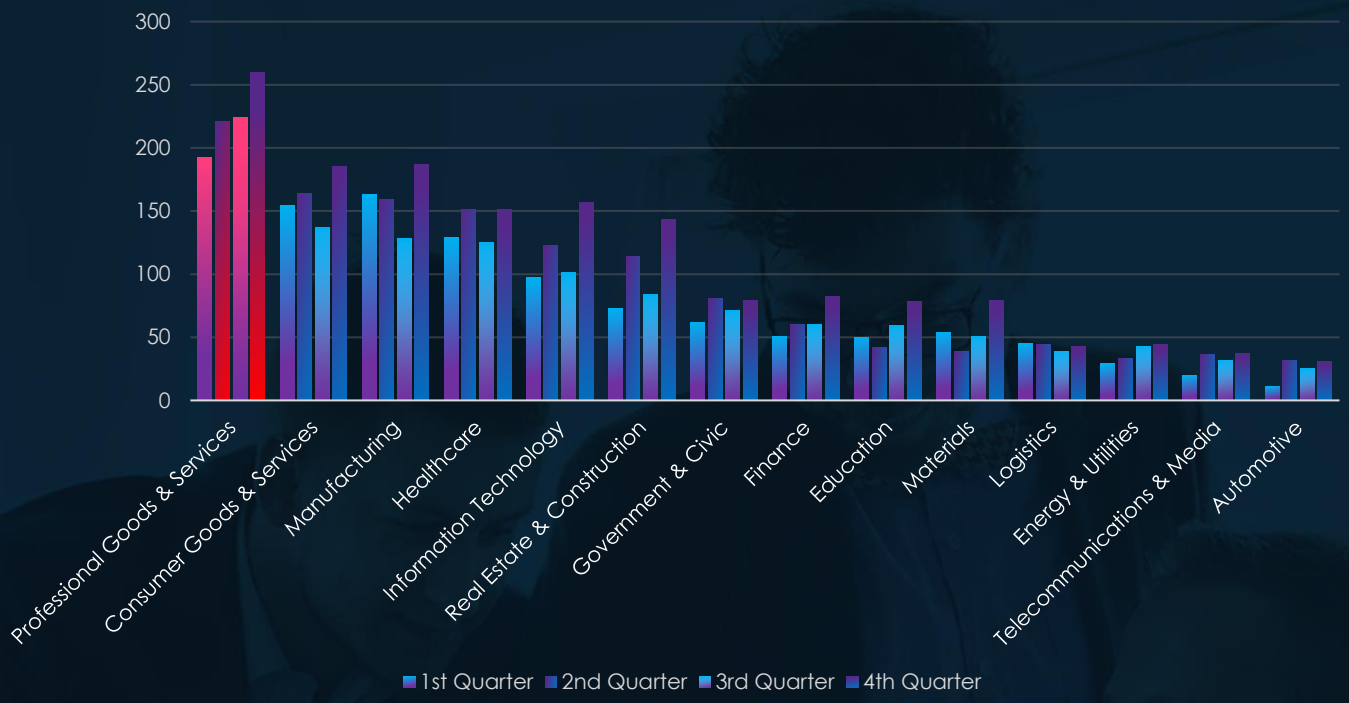


The industry recorded consistently high and growing number of recorded victims, with 11.48% increase from previous year. It ranked at 1st place for both years combined as well as 1st for both consecutive years as the most frequent victims of ransomware.



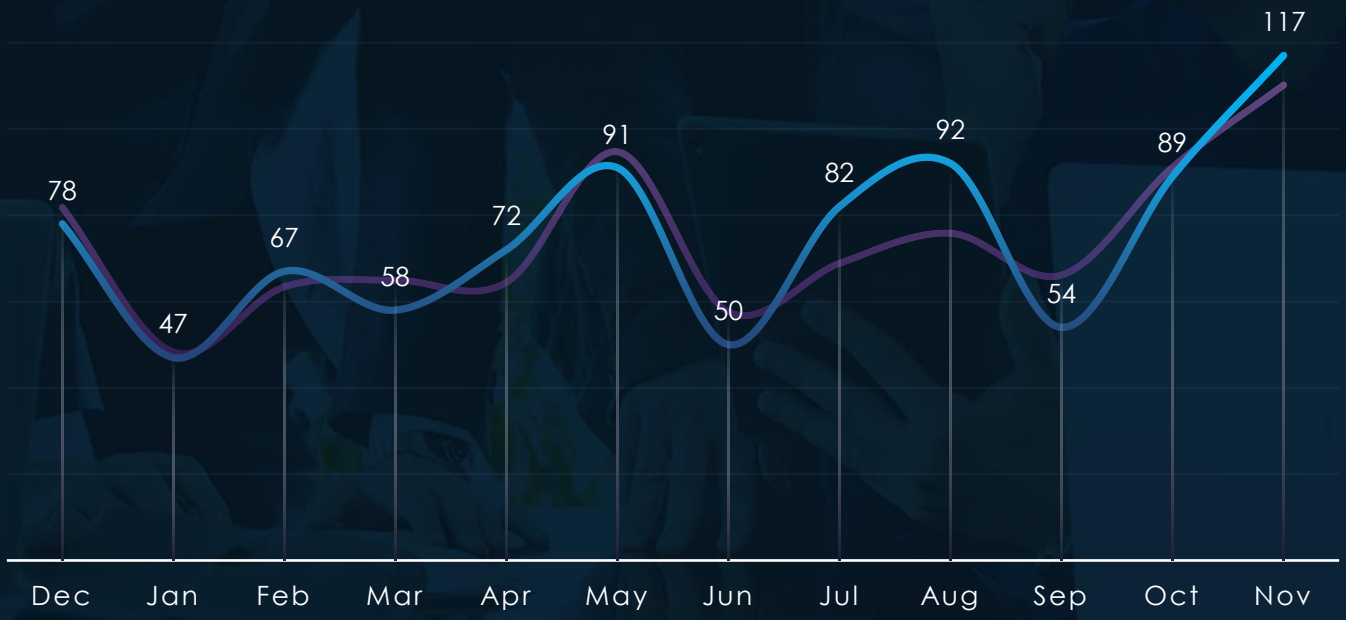
CYFIRMA
DECODING THREATS

QUARTERLY CHANGES DURING 2024



Professional goods & services industry experienced gradual growth from quarter to quarter, further cementing the industry as the most frequent target of ransomware.

INDUSTRY MONTHLY ACTIVITY CHART



Monthly activity nearly perfectly follows the scaled down global trendline. There is mild above average spike in July and August. By the end of the year during October and November number of victims sharply rose in line with global activity, implying elevation into 2025.

CYFIRMA
DECODING THREATS

BREAKDOWN OF ACTIVITY PER GANG

In total 74 out of 97 gangs recorded victims in telecommunications & media technology industry, 76% participation.

A breakdown of top 30 gang's monthly activity provides insights into which gangs were active each month.

Lockbit3 dominated ransomware activity with 95 victims, peaking in February (19 victims). Ransomhub followed with 75 victims, showing increasing activity from August onward, peaking in November (17 victims).

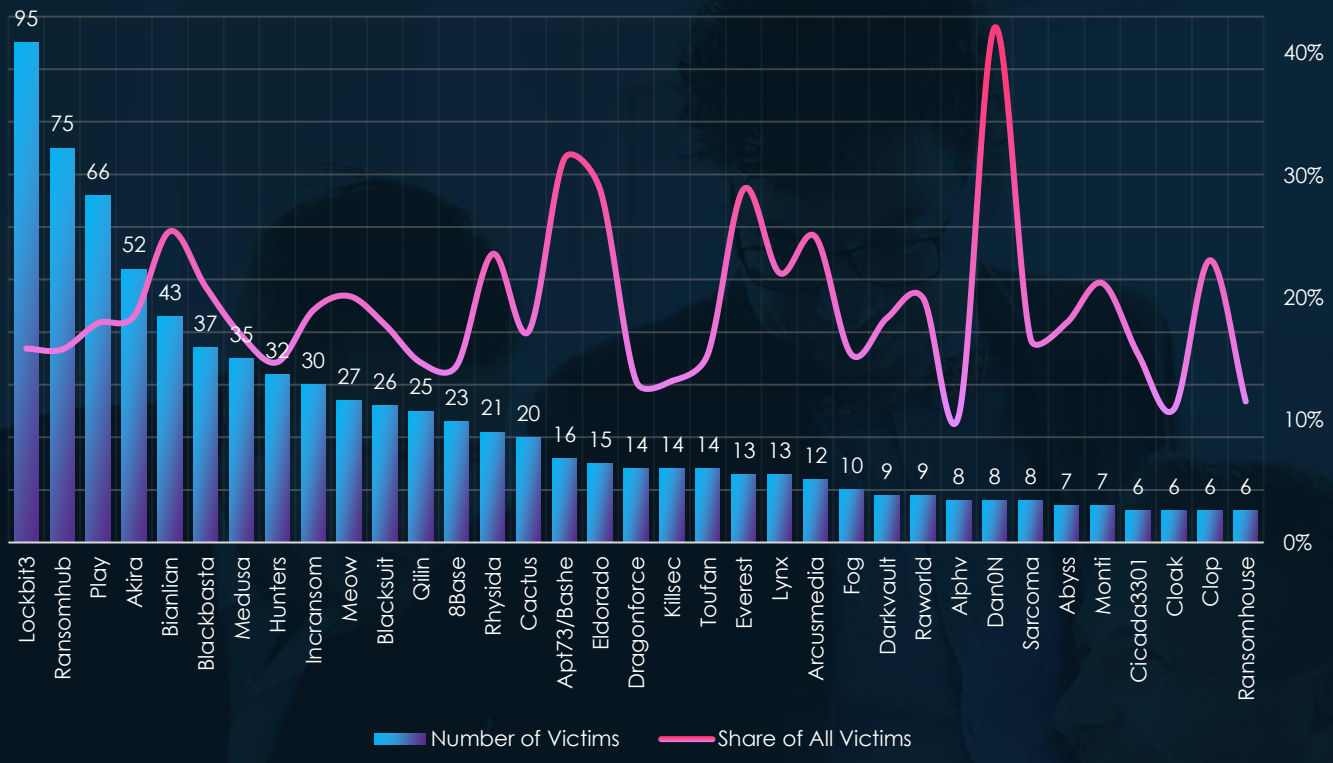
Play targeted 66 victims, maintaining steady activity with peaks in February, March, and November (7 victims each). Akira impacted 52 victims, showing a late-year surge in November (18 victims) and consistent activity in May (10 victims). Bianlian (43 victims) demonstrated moderate activity throughout the year, peaking in February and September.

Blackbasta and Medusa (37 and 35 victims, respectively) maintained steady activity, with Blackbasta active early in the year and Medusa showing consistent operations across multiple months. Hunters (32 victims) and Incransom (30 victims) exhibited scattered campaigns, with notable spikes for Hunters in July and for Incransom in January and November.

Emerging groups like Meow (27 victims) peaked in late summer and fall, particularly August and October, while Blacksuit (26 victims) maintained activity throughout the year, with a late peak in September. Qilin (25 victims) concentrated activity in April and November, while 8Base (23 victims) peaked early in the year.

Smaller groups such as Rhysida (21 victims), Cactus (20 victims), and Eldorado (15 victims) showed intermittent campaigns. Notable isolated surges include Toufan's December victims dump and Sarcoma's October focus (8 victims).

INDUSTRY RANSOMWARE VICTIMS PER GANG



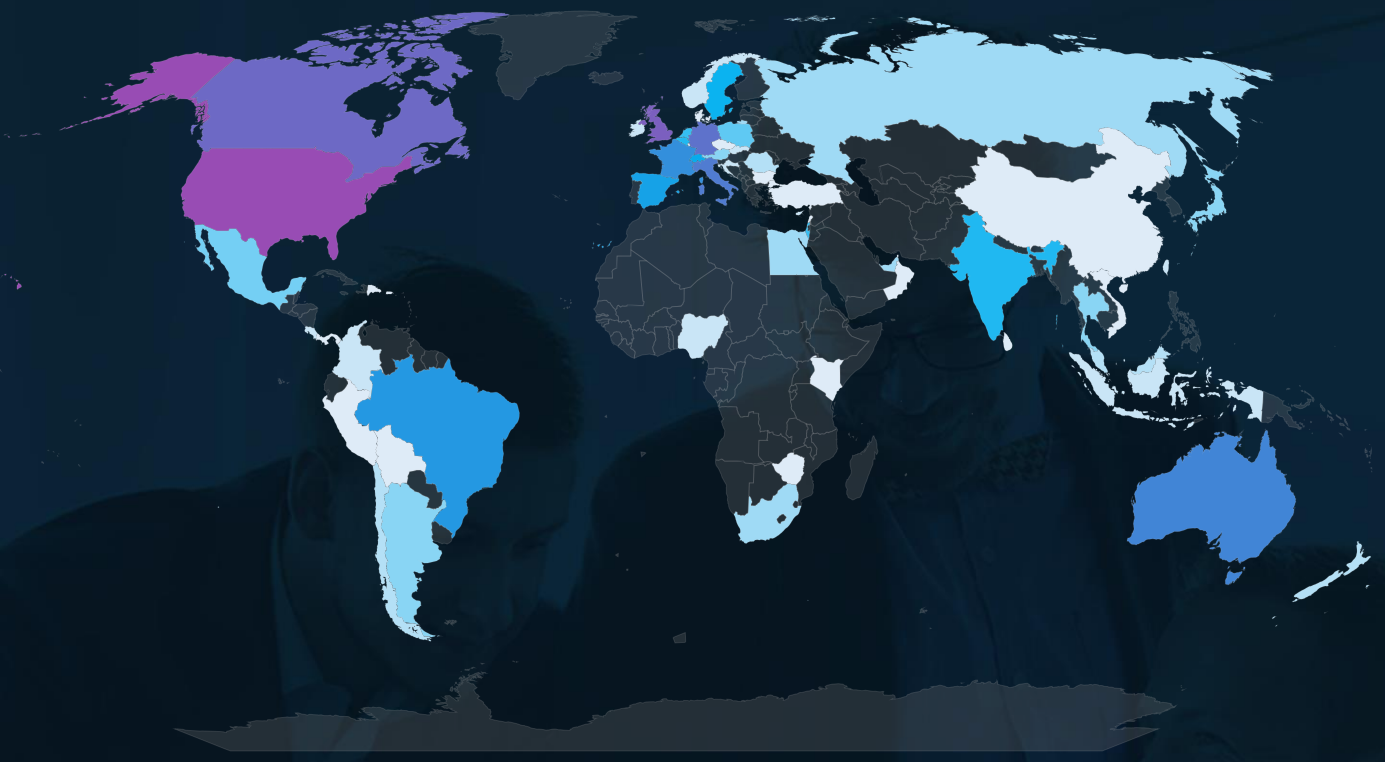
Looking at the top 35 gangs, the share of all victims in this industry is above 10% for all top 35 gangs. The top 5 trendline of the share of all victims starts at 15% and tops 25% for Bianlian gang.

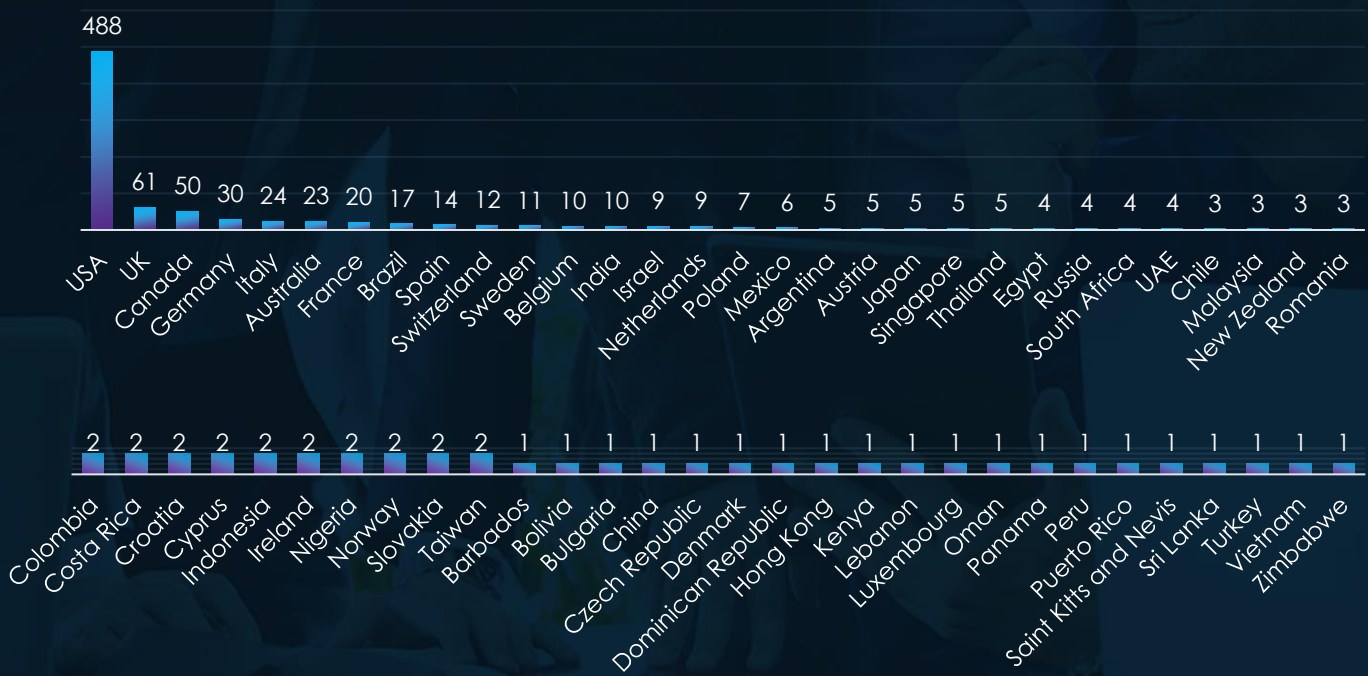
Lockbit3 and Ransomhub lead ransomware activity within this sector, with 95 victims (15.86%) and 75 victims (15.79%), respectively, highlighting significant targeting. Play (66 victims, 17.93%) and Akira (52 victims, 18.51%) also show substantial activity and strong focus on the professional goods and services industry.

Several gangs demonstrate substantial focus on this industry:

- Bianlian (43 victims, 25.44%) and Blackbasta (37 victims, 20.90%) show significant targeting.
- Meow (27 victims, 20.15%) and Rhysida (21 victims, 23.60%) indicate concentrated efforts within this sector.
- Other gangs, such as Medusa (35 victims, 16.91%), Incransom (30 victims, 18.99%), and Blacksuit (26 victims, 17.81%), reflect meaningful targeting alongside high activity levels.

GEOGRAPHIC DISTRIBUTION OF VICTIMS





The USA accounts for 54.4% of ransomware victims in the Professional Goods & Services industry in 2024. The next most affected countries are the UK with 61 victims, Canada with 50, Germany with 30, and Italy with 24.

A total of 61 countries reported victims, with 20 of them having only one victim each.

CYFIRMA
DECODING THREATS

PROFESSIONAL GOODS & SERVICES INDUSTRY EXTERNAL THREAT LANDSCAPE MANAGEMENT (ETLM) OVERVIEW

Risk Level Indicator: High

APT Campaigns

The professional goods & services sector experienced a high 68% incidence rate across observed APT campaigns, driven by nation-state espionage and financially motivated attacks. Chinese groups, including MISSION2025 and Mustang Panda, dominate, while Russian groups like Cozy Bear and Fancy Bear focus on intelligence gathering. Emerging actors like Fox Kitten and Southeast Asian TAs add to the diverse threat landscape.

Actors: MISSION2025, Mustang Panda, Cozy Bear, FIN7, TA505; emerging actors like Fox Kitten.

Geographic Focus: U.S., Japan, U.K.; growing focus on Asia-Pacific (India, Taiwan, South Korea); emerging markets like Vietnam and the Philippines.

Targets: Web applications, operating systems, VPNs, routers, and IaaS solutions.

Malware: Winnti, NukeSped RAT, Cobalt Strike, PlugX; niche tools like Coinminer, Crimson RAT.

Ransomware

The professional goods & services industry was the most frequently targeted sector, with 897 victims (17.19% of global total), marking an 11.48% year-over-year increase. Activity steadily grew across all quarters, peaking in Q4, and is expected to continue rising into 2025.

Victim Trends: Consistent growth; peaks in Q4 and mild spikes in July and August.

Key Actors: Most active were LockBit 3 (95 victims, peak in February), Ransomhub (75 victims, peak in November).

Other notable gangs were Play (66 victims), Akira (52 victims, peak in November), Bianlian (43 victims).

Geography: U.S. accounted for 54% of victims; activity recorded in 61 countries.

Ranking: Professional goods & services industry ranked 1st as the most frequent victim of ransomware.

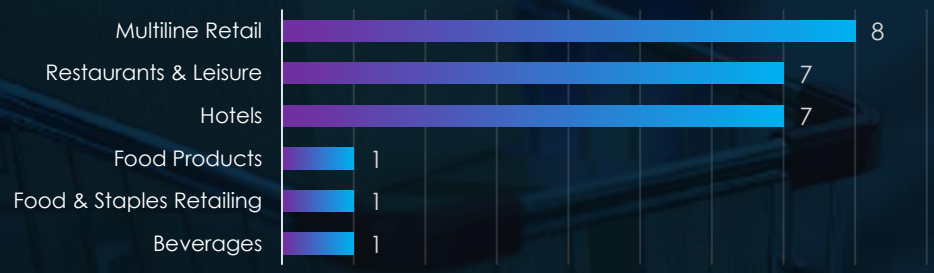
CYFIRMA
DECODING THREATS

CONSUMER GOODS & SERVICES INDUSTRY IN 2024

ADVANCED PERSISTENT THREATS

Over the past 12 months, consumer goods & services organizations recorded victims across 12 of the 34 Advanced Persistent Threat (APT) campaigns observed - an incidence rate of 35%.

These victims spanned multiple segments within the consumer goods & services industry as per below:

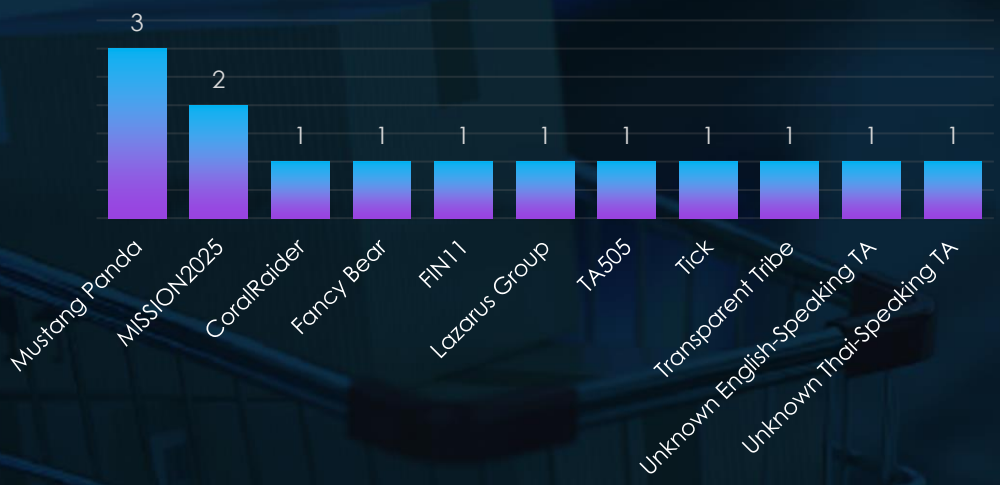


OBSERVED CAMPAIGNS PER MONTH

CYFIRMA
DECODING THREATS

APT CAMPAIGNS
CONSUMER GOODS & SERVICES

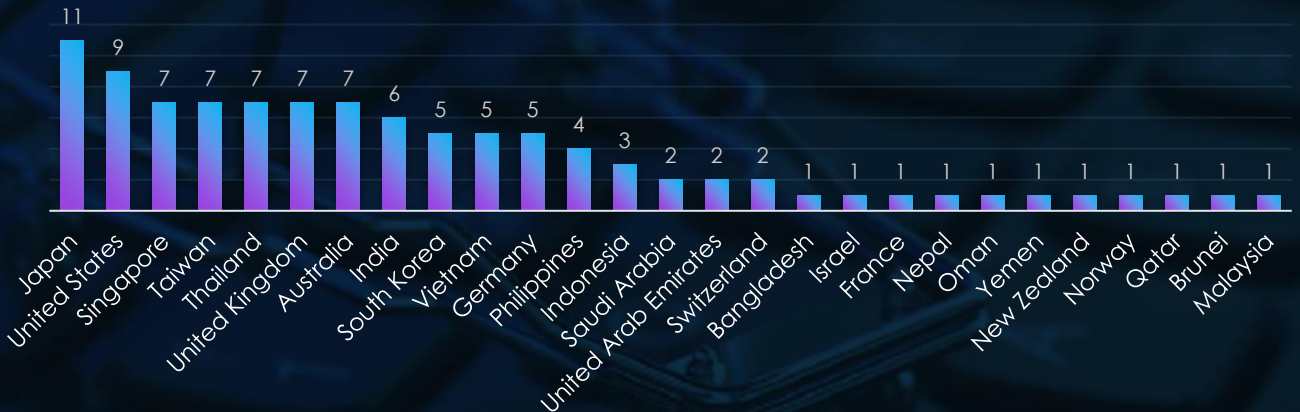
SUSPECTED THREAT ACTORS



The Consumer Goods & Services industry is targeted by a mix of nation-state and financially motivated threat actors. Mustang Panda and MISSION2025 (China) focus on espionage and the theft of valuable data, likely related to supply chains or intellectual property.

Financially motivated groups like FIN11, Lazarus Group, and TA505 exploit the sector for ransomware and data extortion. Actors such as Fancy Bear (Russia) and Transparent Tribe (Pakistan) reflect geopolitical interests, while emerging groups like Unknown Thai-Speaking TA and Unknown English-Speaking TA suggest the industry's appeal to a growing range of adversaries.

GEOGRAPHICAL DISTRIBUTION



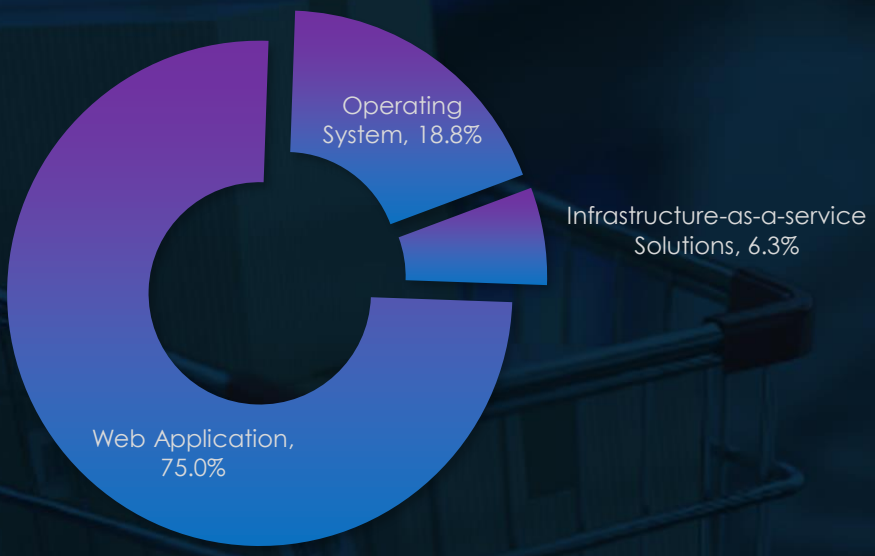
The Consumer Goods & Services industry faces global targeting, with Japan, United States, and Singapore leading, reflecting their prominence in the sector. Asia-Pacific countries, including Taiwan, Thailand, India, and South Korea, are also heavily targeted, highlighting the region's growing role in global consumer markets.

Emerging markets like Philippines and Indonesia further emphasize attackers' expanding reach. The inclusion of smaller nations such as Bangladesh, Nepal, and Brunei underscores the diverse scope of threats, targeting both established and developing markets in this industry.

CYFIRMA
DECODING THREATS

APT CAMPAIGNS
CONSUMER GOODS & SERVICES

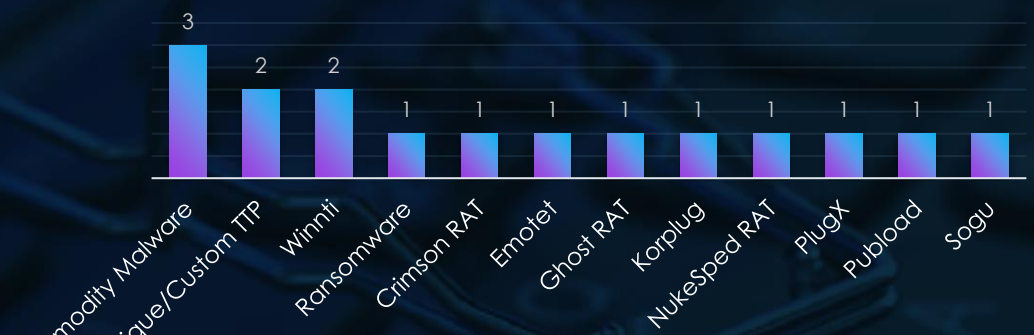
TOP ATTACKED TECHNOLOGY



The industry's most targeted technologies highlight a focus on critical digital infrastructure. Web applications dominate, reflecting their vulnerability as internet-facing systems essential for customer interaction and operational processes.

Operating systems are also key targets, emphasizing attackers' interest in exploiting foundational technologies. Additionally, infrastructure-as-a-service solutions are targeted, underscoring the risks associated with cloud-based services in this sector.

TOP MALWARE



The Consumer Goods & Services industry faces a mix of sophisticated and widely available malware threats. Commodity Malware leads, reflecting its accessibility and effectiveness for broad campaigns, while Unique/Custom TTPs and Winnti emphasize tailored attacks for espionage and persistence.

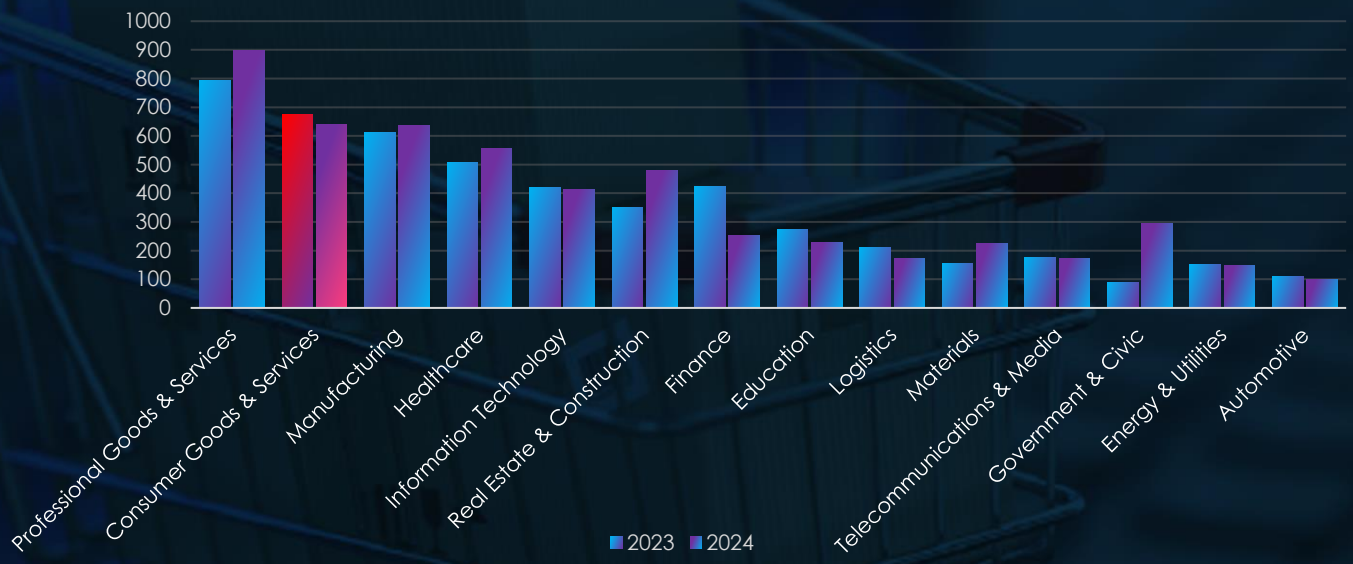
Tools like ransomware and Emotet highlight financial extortion and data theft, while PlugX, Crimson RAT, and NukeSped RAT demonstrate a focus on infiltration and intelligence gathering.

CYFIRMA
DECODING THREATS

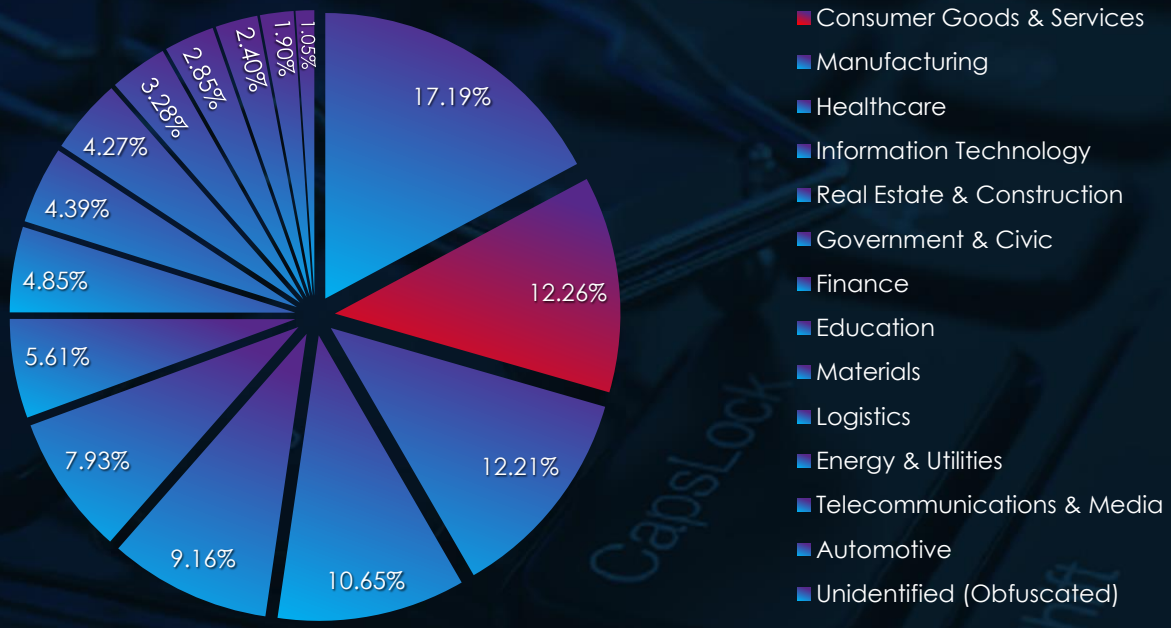
RANSOMWARE VICTIMOLOGY CONSUMER GOODS & SERVICES

In the past 12 months, CYFIRMA has identified 640 verified consumer goods & services organization ransomware victims. This accounts for 12.39% of the overall total of 5,219 ransomware victims during the same period.

GLOBAL DISTRIBUTION BY INDUSTRY

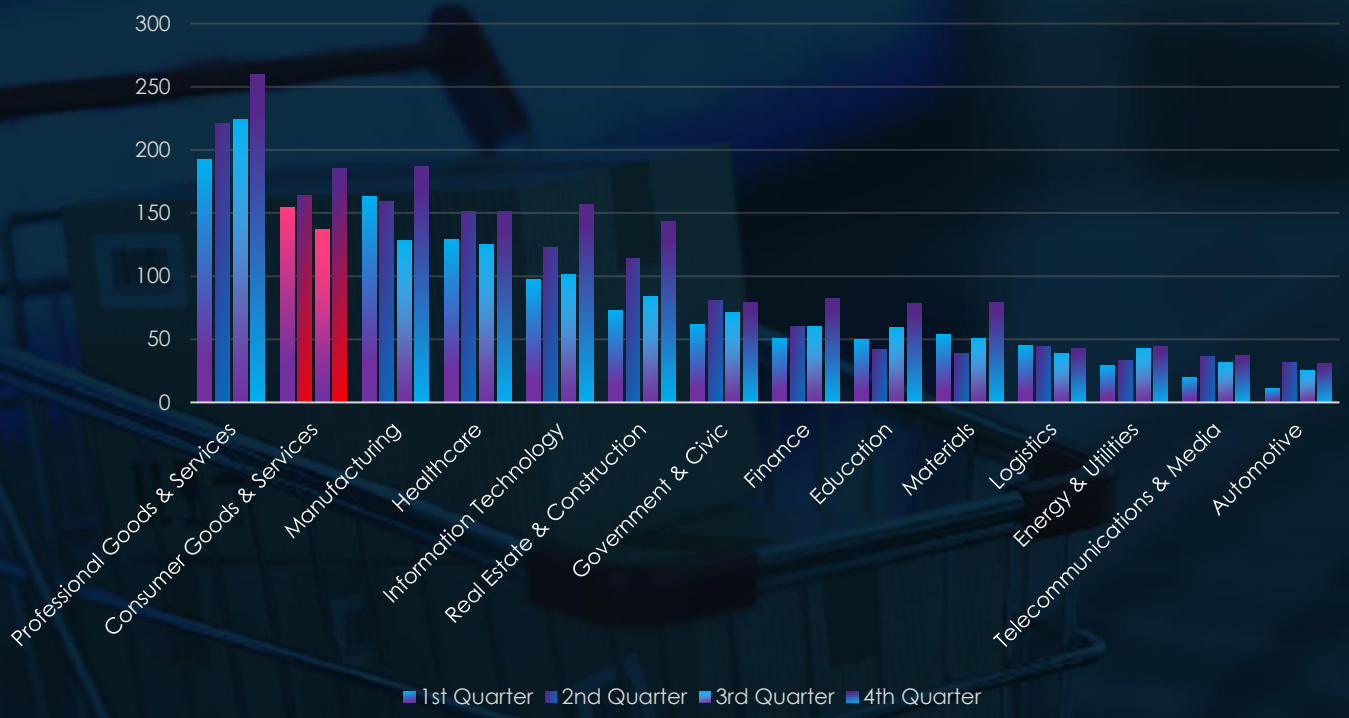


The industry recorded a minor decline of -5.19% in recorded victims from previous year. And placed 2nd in combined number number of victims for both years as well as retained 2nd position as the most frequent victim each year.



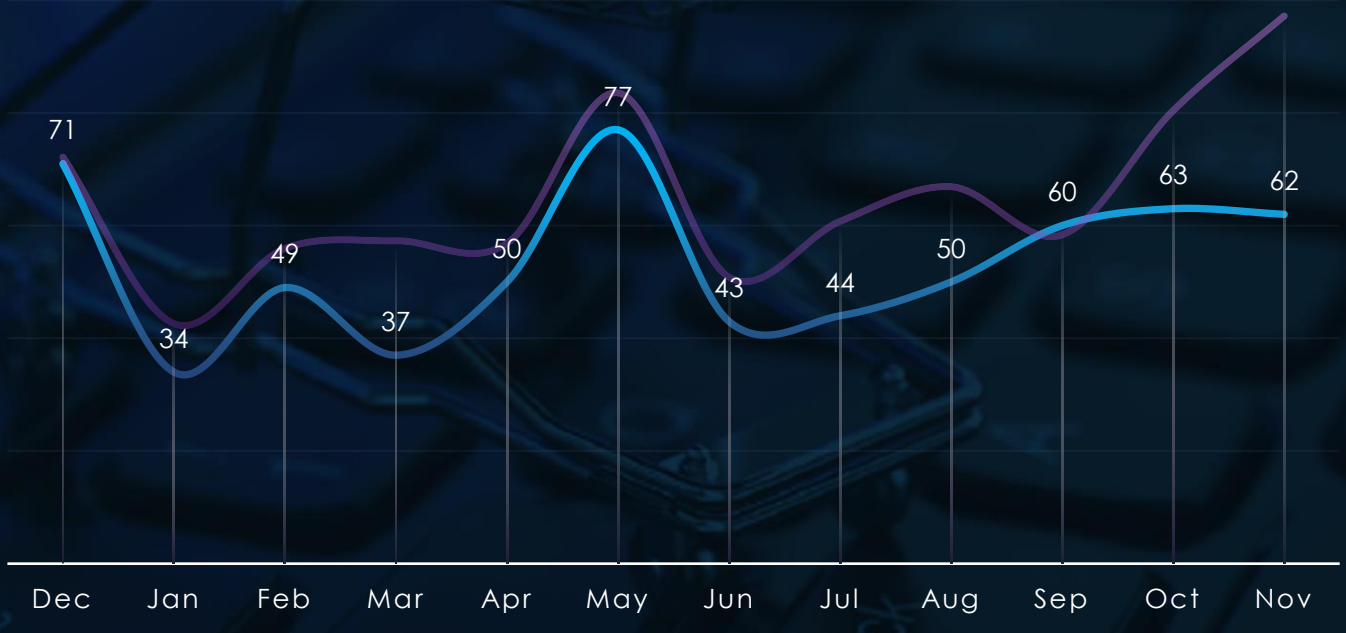
CYFIRMA
DECODING THREATS

QUARTERLY CHANGES DURING 2024



Consumer goods & services shows sustained numbers of victims. Minor dip occurred during third quarter, but was followed by mild spike in fourth quarter.

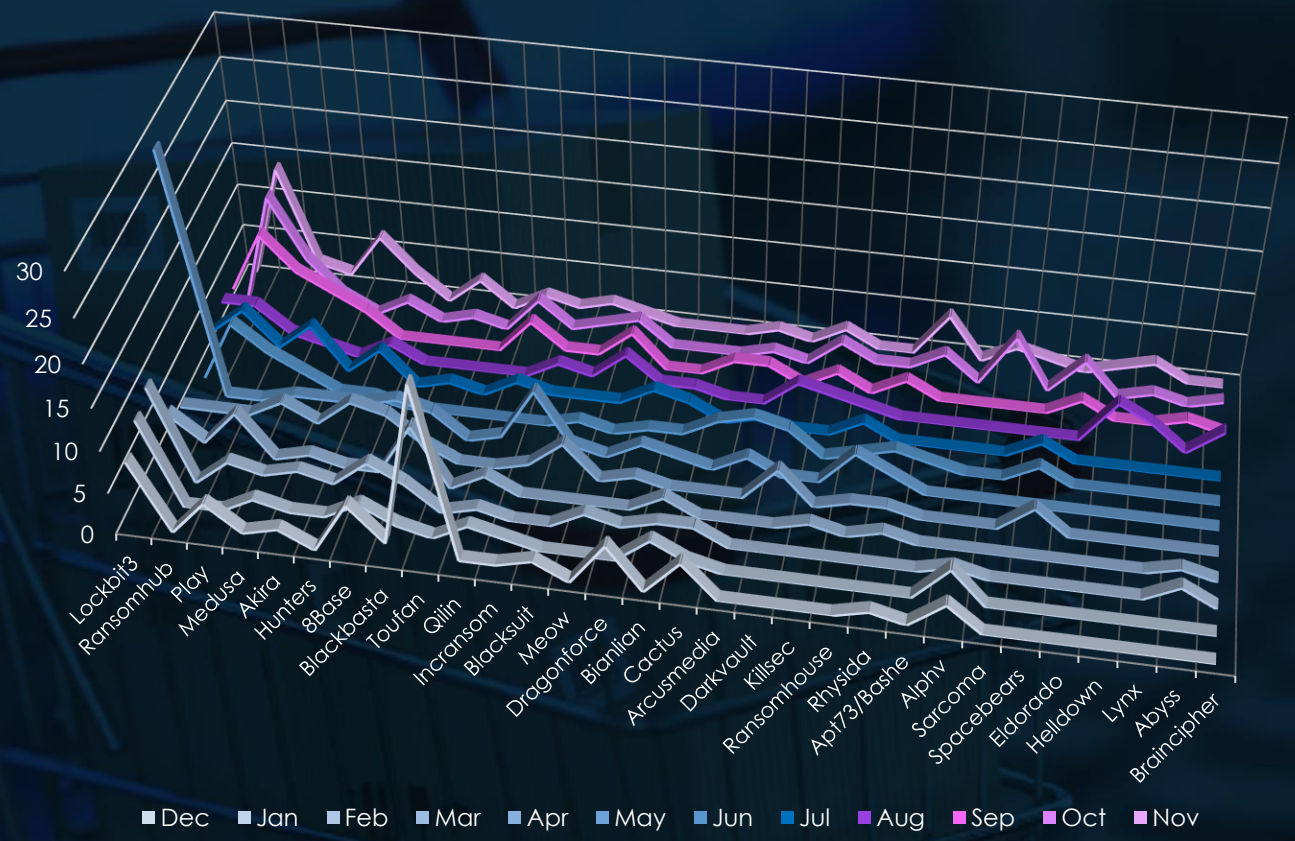
INDUSTRY MONTHLY ACTIVITY CHART



Monthly activity mostly follows the scaled down global trendline. December 2023 and August 2024 recorded significant spiked. In October and November we see downwards trend compared to global line, implying slowdown into 2025.

CYFIRMA
DECODING THREATS

BREAKDOWN OF ACTIVITY PER GANG



In total 73 out of 97 gangs recorded victims in consumer goods & services industry, 75% participation.

A breakdown of top 30 gang's monthly activity provides insights into which gangs were active each month.

Lockbit3 led ransomware activity with 82 victims, with notable spikes in February and January. Ransomhub followed with 65 victims, surging in September through November, peaking at 14 victims in November.

Play impacted 44 victims, showing steady activity across most months. Medusa accounted for 33 victims, maintaining steady operations throughout the year and peaking in May and September. Akira and Hunters targeted 26 and 25 victims, respectively, with Akira peaking in November (7 victims) and Hunters in April (6 victims).

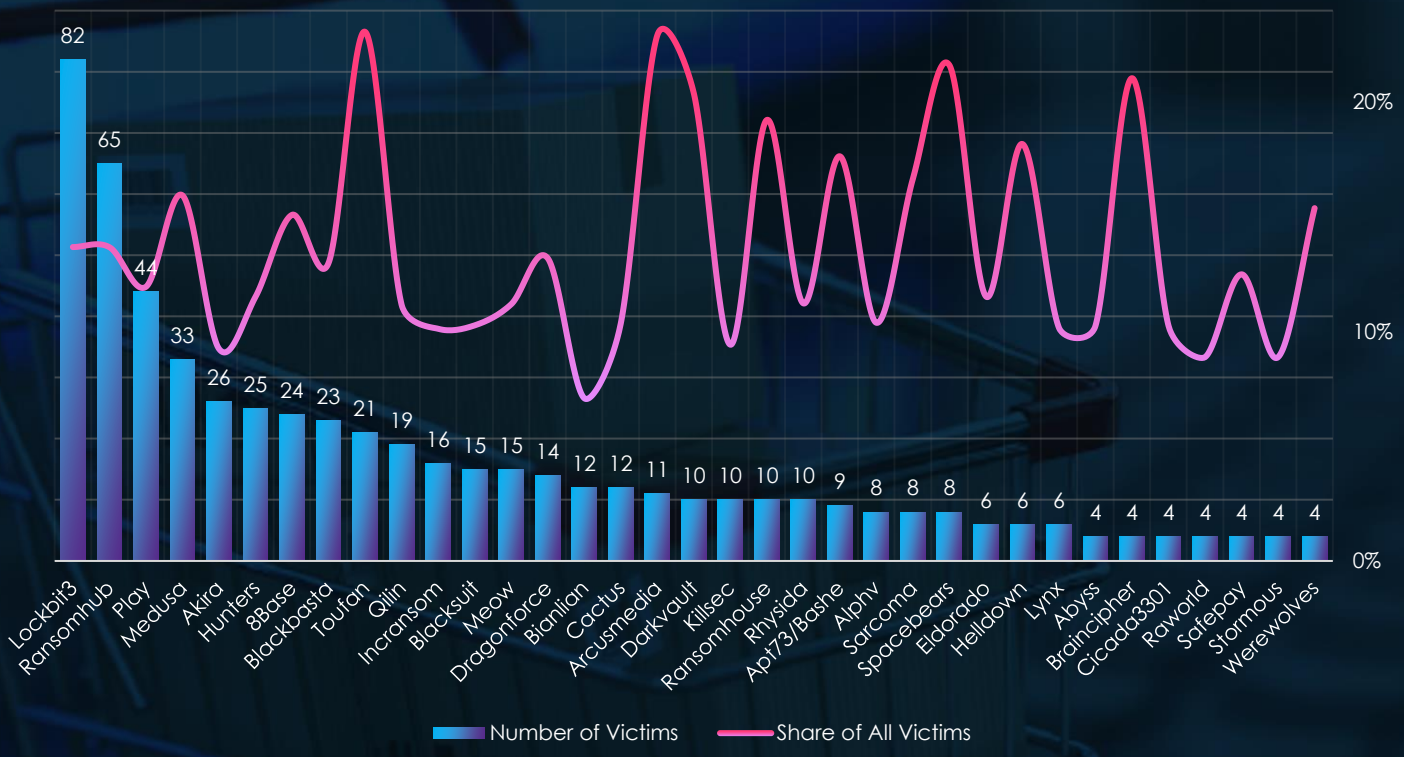
Emerging groups included 8Base (24 victims), active early in the year, peaking in December and February, and Blackbasta (23 victims), showing spikes in March and November. Toufan conducted a singular large campaign in December, affecting 21 victims.

Qilin (19 victims) was consistently active, with peaks in September and October. Groups like Incransom (16 victims) and Blacksuit and Meow (15 victims each) showed scattered campaigns, with Meow active primarily in late summer and fall.

Smaller actors like Dragonforce (14 victims), Bianlian and Cactus (12 each), and Arcusmedia (11 victims) demonstrated sporadic but impactful campaigns. Groups such as Darkvault, Killsec, and Ransomhouse (10 victims each) had targeted activity, often peaking mid-year.

Emerging groups like Sarcoma, Spacebears, and Alphv (8 victims each) had limited but concentrated activity, while others such as Eldorado, Helldown, and Lynx (6 victims each) contributed with isolated late-year campaigns.

INDUSTRY RANSOMWARE VICTIMS PER GANG



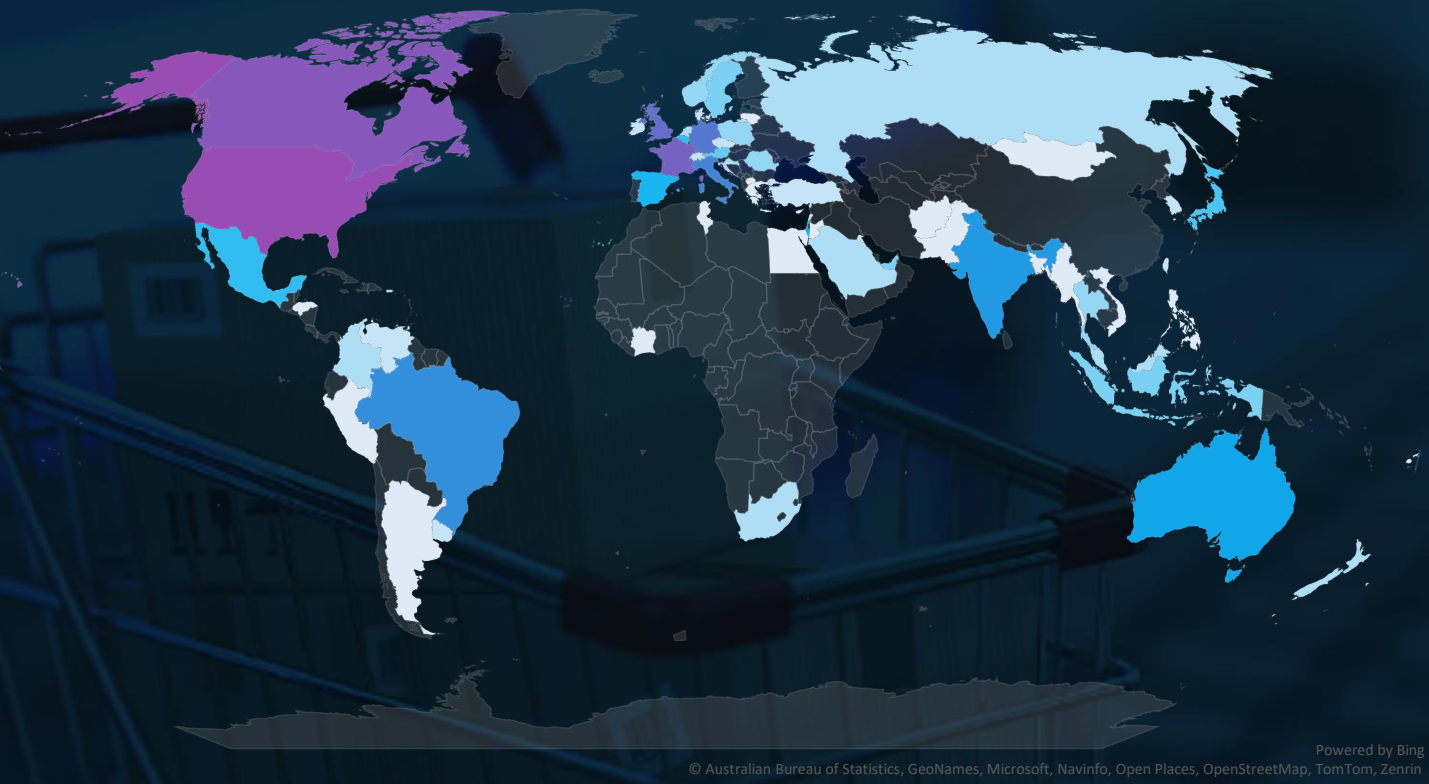
Analysis of the top 35 gangs shows Lockbit3 (82 victims, 13.69%) and Ransomhub (65 victims, 13.68%) lead ransomware activity in this sector, reflecting strong targeting. Play (44 victims, 11.96%) and Medusa (33 victims, 15.94%) also show significant activity and focus on consumer goods and services.

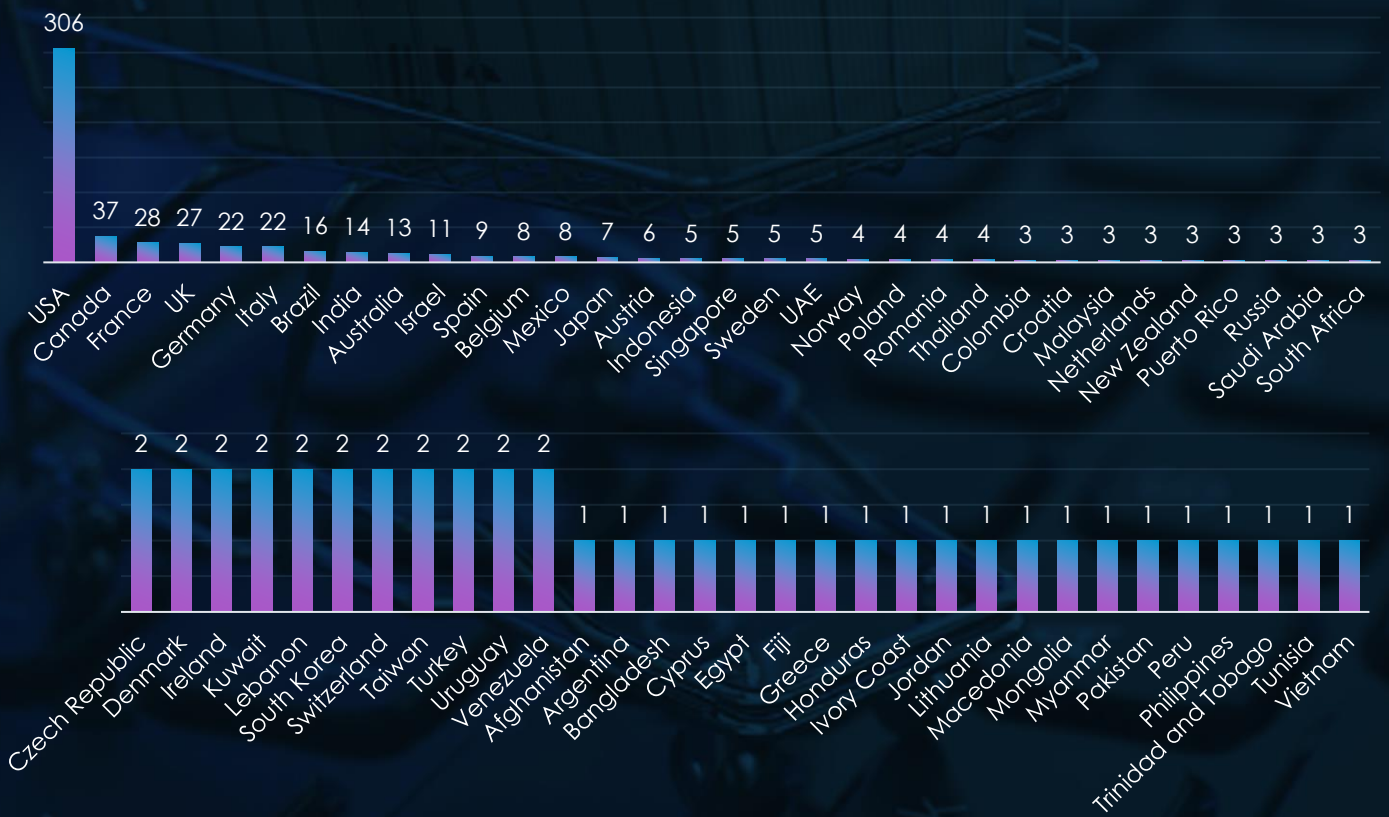
Several gangs exhibit notable focus on this industry:

- Toufan (21 victims, 23.08%) and Arcusmedia (11 victims, 22.92%) demonstrate concentrated efforts in this sector.
- Darkvault (10 victims, 20.41%), Ransomhouse (10 victims, 19.23%), and Helldown (6 victims, 18.18%) indicate strong focus with moderate victim counts.
- 8Base (24 victims, 15.09%), Sarcoma (8 victims, 16.67%), and Spacebears (8 victims, 21.62%) further highlight significant targeting.

It is important to note that consumer goods & services includes many small to medium-size businesses, which are easier targets for smaller gangs willing to accept relatively smaller ransoms. Therefore, the share of victims is among the highest across industries.

GEOGRAPHIC DISTRIBUTION OF VICTIMS



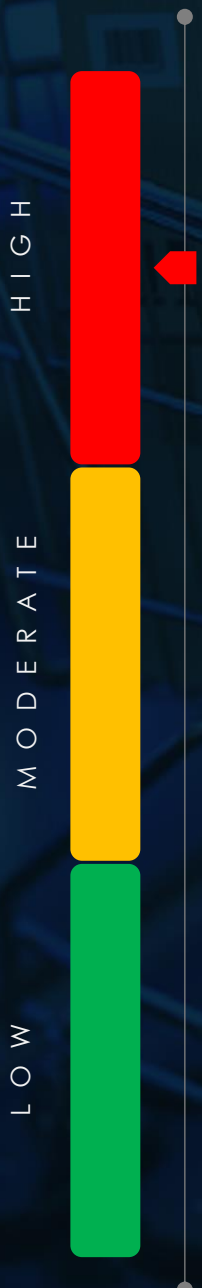


The USA accounts for 47.8% of ransomware victims in the Consumer Goods & Services industry in 2024. The next most affected countries are Canada with 37 victims, France with 28, the UK with 27, and Italy with 22.

A total of 64 countries reported victims, with 21 of them having only one victim each.

CYFIRMA
DECODING THREATS

CONSUMER GOODS & SERVICES INDUSTRY EXTERNAL THREAT LANDSCAPE MANAGEMENT (ETLM) OVERVIEW



Risk Level Indicator: High

APT Campaigns

The consumer goods & services sector recorded a 35% incidence rate across observed APT campaigns, driven by a mix of nation-state espionage and financially motivated attacks. Groups like MISSION2025 and Mustang Panda target intellectual property and supply chain data, while financially driven actors such as Lazarus Group and FIN11 pursue ransomware and extortion. Emerging actors underscore the industry's growing appeal to adversaries.

Actors: Mustang Panda, MISSION2025, FIN11, Lazarus, Fancy Bear; emerging Thai- and English-speaking TAs.

Geographic Focus: U.S., Japan, Singapore; heavy targeting in Asia-Pacific (Taiwan, Thailand, South Korea); expanding in Indonesia and the Philippines.

Targets: Web applications, operating systems, IaaS solutions.

Malware: Commodity Malware, Clop Ransomware, Emotet, PlugX, Crimson RAT, NukeSped RAT.

Ransomware

The consumer goods & services sector ranked as the second most targeted industry, with 640 victims (12.39% of global total), despite a slight -5.19% year-over-year decrease. Activity remained steady across the year, with spikes in December 2023 and August 2024, and a tapering trend into late 2024.

Victim Trends: Sustained activity; peaks in December 2023 and August 2024, with mild Q3 dip.

Key Actors: Most active were LockBit 3 (82 victims, spikes in January/February), Ransomhub (65 victims, peak in November).

Other notable gangs were Play (44 victims), Medusa (33 victims, peaks in May/September), Akira (26 victims, peak in November).

Geography: U.S. accounted for 48% of victims; activity recorded in 64 countries.

Ranking: Professional goods & services industry ranked 2nd as the second most frequent victim of ransomware.

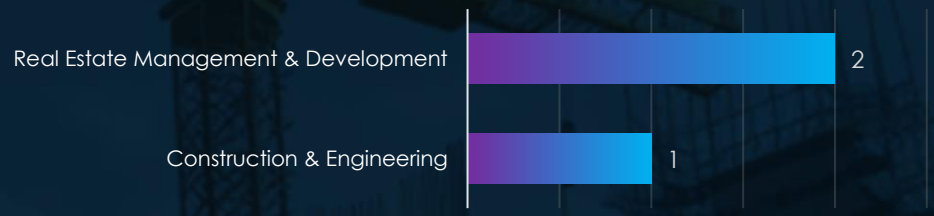
CYFIRMA
DECODING THREATS

REAL ESTATE & CONSTRUCTION INDUSTRY IN 2024

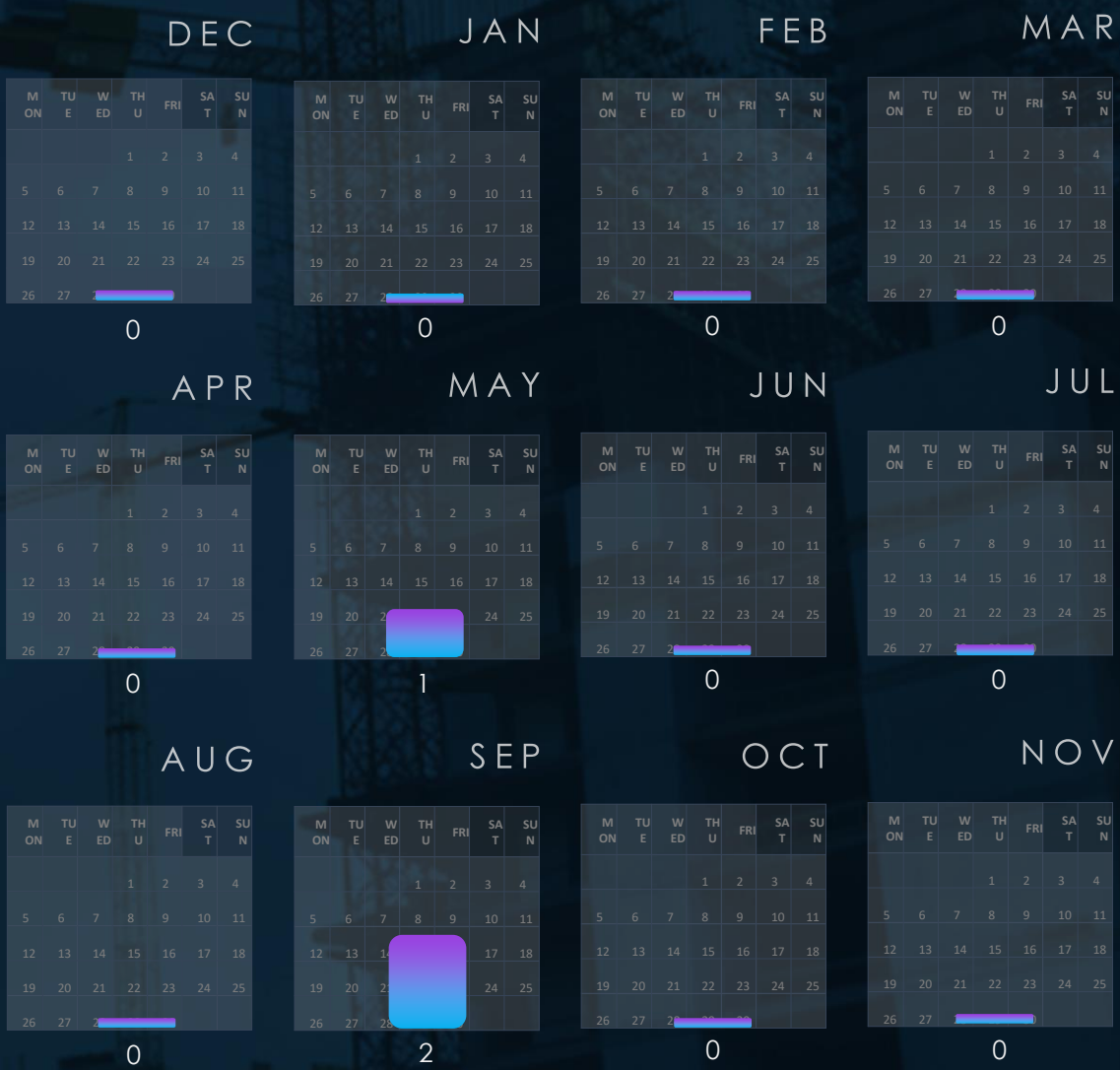
ADVANCED PERSISTENT THREATS

Over the past 12 months, real estate & construction organizations recorded victims across 3 of the 34 Advanced Persistent Threat (APT) campaigns observed - an incidence rate of 9%.

These victims spanned multiple segments within the real estate & construction industry as per below:



OBSERVED CAMPAIGNS PER MONTH



CYFIRMA
DECODING THREATS

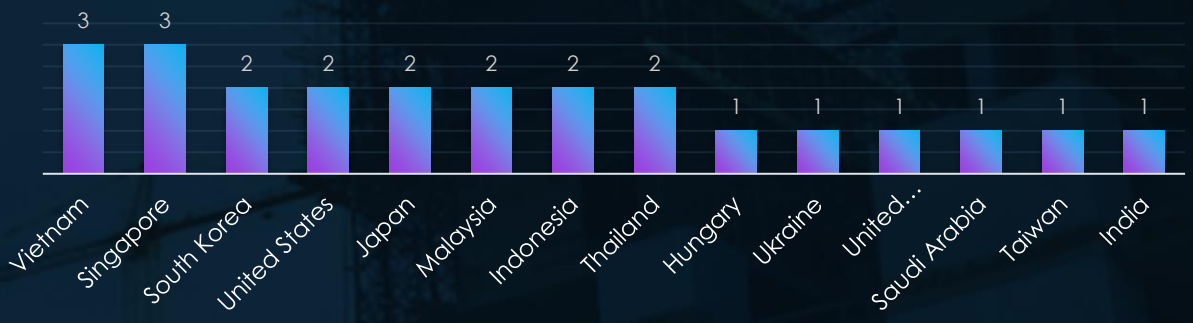
APT CAMPAIGNS
REAL ESTATE & CONSTRUCTION

SUSPECTED THREAT ACTORS

The Real Estate & Construction industry is primarily targeted by financially motivated threat actors. Groups like TA505, FIN11, and FIN7 exploit the sector for data extortion and ransomware attacks, leveraging its reliance on critical operational data.

The inclusion of Savvy Seahorse, a less well-known actor, suggests emerging threats targeting the industry. This focus on financial gain highlights the sector's vulnerability to opportunistic and profit-driven cybercriminals.

GEOGRAPHICAL DISTRIBUTION



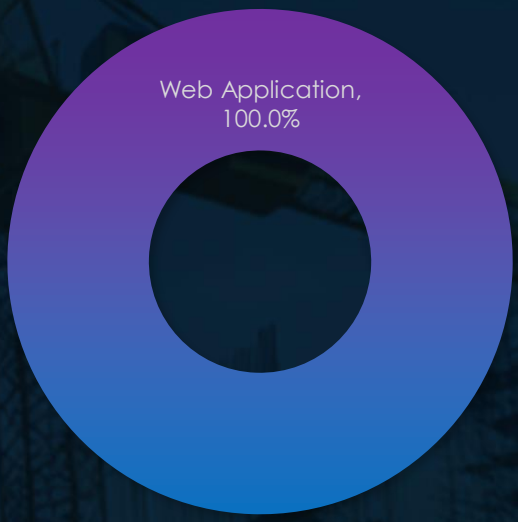
The Real Estate & Construction industry faces targeted attacks across a range of countries, with a notable focus on the Asia-Pacific region. Vietnam, Singapore, and South Korea lead, reflecting the region's growing development and investment in real estate infrastructure.

Other heavily targeted nations, such as the United States and Japan, highlight attackers' interest in established markets. Countries like Malaysia, Indonesia, and Thailand further emphasize the focus on emerging economies, while smaller markets such as Hungary and Ukraine illustrate the sector's global appeal to cybercriminals.

CYFIRMA
DECODING THREATS

APT CAMPAIGNS
REAL ESTATE & CONSTRUCTION

TOP ATTACKED TECHNOLOGY



The Real Estate & Construction industry's primary targeted technology is web applications, reflecting their critical role in managing projects, client interactions, and operational data. As internet-facing systems, they are particularly vulnerable to exploitation

TOP MALWARE

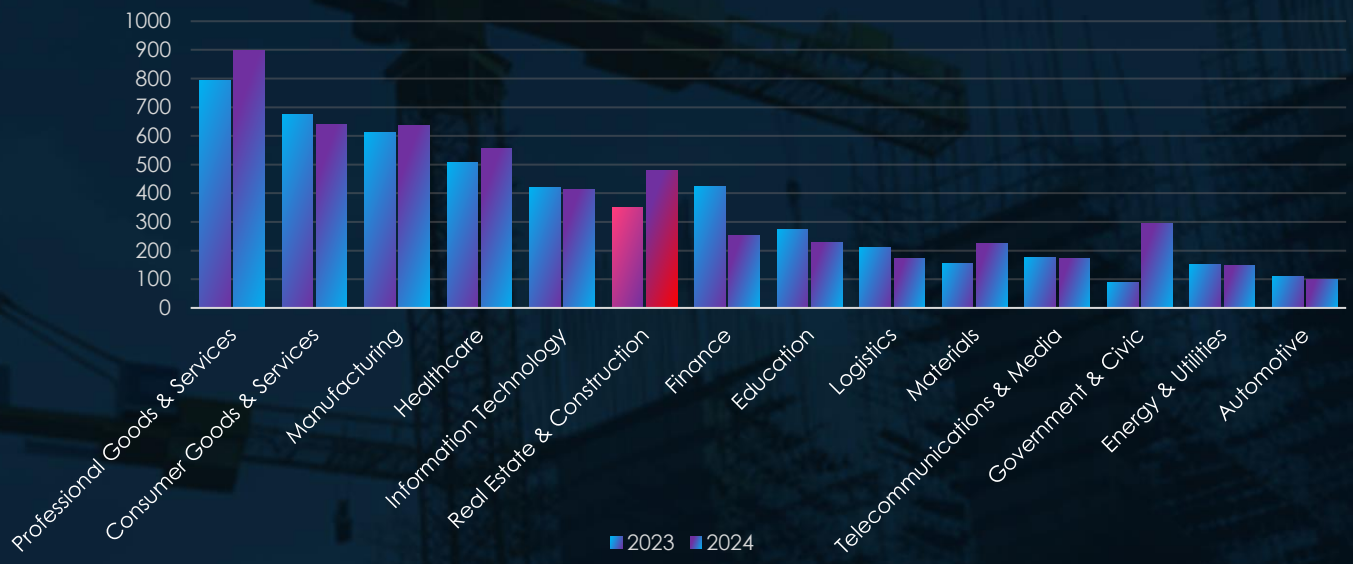
The Real Estate & Construction industry is targeted with Unique/Custom TTPs, reflecting attackers' tailored approaches to exploiting specific vulnerabilities within the sector.

CYFIRMA
DECODING THREATS

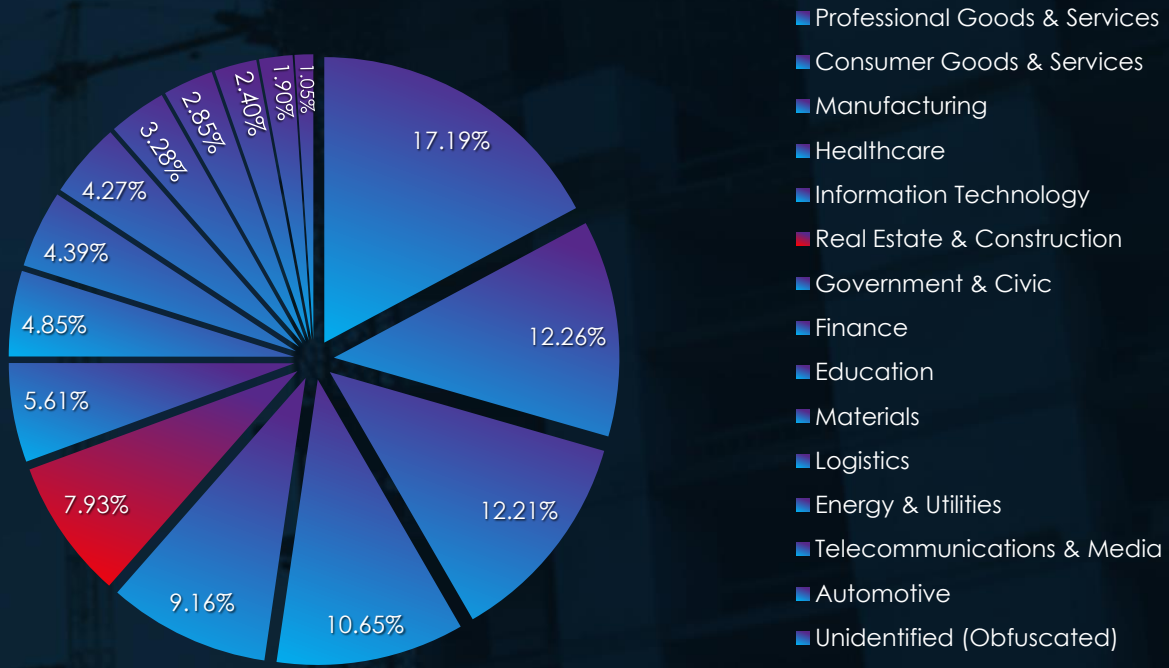
RANSOMWARE VICTIMOLOGY
REAL ESTATE & CONSTRUCTION

In the past 12 months, CYFIRMA has identified 414 verified real estate & construction industry ransomware victims. This accounts for 7.93% of the overall total of 5,219 ransomware victims during the same period.

GLOBAL DISTRIBUTION BY INDUSTRY

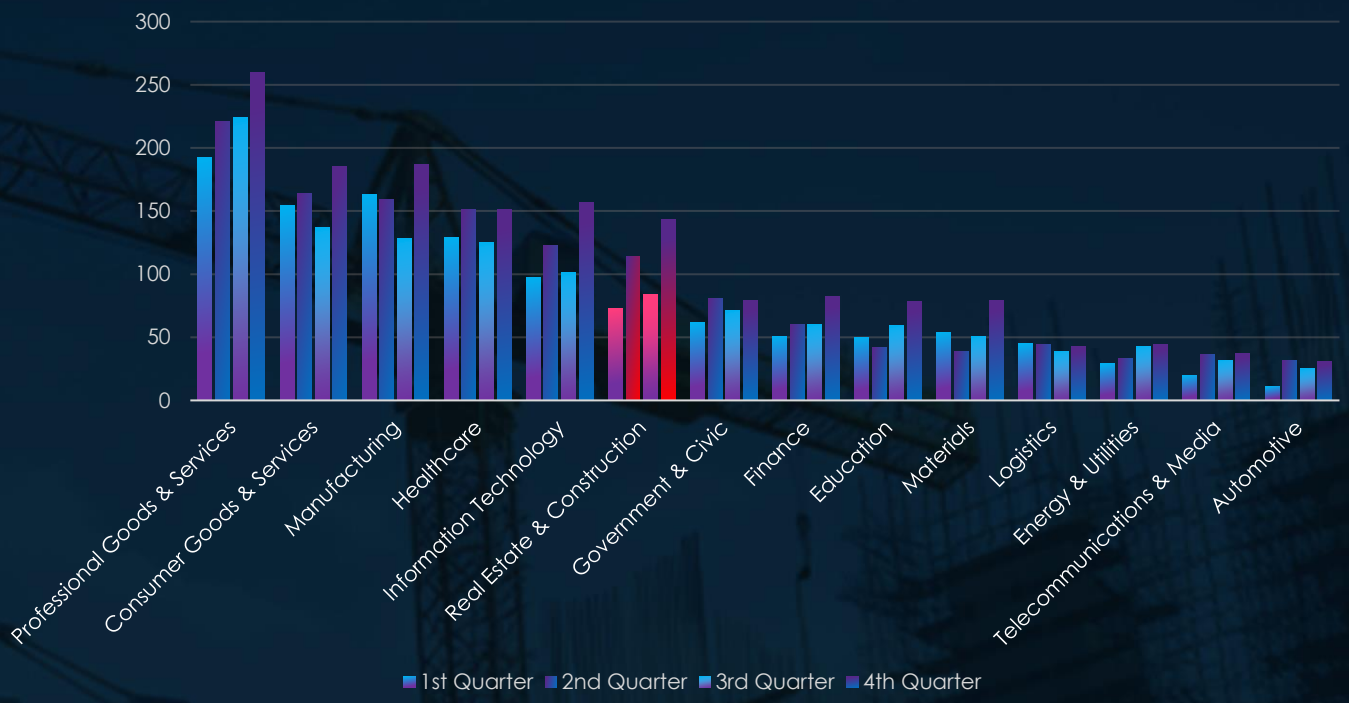


The industry recorded moderately high and significantly growing number of recorded victims, with 26.36% increase from previous year. It ranked at 5th place for both years combined. And it moved up from the 7th to the 6th position, securing the sixth spot as the most frequent victims of ransomware.



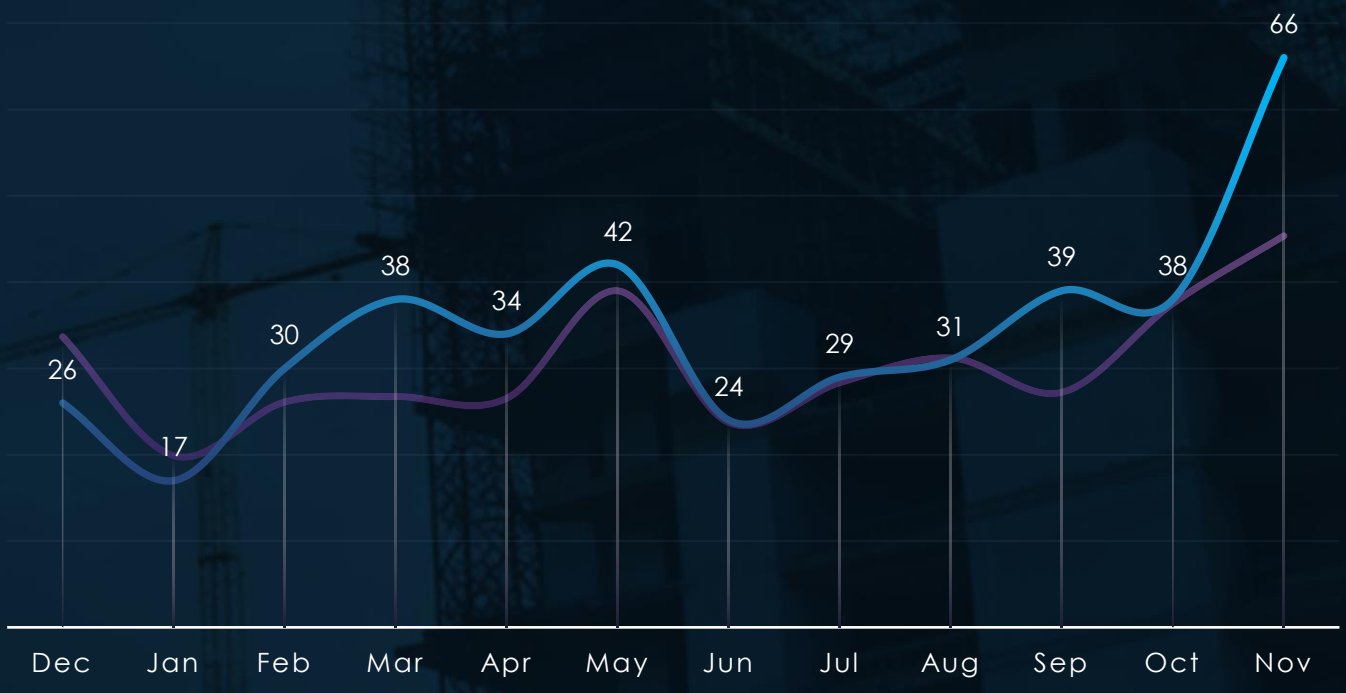
CYFIRMA
DECODING THREATS

QUARTERLY CHANGES DURING 2024



Real estate & construction industry experienced alternate growth from quarter to quarter, with spikes during second and fourth quarters.

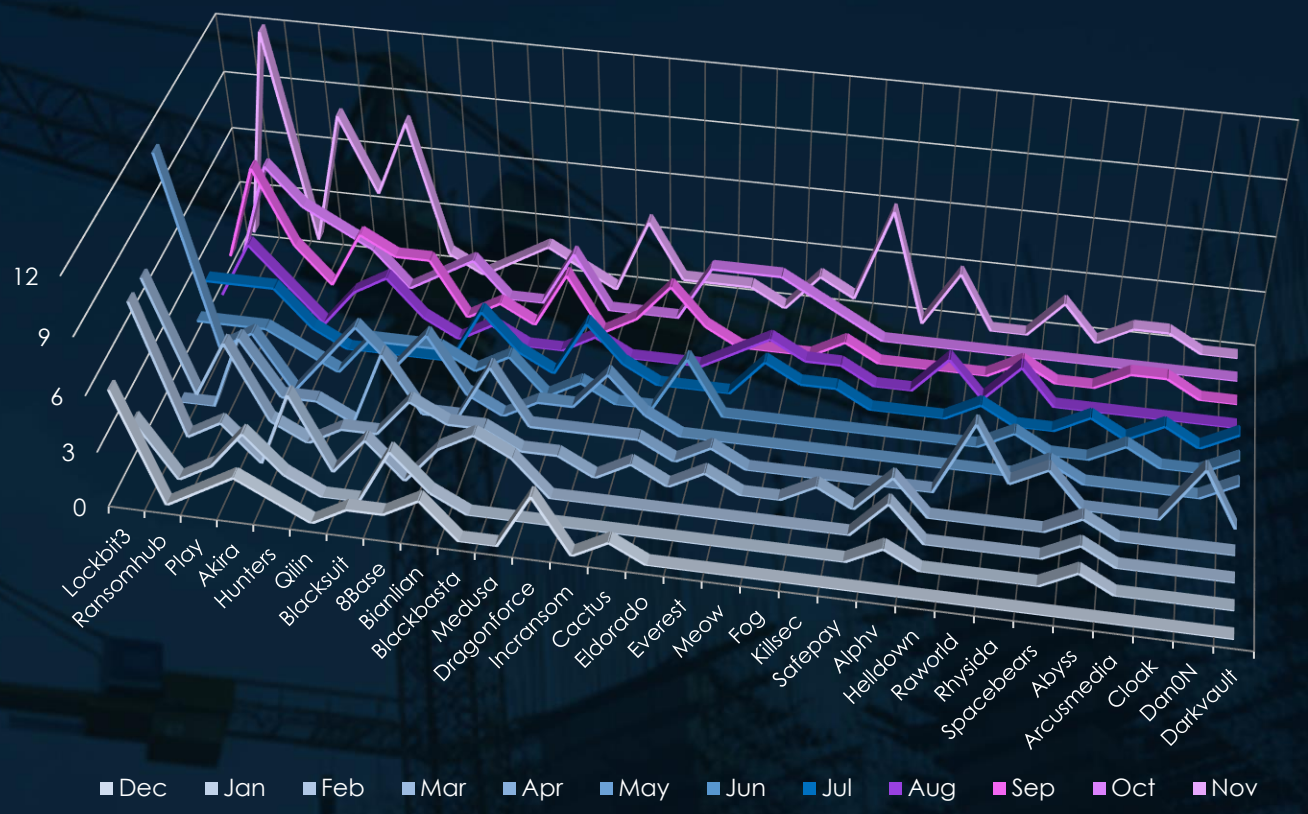
INDUSTRY MONTHLY ACTIVITY CHART



Monthly activity only roughly follows the scaled down global trendline. There is mild above average spike from February to May. And after few months of alignment, activity in the industry spiked above average in September and especially in November, strongly suggesting elevation going into 2025.

CYFIRMA
DECODING THREATS

BREAKDOWN OF ACTIVITY PER GANG



In total 59 out of 97 gangs recorded victims in real estate & construction industry, 61% participation.

A breakdown of top 30 gang's monthly activity provides insights into which gangs were active each month.

Lockbit3 led ransomware activity with 47 victims. Ransomhub followed with 39 victims, peaking in November (12 victims) and maintaining steady activity from July onward.

Play targeted 31 victims, with notable activity in March, April, and October. Akira, Hunters, and Qilin each accounted for 21 victims. Akira peaked in November (8 victims), Hunters in October and November, and Qilin surged in May and November.

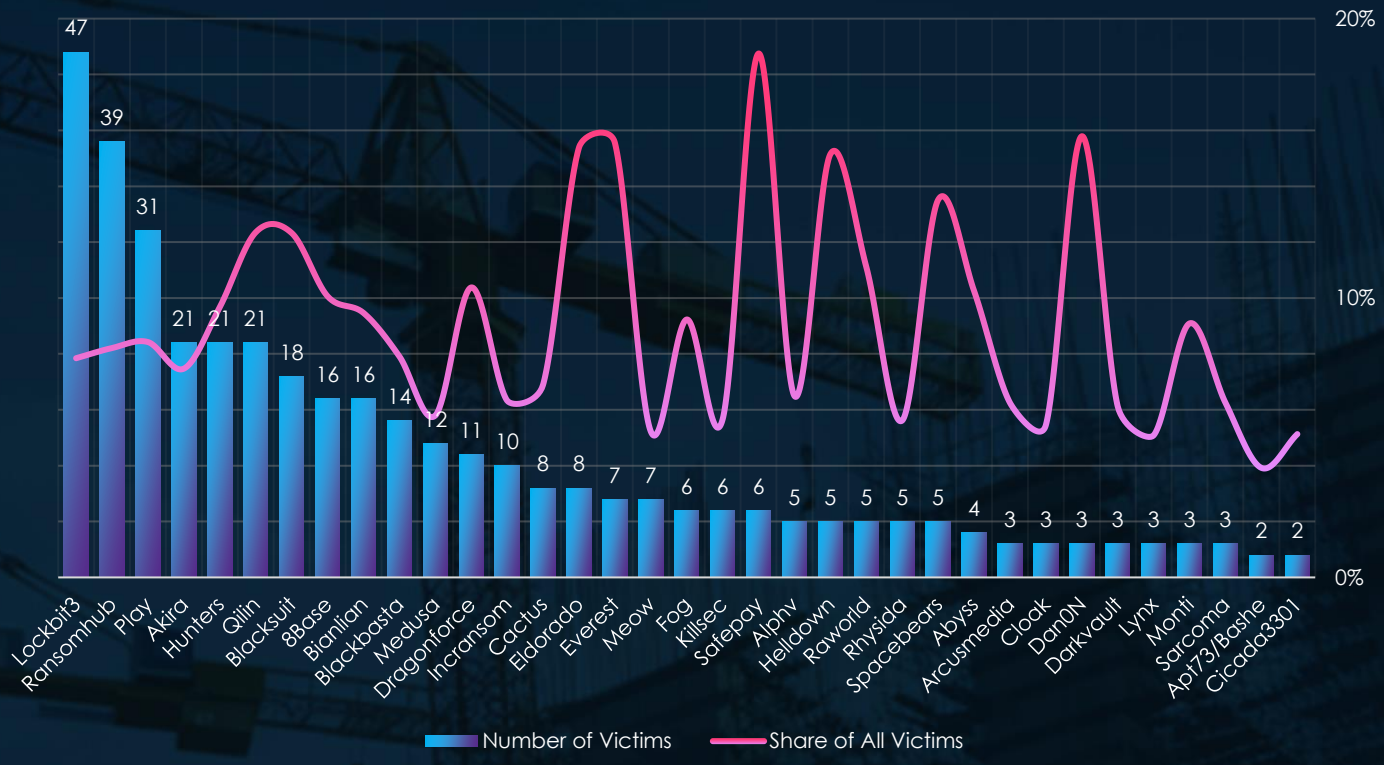
Blacksuit (18 victims) and 8Base and Bianlian (16 each) maintained moderate activity, with Blacksuit peaking in April. Blackbasta (14 victims) was active early in the year, with peaks in March and May. Medusa (12 victims) and Dragonforce (11 victims) focused their campaigns in spring and summer, with Medusa peaking in October.

Smaller groups included Incransom (10 victims), Cactus, and Eldorado (8 each), with Eldorado showing late-year spikes. Meow and Everest (7 each) focused on fall operations, and Fog and Killsec (6 each) showed limited but steady activity.

Emerging actors such as Safepay (6 victims) concentrated all their activity in November, while Alphv, Helldown, Raworld, and Spacebears (5 victims each) demonstrated isolated campaigns. Minor actors like Abyss (4 victims), Arcusmedia, and Cloak (3 each) contributed to the fragmented landscape.

Overall, Lockbit3, Ransomhub, and Play dominated the landscape, while Akira and Hunters showed seasonal peaks.

INDUSTRY RANSOMWARE VICTIMS PER GANG



Review of thetop 35 gangs showsLockbit3 leads ransomware activity in this sector, with 47 victims (7.85%), reflecting widespread activity but not a concentrated focus. Ransomhub (39 victims, 8.21%) and Play (31 victims, 8.42%) also show significant activity but are distributed across multiple industries. Akira and Hunters, each with 21 victims (7.47% and 9.68%, respectively), also highlight moderate activity within this industry.

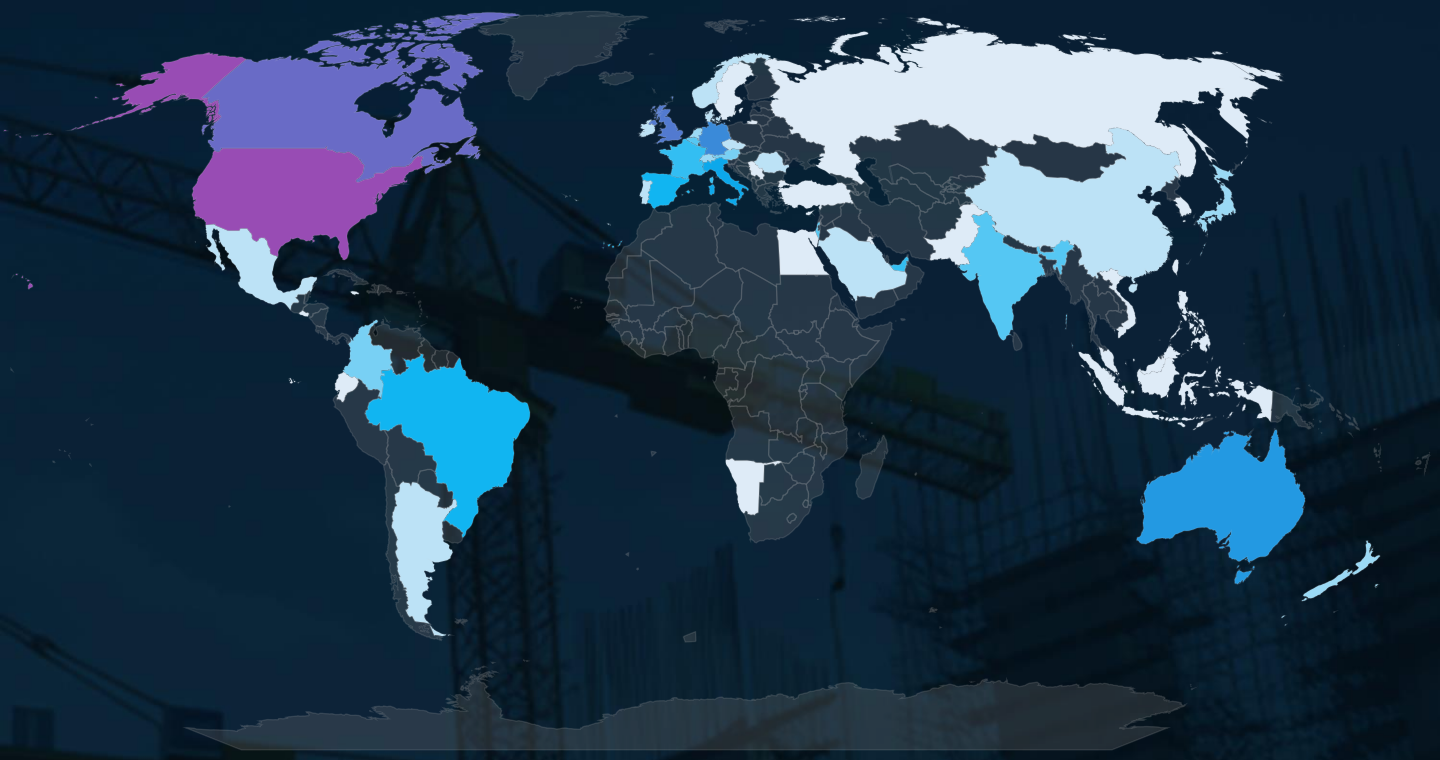
Several gangs demonstrate meaningful focus on the real estate and construction industry:

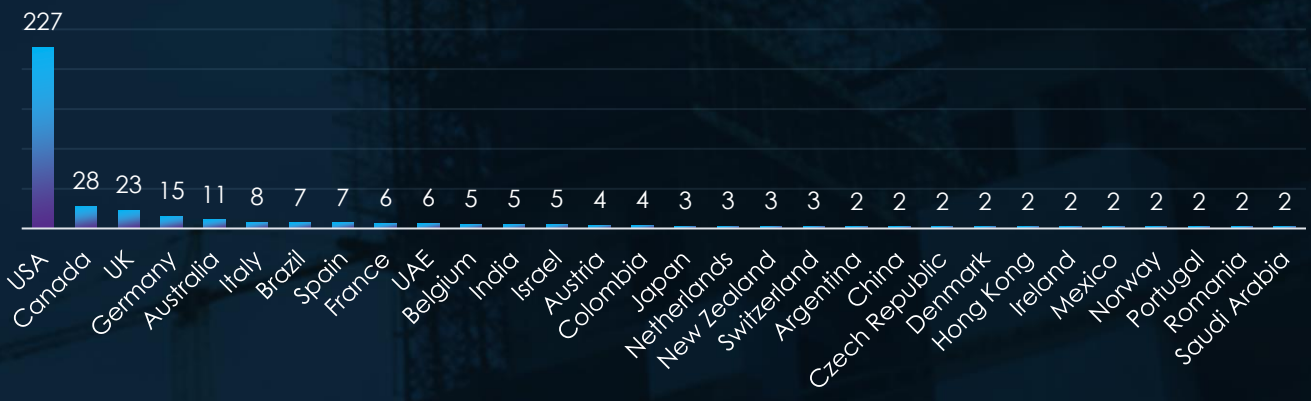
- Qilin (21 victims, 12.35%) and Blacksuit (18 victims, 12.33%) show significant targeting within the sector.
- Other gangs, like 8Base (16 victims, 10.06%), Dragonforce (11 victims, 10.38%), and Spacebears (5 victims, 13.51%), indicate concentrated efforts relative to their total activity.
- Safepay (6 victims, 18.75%), Eldorado (8 victims, 15.38%), and Helldown (5 victims, 15.15%) demonstrate high percentages, reflecting strong focus.

Some gangs exhibit disproportionately high percentages due to low victim counts:

- Dan0N (3 victims, 15.79%) and Everest (7 victims, 15.56%) show high percentages but are limited by their small numbers.
- Safepay (6 victims, 18.75%) and Eldorado (8 victims, 15.38%) also show high percentages with relatively lower victim counts.
- Spacebears (5 victims, 13.51%) and Helldown (5 victims, 15.15%) similarly reflect elevated focus but limited overall impact.

GEOGRAPHIC DISTRIBUTION OF VICTIMS





The USA accounts for 54.8% of ransomware victims in the Real Estate & Construction industry in 2024. The next most affected countries are Canada with 28 victims, the UK with 23, Germany with 15, and Australia with 11.

A total of 49 countries reported victims, with 19 of them having only one victim each.

CYFIRMA
DECODING THREATS

REAL ESTATE & CONSTRUCTION INDUSTRY EXTERNAL THREAT LANDSCAPE MANAGEMENT (ETLM) OVERVIEW

Risk Level Indicator: Low/Moderate

APT Campaigns

The real estate & construction sector recorded a low 9% incidence rate across observed APT campaigns, driven primarily by financially motivated groups such as TA505, FIN11, and FIN7. Emerging actors like Savvy Seahorse highlight the sector's vulnerability to opportunistic threats focused on data extortion and ransomware.

Actors: TA505, FIN11, FIN7; emerging actor Savvy Seahorse.

Geographic Focus: Asia-Pacific (Vietnam, Singapore, South Korea); established markets like U.S. and Japan; emerging markets including Malaysia, Indonesia, and Thailand.

Targets: Web applications, reflecting their critical role in managing projects and operational data.

Malware: Unique/Custom TTPs targeting industry-specific vulnerabilities.

Ransomware

The real estate & construction industry accounted for 414 ransomware victims (7.93% of global total), with a 26.36% year-over-year increase. Activity alternated across quarters, with notable spikes in Q2 and Q4, especially in September and November, signaling heightened risks into 2025.

Victim Trends: Sustained activity; Peaks in Q2 (April-May) and Q4 (November).

Key Actors: Most active were LockBit 3 (47 victims), Ransomhub (39 victims, peak in November).

Other notable gangs were Play (31 victims, active in March, April, October), Akira (21 victims, peak in November).

Geography: U.S. accounted for 55% of victims; activity recorded in 49 countries.

Ranking: Real estate & construction industry ranked as 6th most frequent victim of ransomware.

CYFIRMA
DECODING THREATS

GOVERNMENT & CIVIC ORGANIZATIONS IN 2024

ADVANCED PERSISTENT THREATS

Over the past 12 months, government organizations recorded victims across 29 of the 34 Advanced Persistent Threat (APT) campaigns observed - an incidence rate of 35%.

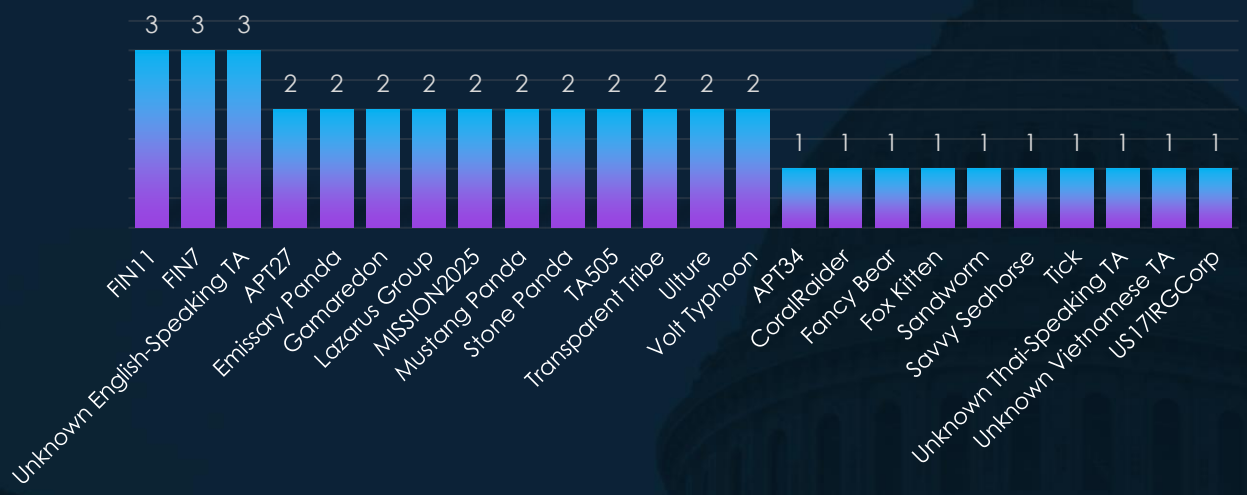
We track only single segment in government category for APT campaigns as per below:

OBSERVED CAMPAIGNS PER MONTH

CYFIRMA
DECODING THREATS

APT CAMPAIGNS – GOVERNMENT

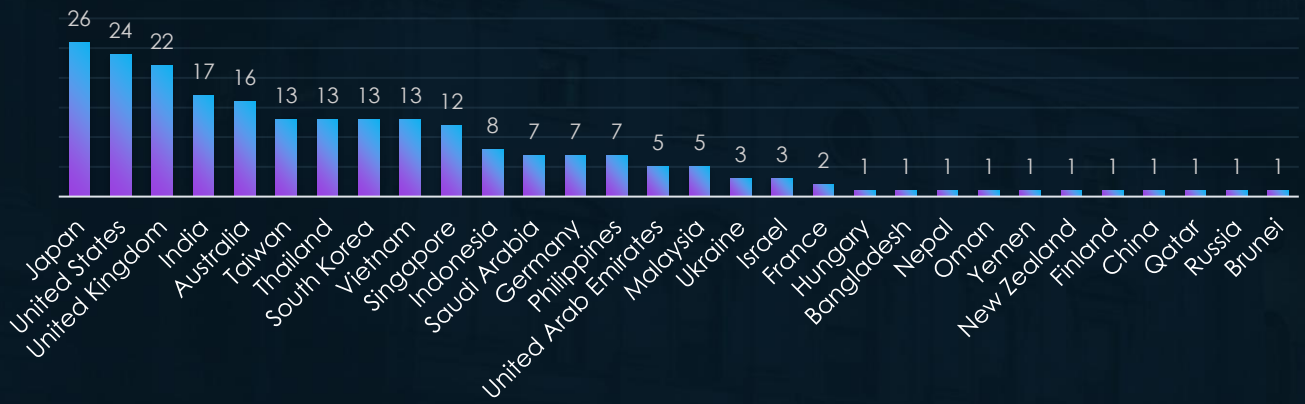
SUSPECTED THREAT ACTORS



The government sector faces a diverse range of threats from both nation-state and financially motivated actors. FIN11 and FIN7 lead in targeting, reflecting financially driven motives such as ransomware and data extortion.

Nation-state groups like Lazarus Group, MISSION2025, and Mustang Panda (China) focus on espionage and the theft of sensitive information. Russian actors, including Gamaredon, Fancy Bear, and Sandworm, prioritize geopolitical objectives and intelligence gathering. Emerging actors, such as Unknown Thai-Speaking TA and Unknown Vietnamese TA, highlight the sector's appeal to a broader range of adversaries.

GEOGRAPHICAL DISTRIBUTION

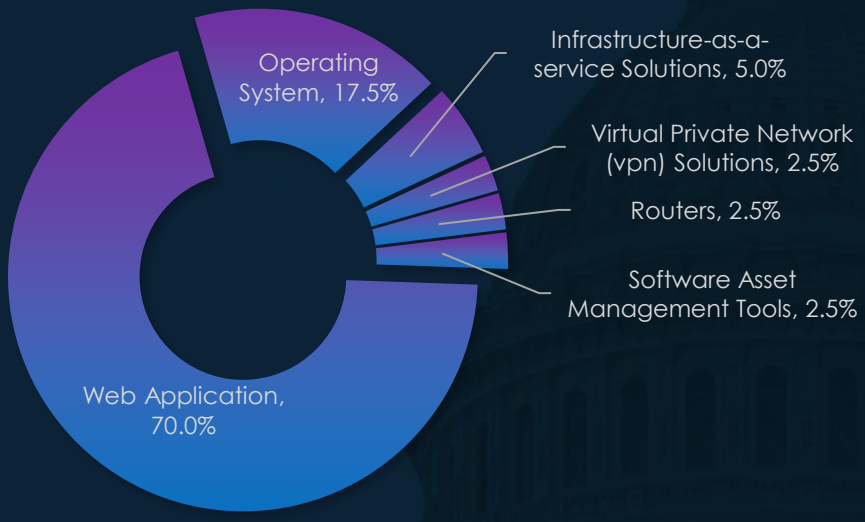


Government organizations are globally targeted, with a strong emphasis on advanced economies like Japan, United States, and United Kingdom, reflecting their prominence in geopolitical and global affairs. Asia-Pacific countries, including India, Taiwan, and South Korea, also feature prominently, highlighting the region's growing strategic importance.

Emerging markets like Indonesia, Philippines, and Malaysia further underscore attackers' interest in developing nations. Smaller nations such as Oman, Nepal, and Brunei illustrate the sector's appeal to a wide range of adversaries, targeting both established and less fortified government systems globally.

APT CAMPAIGNS – GOVERNMENT

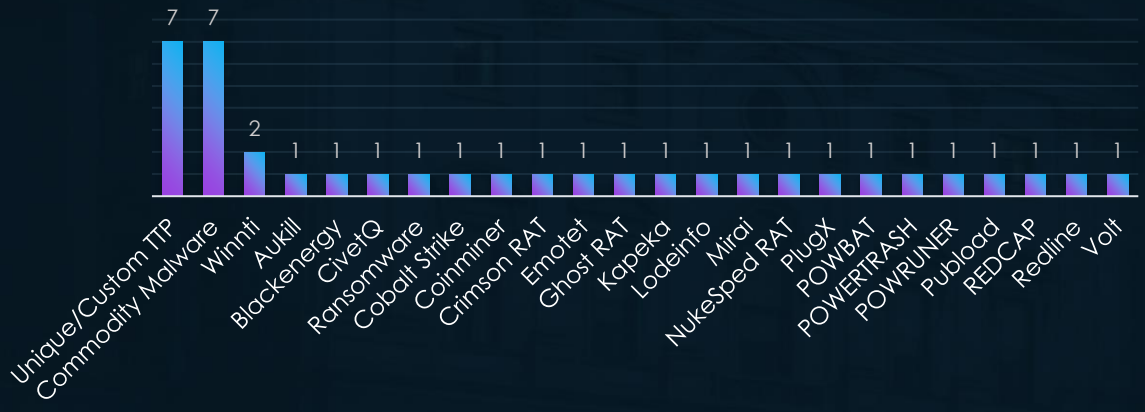
TOP ATTACKED TECHNOLOGY



The Government & Civic Organizations sector's most targeted technologies emphasize the attackers' focus on foundational and internet-facing systems. Web applications dominate, reflecting their critical role in service delivery and their vulnerability to exploitation.

Operating systems also see significant targeting, highlighting their importance in maintaining governmental infrastructure. Additionally, technologies like infrastructure-as-a-service solutions, VPN solutions, and routers are targeted, underscoring the sector's reliance on secure and resilient IT systems to protect sensitive operations and data.

TOP MALWARE



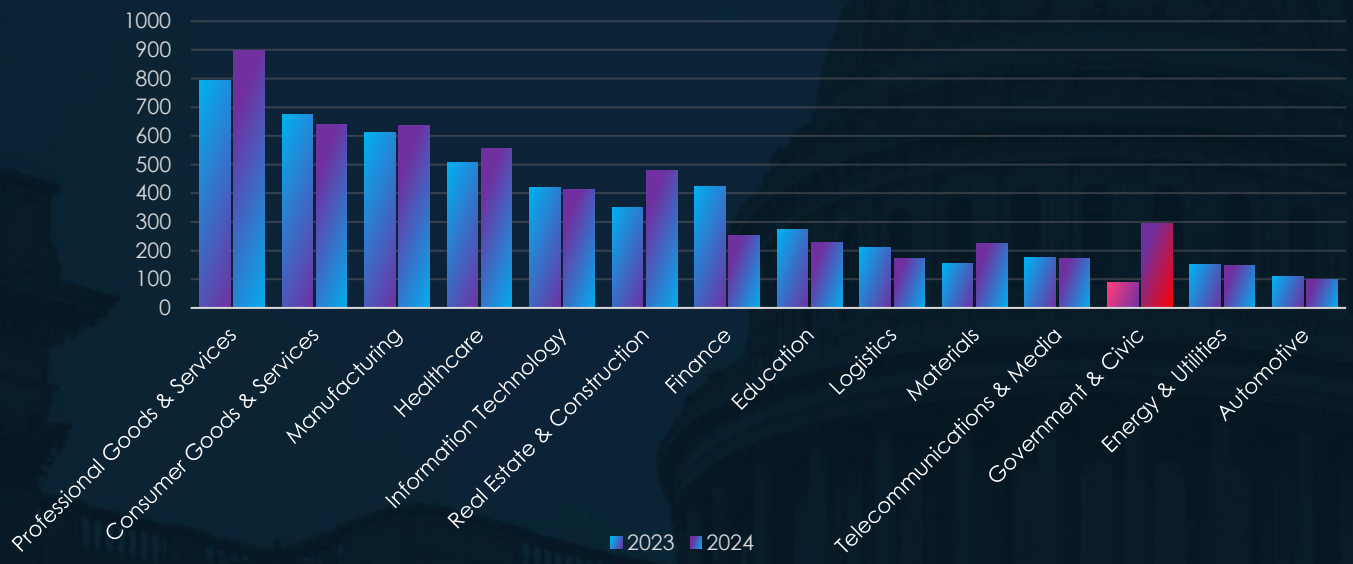
The Government & Civic Organizations sector is targeted with a diverse range of malware, reflecting both tailored and scalable approaches. Unique/Custom TTPs and Commodity Malware dominate, highlighting the balance between sophisticated, targeted attacks and accessible, off-the-shelf tools.

Winnti and tools like NukeSped RAT, PlugX, and Cobalt Strike underscore a focus on espionage and long-term infiltration. Financially motivated malware, such as ransomware and Emotet, emphasizes data theft and extortion, while niche tools like Mirai and Redline demonstrate opportunistic campaigns.

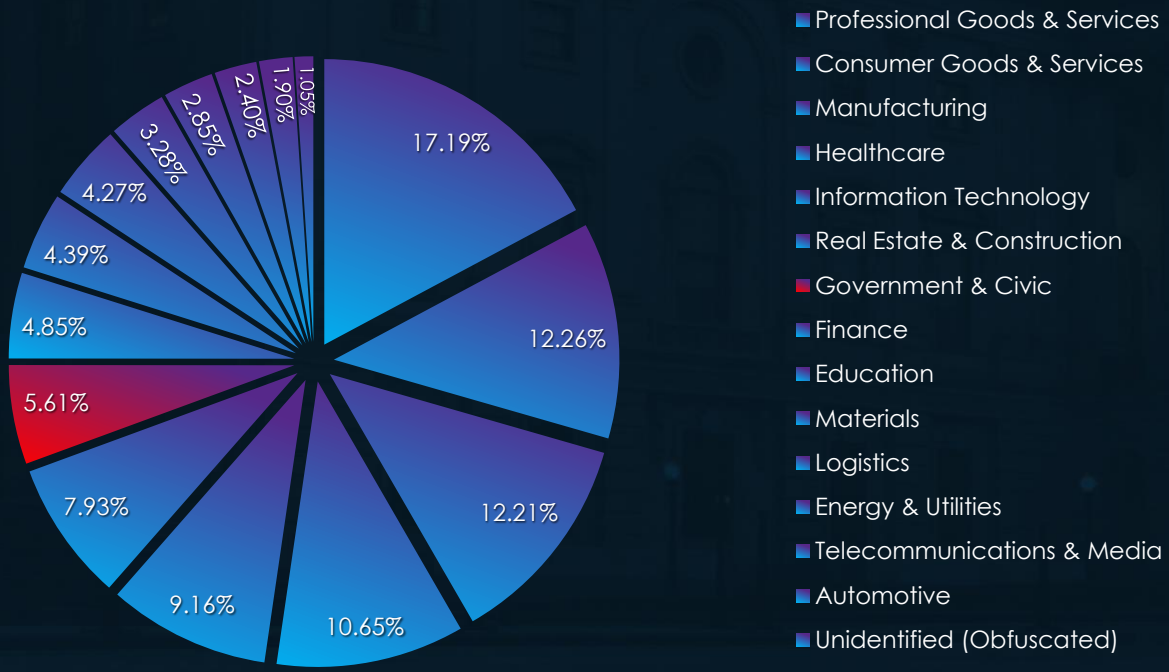
RANSOMWARE VICTIMOLOGY GOVERNMENT & CIVIC

In the past 12 months, CYFIRMA has identified 293 verified government & civic sectors ransomware victims. This accounts for 5.61% of the overall total of 5,219 ransomware victims during the same period.

GLOBAL DISTRIBUTION BY INDUSTRY

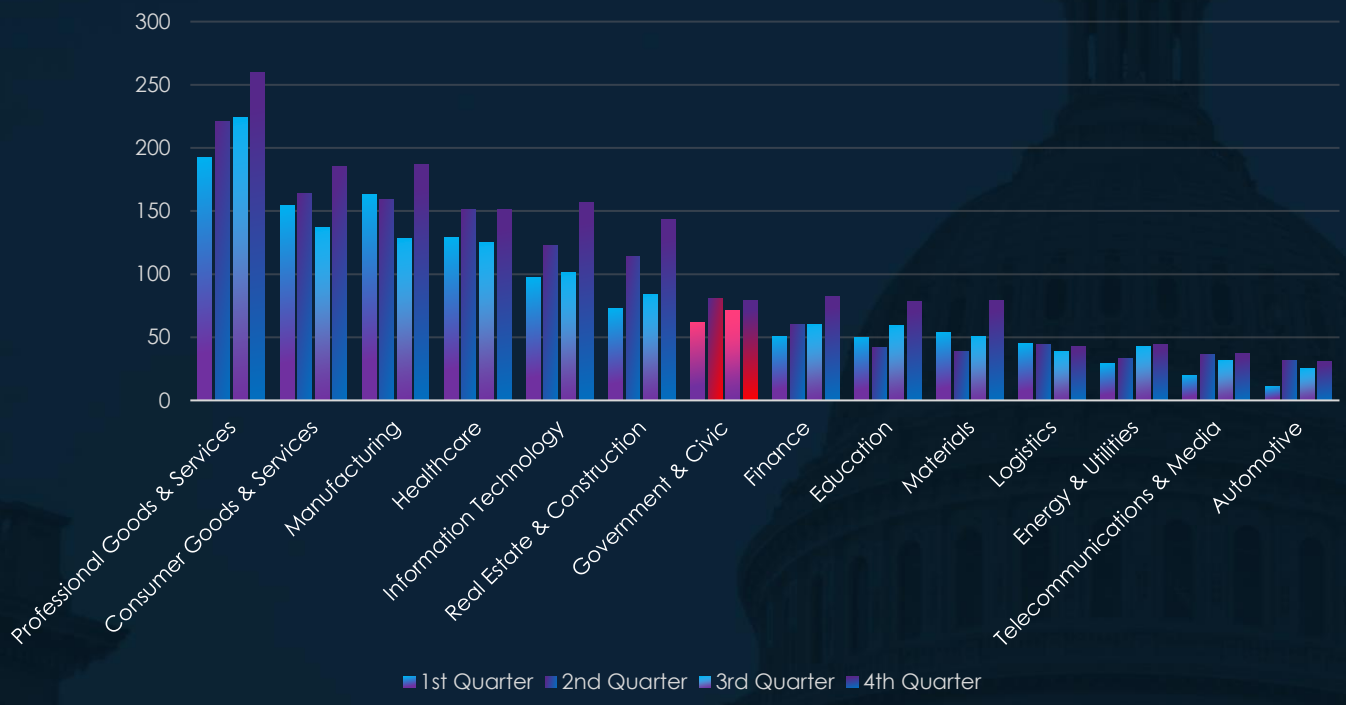


The government & civic organizations recorded the highest year-to-year growth of recorded victims, with 69.62% increase from previous year. It ranked at 11th place for both years combined. However, it moved up from last 13th in 2023 to 7th place as sixth most frequent victims of ransomware in 2024.



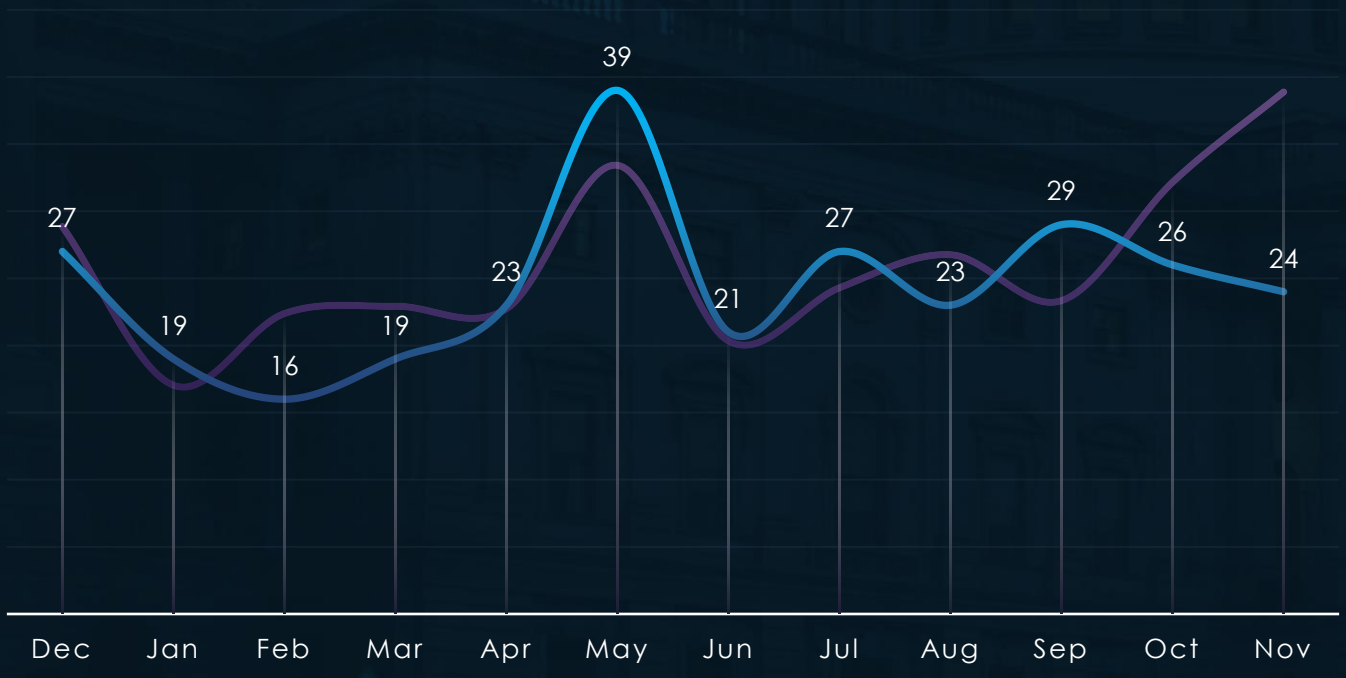
CYFIRMA
DECODING THREATS

QUARTERLY CHANGES DURING 2024



Government & civic organizations experienced sustained activity with moderate and alternate growth from quarter to quarter, second and fourth quarters showing mild spikes.

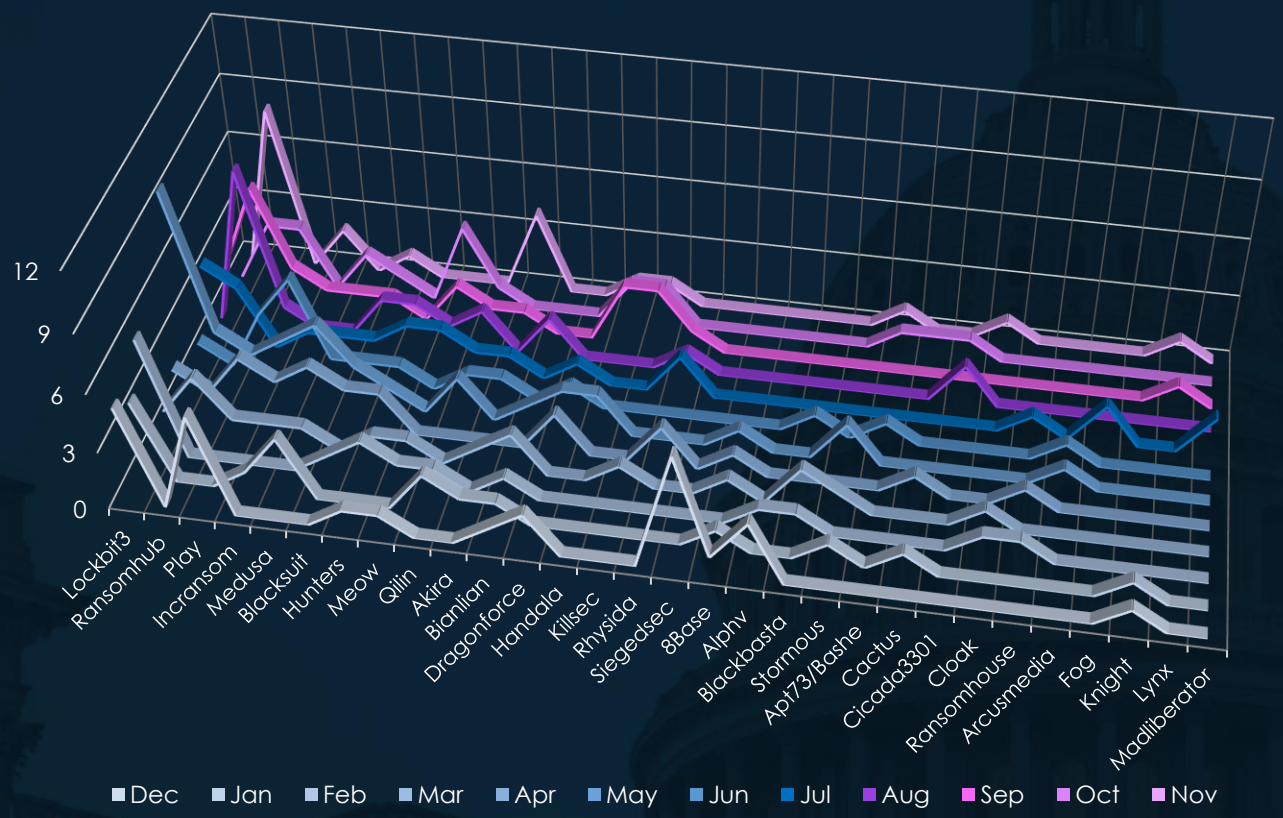
INDUSTRY MONTHLY ACTIVITY CHART



Monthly activity follows the scaled down global trendline with mostly minor divergences. February, March and August recorded mild dips. Global spike in May was moderately amplified for government & civic organization. And despite small spike in September, this sector diverged from strong global upswing in October and November, suggesting start 2025 calmer relative to other industries.

CYFIRMA
DECODING THREATS

BREAKDOWN OF ACTIVITY PER GANG



In total 54 out of 97 gangs recorded victims in government & civic organizations industry, 56% participation.

Lockbit3 and Ransomhub led ransomware activity, each targeting 35 victims. Ransomhub saw a late-year surge, peaking in November (8 victims), and consistent operations from July onward.

Play targeted 20 victims, with steady activity across the year and peaks in December, April, and October. Incransom and Medusa followed with 16 victims each. Incransom peaked in June and showed sporadic activity, while Medusa had its strongest months in May and October.

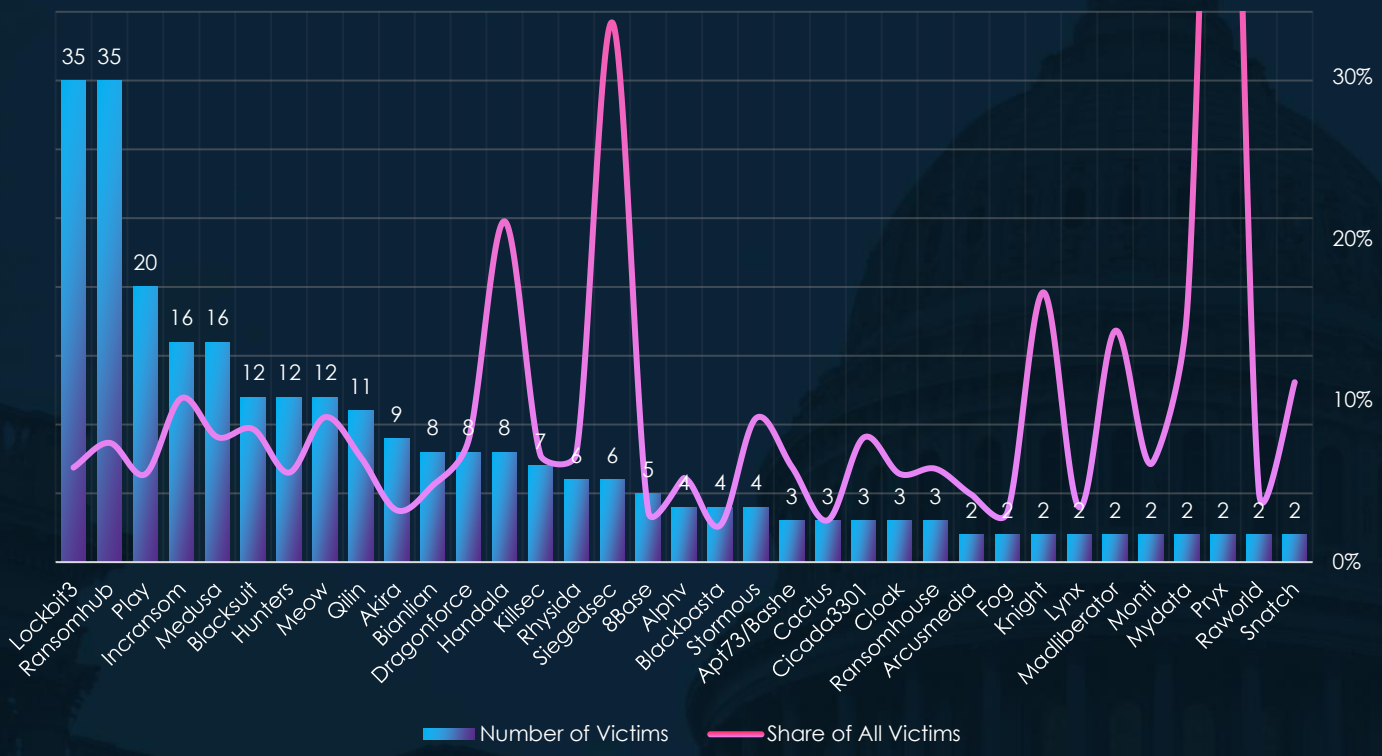
Blacksuit, Hunters, and Meow each accounted for 12 victims. Meow peaked in October with four victims, while Hunters and Blacksuit maintained steady but lower levels of activity throughout the year. Qilin (11 victims) was active sporadically, with peaks in February and August.

Less active groups like Akira (9 victims) and Bianlian, Dragonforce, and Handala (8 victims each) showed scattered activity, with Handala focusing on late-year operations. Emerging actors such as Killsec (7 victims) and Rhysida (6 victims) demonstrated limited campaigns, with peaks in October.

Siegedsec had a focused campaign in December, targeting six victims. Large gangs like 8Base (5 victims), Alphv (4 victims), and Blackbasta (4 victims) reported isolated victims. Stormous (4 victims) and groups like Cactus and Cicada3301 (3 victims each) reflected sporadic operations.

Overall, Lockbit3 and Ransomhub dominated with year-round campaigns, while Play and other mid-tier actors maintained steady operations. Smaller and emerging groups contributed sporadic but impactful campaigns, emphasizing a diverse ransomware ecosystem.

INDUSTRY RANSOMWARE VICTIMS PER GANG



Looking at top 35 gangs, Lockbit3 and Ransomhub lead in activity within this sector, with 35 victims each (5.84% and 7.37%, respectively), indicating significant activity but distributed targeting. Play (20 victims, 5.43%) also shows moderate activity. Other notable actors include Incransom (16 victims, 10.13%) and Medusa (16 victims, 7.73%), both showing stronger focus.

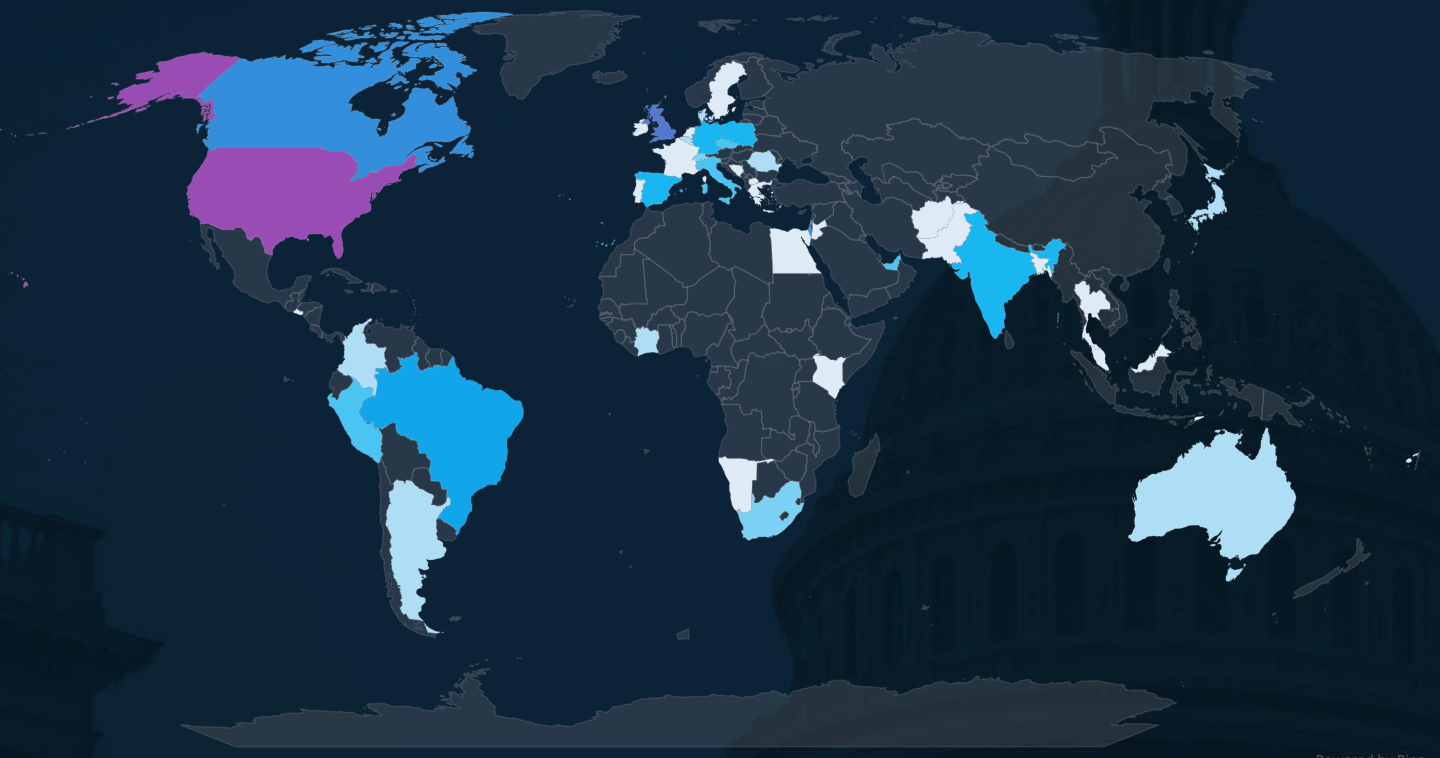
Several gangs demonstrate notable focus on government and civic organizations:

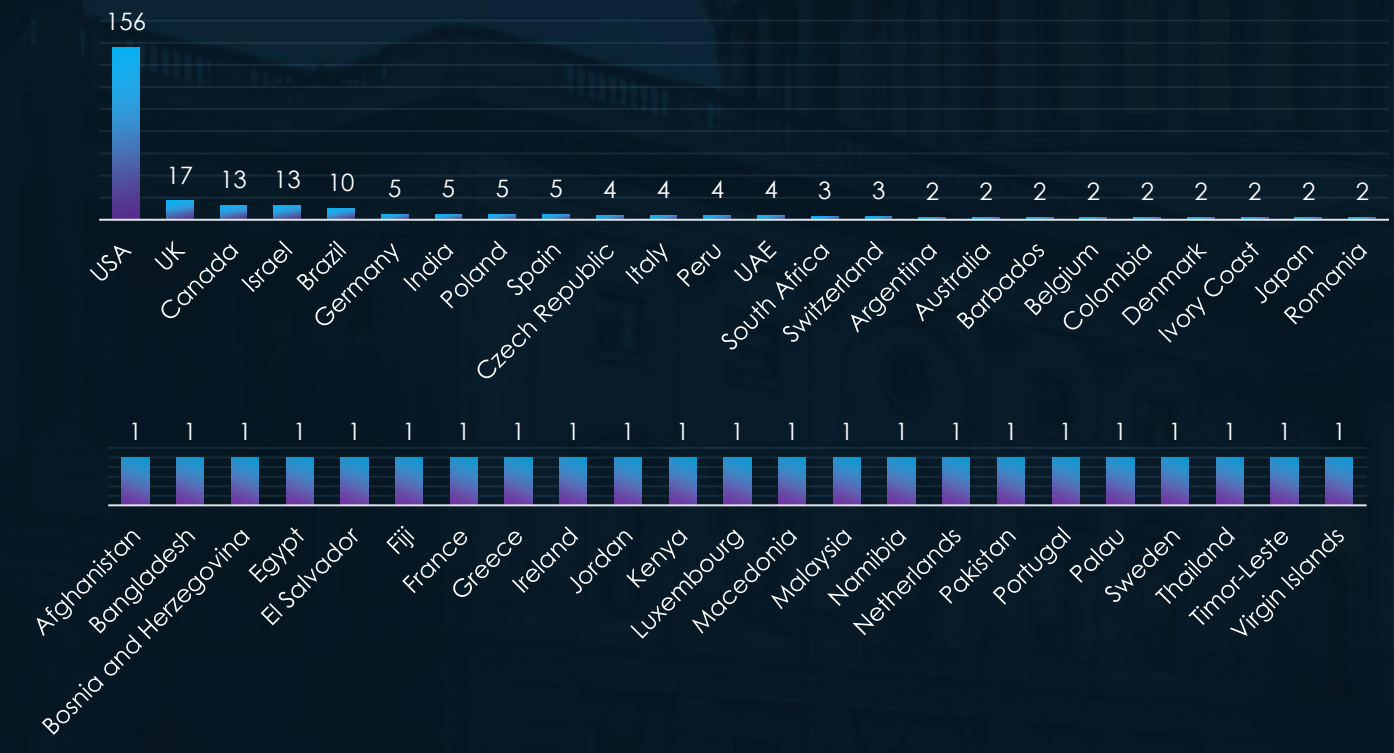
- Handala (8 victims, 21.05%) and Siegedsec (6 victims, 33.33%) reflect concentrated targeting efforts.
- Meow (12 victims, 8.96%), Blacksuit (12 victims, 8.22%), and Dragonforce (8 victims, 7.55%) also indicate meaningful focus.
- Stormous (4 victims, 8.89%) and Cicada3301 (3 victims, 7.69%) highlight focused efforts despite lower victim counts.

Some gangs exhibit disproportionately high percentages due to low victim counts:

- Pryx (2 victims, 66.67%) and Siegedsec (6 victims, 33.33%) show extremely high percentages driven by small absolute numbers.
- Knight (2 victims, 16.67%) and Mydata (2 victims, 15.38%) also display elevated percentages that are skewed by minimal activity.
- Madliberator (2 victims, 14.29%) and Snatch (2 victims, 11.11%) reflect similar trends of high focus but limited overall impact.

GEOGRAPHIC DISTRIBUTION OF VICTIMS



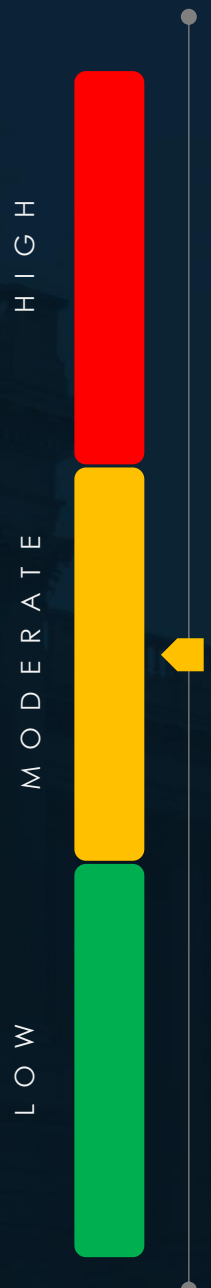


The USA accounts for 53.2% of ransomware victims in the Government & Civic Organizations industry in 2024. The next most affected countries are the UK with 17 victims, Canada with 13, Israel with 13, and Brazil with 10.

A total of 48 countries reported victims, with 24 of them having only one victim each.

CYFIRMA
DECODING THREATS

GOVERNMENT & CIVIC ORGANIZATIONS EXTERNAL THREAT LANDSCAPE MANAGEMENT (ETLM) OVERVIEW



Risk Level Indicator: Moderate

APT Campaigns

Government and civic organizations experienced a 35% incidence rate across APT campaigns, driven by nation-state and financially motivated actors. Groups like Lazarus and MISSION2025 focus on espionage and intelligence gathering, while financially driven actors like FIN11 and FIN7 pursue ransomware and extortion. Emerging groups like Handala and Siegedsec reflect diverse motivations, including political and social agendas.

Actors: FIN11, FIN7, Lazarus, MISSION2025, Mustang Panda, Gamaredon, Fancy Bear, emerging groups like Handala and Siegedsec.

Geographic Focus: U.S., Japan, U.K.; Asia-Pacific nations (India, Taiwan, South Korea); emerging markets (Indonesia, Philippines, Malaysia).

Targets: Web applications, operating systems, IaaS solutions, VPNs, and routers.

Malware: Winnti, NukeSped RAT, PlugX, Cobalt Strike; ransomware and tools like Mirai and Emotet.

Ransomware

The government & civic sector recorded 293 ransomware victims (5.61% of global total), reflecting the highest year-over-year growth (+69.62%) among industries. Activity was consistent with peaks in Q2 and Q4, though the sector diverged from the global trend with a calmer October and November, suggesting a slower start to 2025.

Victim Trends: Peaks in May and November; minor dips in February, March, and August.

Key Actors: Most active were Lockbit3 (35 victims, steady activity) and Ransomhub (35 victims, peak in November).

Other notable gangs were Play (20 victims, peaks in December, April, October); Incransom and Medusa (16 each).

Geography: U.S. accounted for 53% of victims; activity recorded in 47 countries.

Ranking: Government & civic organizations ranked as 7th most frequent victim of ransomware.

CYFIRMA
DECODING THREATS

THANK YOU

LET'S GET IN TOUCH

www.cyfirma.com

CYFIRMA DECODING THREATS

CYFIRMA is an external threat landscape management platform company. We combine cyber intelligence with attack surface discovery and digital risk protection to deliver early warning, personalized, contextual, outside-in, and multi-layered insights. Our cloud-based AI and ML-powered analytics platform provides the hacker's view with deep insights into the external cyber landscape, helping clients prepare for impending attacks. CYFIRMA is headquartered in Singapore with offices across APAC, US and EMEA. The company is funded by Goldman Sachs, Zodius Capital, Z3 Partners and L&T Innovations Fund.