CYBLE®

# GLOBAL THREAT LANDSCAPE H1 2025

REPORT

# Table of Contents

# Executive Summary

The first half of 2025 saw an unprecedented 54% increase in ransomware attacks compared to the same period in 2024, totaling 3,201 reported incidents. February was the most active month, with 848 attacks, largely driven by the aggressive campaigns of the CL0P ransomware group.

## Key Highlights

- North America remained the most targeted region, accounting for 65% of all attacks, with the United States alone experiencing 1,814 incidents (57% of the global total).
- The Construction and Professional Services sectors were the most attacked globally.
- Three ransomware operators—CL0P, Akira, and Qilin—were behind 34% of all attacks, emphasizing the growing dominance of fewer, more capable threat groups.

## Top Threat Actors

- CL0P led global activity, accounting for 37% of February's attacks alone. The group's hallmark is its exploitation of zero-day vulnerabilities in enterprise file transfer software, such as MOVEit and GoAnywhere MFT, with a focus on North America.
- Akira focused on North America and Europe, particularly targeting Germany's manufacturing and professional services sectors.
- Qilin, operating as a Ransomware-as-a-Service (RaaS), was notably active in the U.S., Europe, and Asia, with a significant April attack on the UK's NHS, demanding $50 million in ransom.

## Regional Breakdown

- **Europe:** Germany and the UK were hardest hit. Akira dominated with nearly 100 attacks, particularly targeting professional services and construction. Transportation infrastructure also faced significant disruption.
- **APAC:** Taiwan, Singapore, and India were the top targets. Groups like CrazyHunter, Qilin, RansomHub, and NightSpire exploited regional geopolitical tensions.
- **ANZ:** Ransomware attacks doubled year-over-year in Australia and New Zealand. Healthcare, SMEs, and professional services faced the brunt.
- **Middle East & Africa:** UAE and South Africa were top targets. Groups like Everest, RansomHub, and Lynx focused on IT, construction, and energy sectors.

## Zero-Day Exploitation Trends

- 63 zero-days were reported in H1 2025, with Microsoft (19) and Apple (6) being the most affected vendors.
- Exploitation of Microsoft Windows, Edge, and Ivanti Connect Secure was rampant, enabling deeper and faster intrusions.
- Supply Chain Threats on the Rise
- A 30% rise in software supply chain attacks was observed, with April alone recording 31 incidents.
- Most targeted were IT, telecom, and tech service providers, exposing downstream organizations in finance, government, and healthcare.

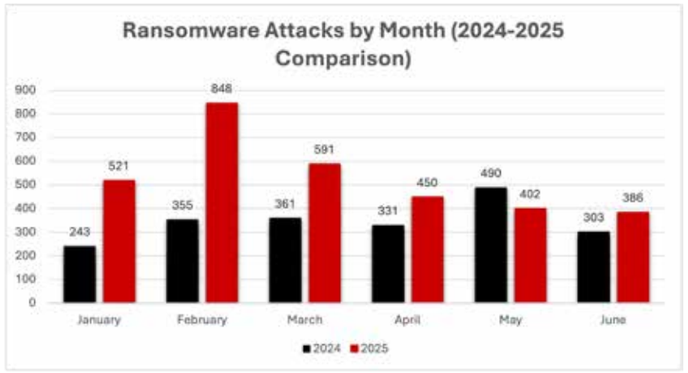
## Emerging Ransomware Groups

- Groups like Dire Wolf, DATACARRY, Silent Team, and Gunra have surfaced with new leak sites, targeting victims across Asia, Europe, and the Americas.
- These groups are experimenting with data extortion, some without even deploying lockers, signaling a tactical evolution.
- Hacktivism Evolves into Industrial Threat
- Hacktivist campaigns in 2025 showed a dramatic increase in sophistication and scale.
- Russia-linked groups Z-Pentest, Sector 16, and Dark Engine launched coordinated attacks on industrial control systems (ICS) in energy, transportation, and utilities sectors.
- Cyber campaigns tied to geopolitical conflicts (e.g., Iran-Israel, Ukraine-Russia) now regularly feature ransomware and ICS exploits.

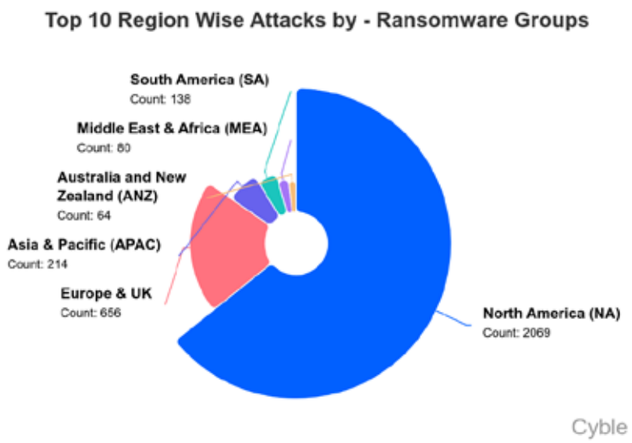
H1 2025 marks a clear escalation in both volume and sophistication of ransomware attacks. From zero-day abuse and sector-specific targeting to the rise of multi-continent hacktivism and software supply chain threats, organizations face a landscape that demands proactive threat intelligence, robust patching hygiene, and cross-sector cyber resilience strategies.

# Key Statistics

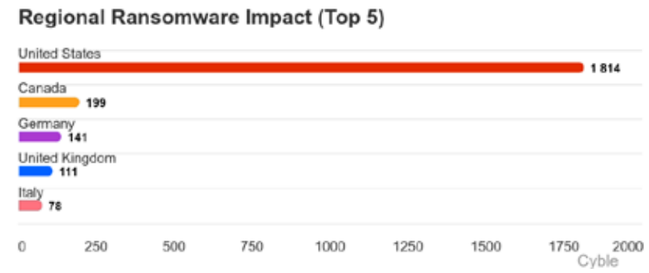
**54%**
First half of 2025 saw a 54% increase in ransomware attacks as compared to last year



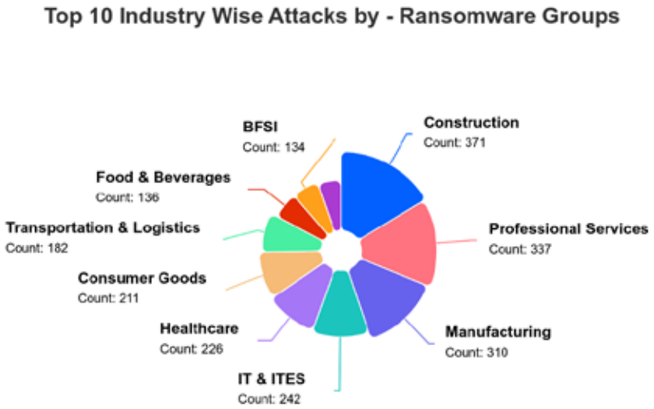

**65%**
North America continued to be the most targeted region



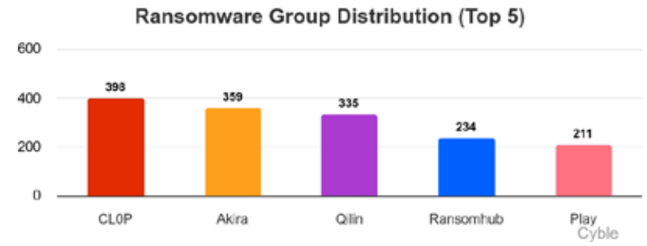

**3201**
Total no. of ransomware incidents in H1 2025




**Most Targeted Sectors**
Construction and Professional Services




**34%**
One in three ransomware attack was carried out by either CL0P, Akira, Qilin

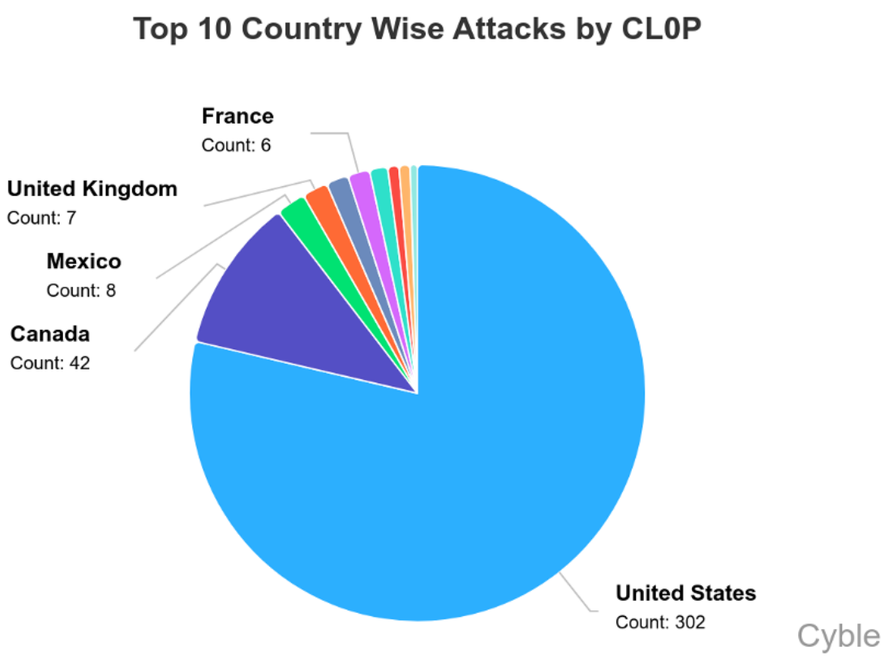


# CL0P, Akira, Qilin Ransomware Operators Top Contributors

## Cl0P

While Cl0P ransomware actors targeted organizations globally, their primary focus remained North America – particularly the Unites States and Canada which together accounted for 344 victims of the group. 3 out of their every 4 victims was from the North American region.

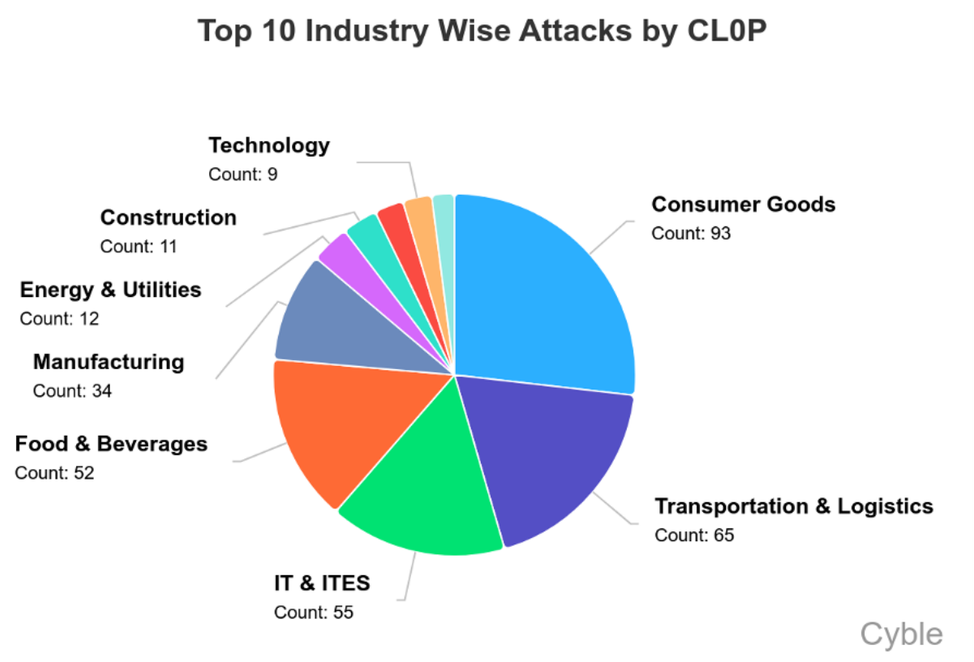
Cl0P also recorded 37% of all February ransomware attacks globally. February saw the highest number of ransomware attacks this year with 848 incidents.




The Cl0P ransomware group, active since at least 2019, is a financially motivated threat actor known for high-impact, large-scale cyber extortion campaigns. Cl0P's expertise lies in exploiting zero-day vulnerabilities in widely used enterprise software to gain initial access, exfiltrate sensitive data, and deploy ransomware. Their hallmark is the use of double extortion: not only encrypting victims' data but also leaking or threatening to leak stolen information on their dedicated leak site, "CL0P^_- LEAKS."

What sets Cl0P apart is its use of sophisticated zero-day vulnerabilities. Most notably, the group exploited CVE-2023-34362—a critical SQL injection flaw in Progress Software's MOVEit Transfer managed file transfer application. The exploitation allowed unauthorized access and data exfiltration from hundreds of organizations globally before the vulnerability became publicly known. Cl0P previously targeted similar platforms, exploiting Accellion FTA (CVE-2021-27101, CVE-2021-27102, CVE-2021-27103, CVE-2021-27104) and GoAnywhere MFT (CVE-2023-0669), revealing a pattern of targeting secure file transfer solutions used by enterprises.

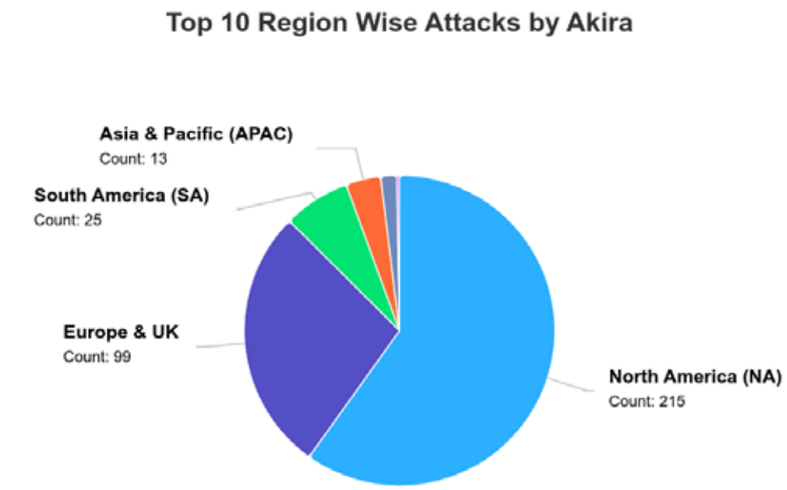
Cyble's Research and Intelligence Labs has historically observed Cl0P typically targeting organizations in finance, education, healthcare, and government, often selecting victims based on their size and data value. But their focus in H1 2025 has shifted to Consumer Goods, Transportation and Logistics and IT & ITES. The group's operations are linked to TA505, a cybercriminal group with a history of advanced phishing and malware campaigns, amplifying Cl0P's reach and capabilities.



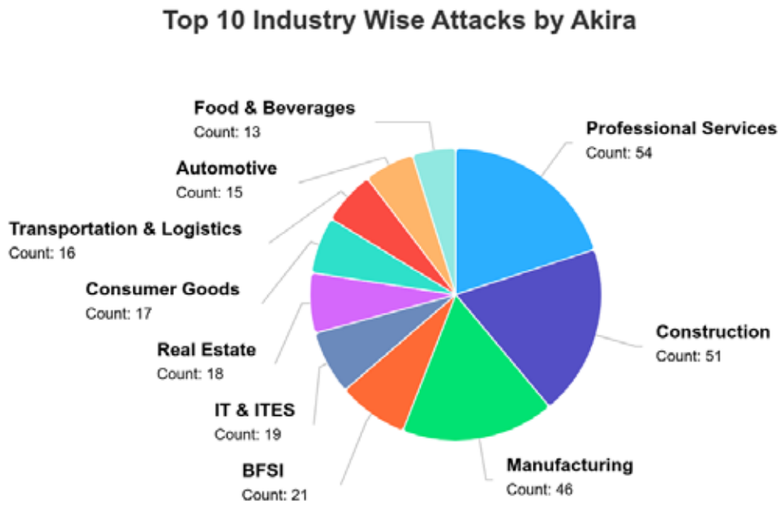

Unlike many ransomware-as-a-service (RaaS) operations, Cl0P is more centralized, controlling the entire attack lifecycle from initial access to extortion. This model, combined with rapid exploitation of zero-days and data-centric extortion tactics, makes Cl0P one of the most disruptive ransomware gangs operating today.

## Akira

Akira has majorly targeted the North American region – again with U.S. under the scanner. However, the ransomware group also focused on Europe where the core sectors of the economy – professional services, construction and manufacturing – were the prime targets.



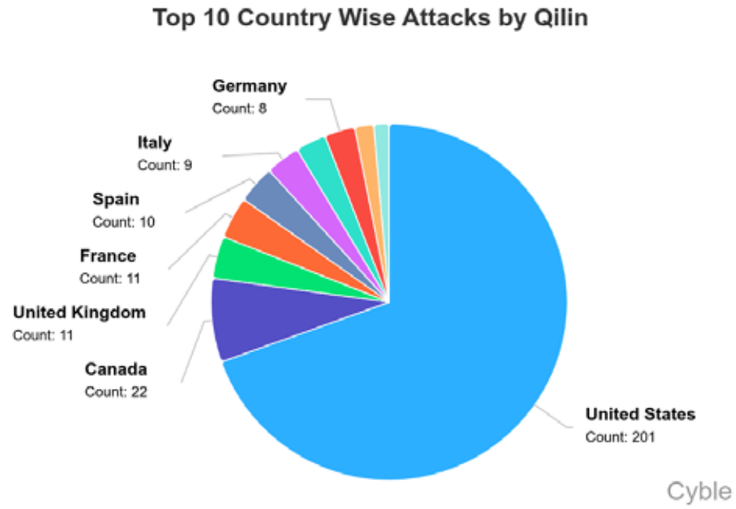

In Europe, Germany was the most attacked country. Being the manufacturing hub, the sector's contribution to GDP remains a significant part of the economy. In 2024, the value added by the manufacturing sector was 19.7% of GDP, according to deutschland.de. The same year, the turnover of companies in the manufacturing sector was recorded at 2,900 billion euros, with the automotive and manufacturing industry being the largest. While the services sector has grown in prominence, manufacturing continues to be a major driver of the German economy and likely the deciding factor for threat actors' adversarial targeting.



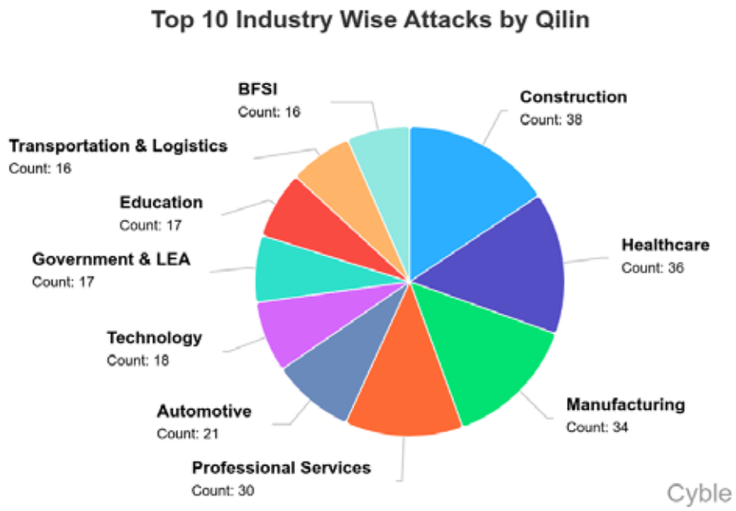



## Qilin

Qilin ransomware operators complete the top three most active ransomware actors list and like others, with over 200 attacks, these operators also mainly targeted the U.S.



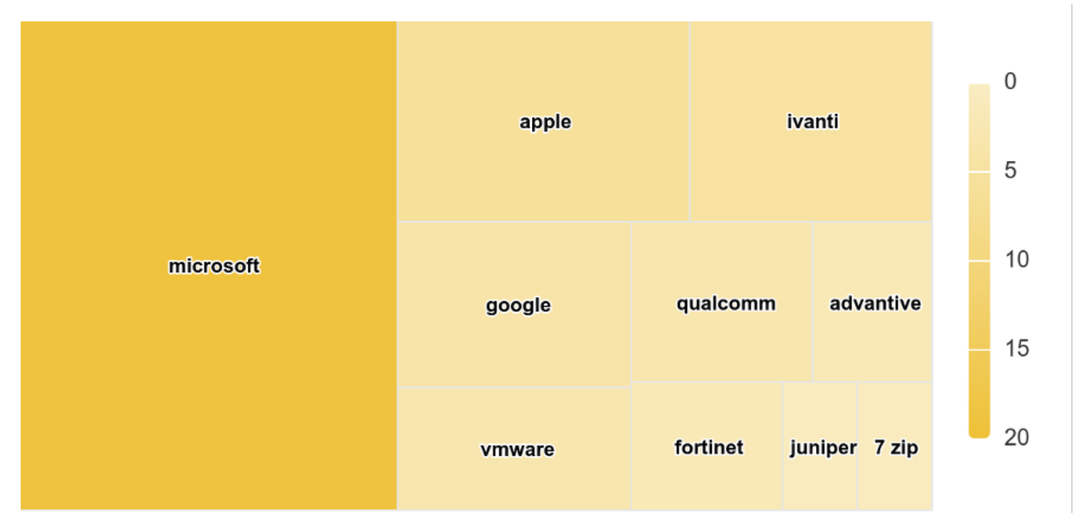

Qilin operates in the ransomware-as-a-service provider bracket and enables affiliates to launch highly customizable attacks across various sectors, including healthcare, manufacturing, and government services. Other notable sectors in H1 2025 for Qilin were construction, professional services and automotive.




Qilin operators listed most number of victims (72) in April 2025. The gang grabbed most attention for its attack on the Synnovis systems that crippled emergency services at UK's NHS centers. The group made an outrageous ransom demand of $50 million, which the authorities turned down. NHS recently stated that even after a year since the attack, it is still reeling through the aftermath.

# List of Weaponized Vulnerabilities

During the reporting period, Linux fixed 2619 vulnerabilities followed by a distant second Microsoft with 584 flaw fixes. But the numbers that matter most is the top affected vendors by zero-days and the Redmond giant topped this. Microsoft reported 19 zero-days. The list of top five vendors impacted by zero-days was completed by Apple (6), Ivanti (5), Google (4) and VMware (3).




A total of 63 zero-days were reported in H1 2025 but some of the most notable ones which Cyble believes to have seen a proof-of-concept available in the open are listed below:

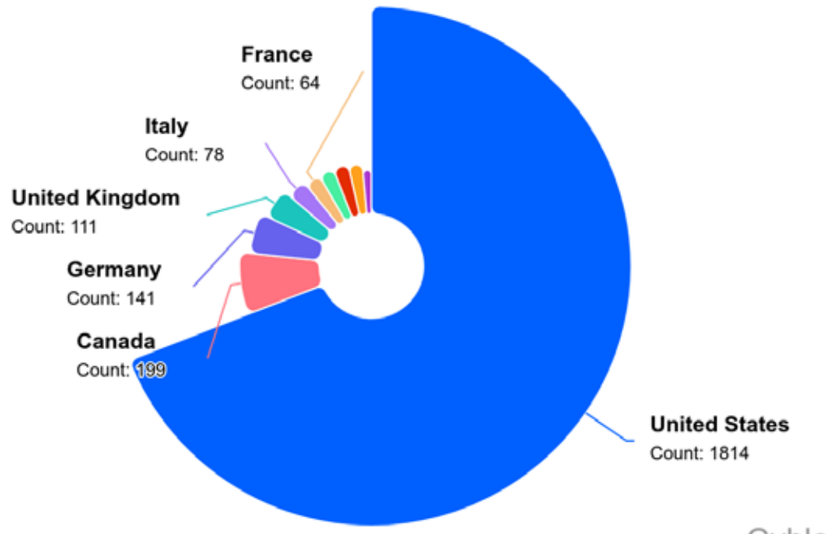
| Vulnerability CVE | Vendor | Product |
|---|---|---|
| CVE-2025-33053 | Microsoft | Windows 10 |
| CVE-2025-5419 | Microsoft | Edge Chromium |
| CVE-2025-30400 | Microsoft | Windows 10 |
| CVE-2025-30397 | Microsoft | Windows 10 |
| CVE-2025-24993 | Microsoft | Windows 10 |
| CVE-2025-24201 | Apple | MacOS |
| CVE-2025-24085 | Apple | TvOS |
| CVE-2025-43200 | Apple | iOS and iPadOS |
| CVE-2025-0282/0283 | Ivanti | Connect Secure |
| CVE-2025-4427/4428 | Ivanti | EPMM |
| CVE-2025-22457 | Ivanti | Connect Secure, Policy Secure, Neurons for ZTA Gateways |
| CVE-2025-5419 | Google | Chrome |
| CVE-2025-6554 | Google | Chrome |
| CVE-2025-22224 | VMware | ESXi |
| CVE-2025-22225 | VMware | Cloud Foundation |
| CVE-2025-22226 | VMware | Workstation |

# Region Wise Ransomware Threat Landscape

## United States

The U.S. once again led all countries in ransomware with 1814 attacks, or 57% of the global total, against them followed by a distant second Canada (199).

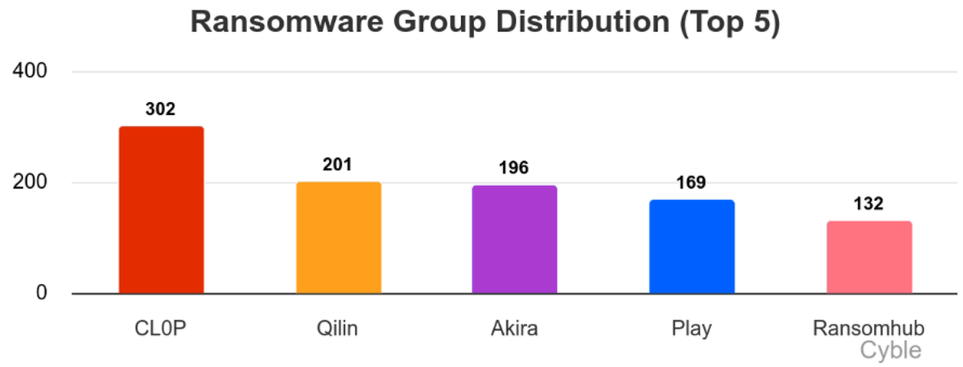
### Top 10 Country Wise Attacks by - Ransomware Groups




Following on global trends, CL0P most actively targeted organizations and businesses in the U.S. with 302 attacks under its name. Qilin and Akira followed suit.

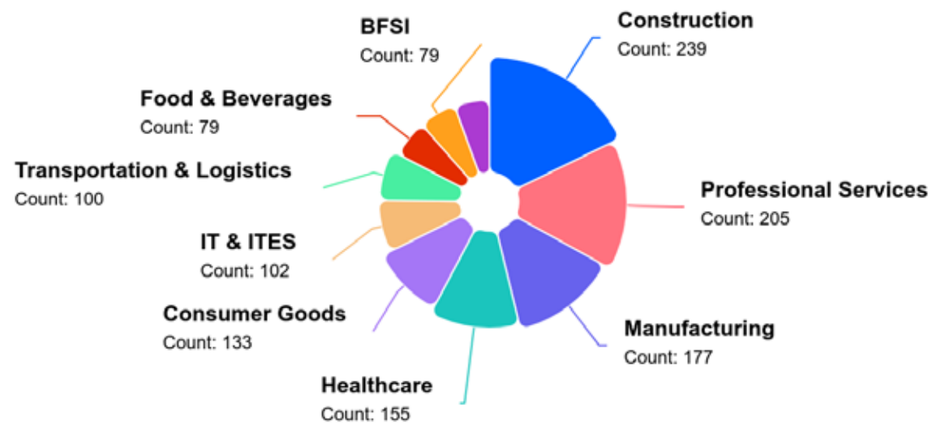


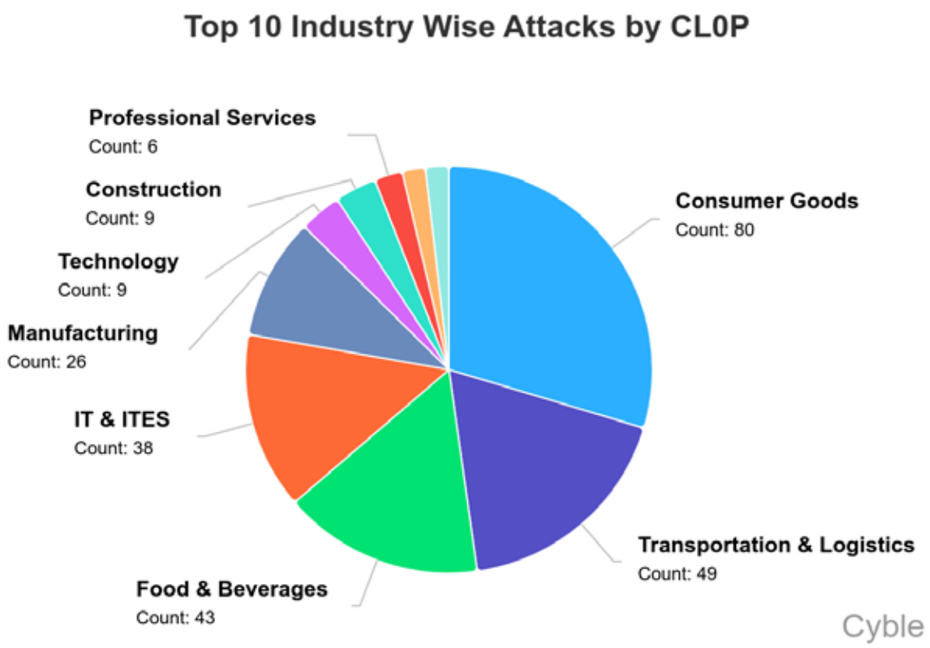

### Ransomware Group Distribution (Top 5)




While industry-wise Construction and Professional Services were the most targeted sectors in the U.S., CL0P concentrated on the Consumer Goods, Transport & Logistics, and Food & Beverages sectors.

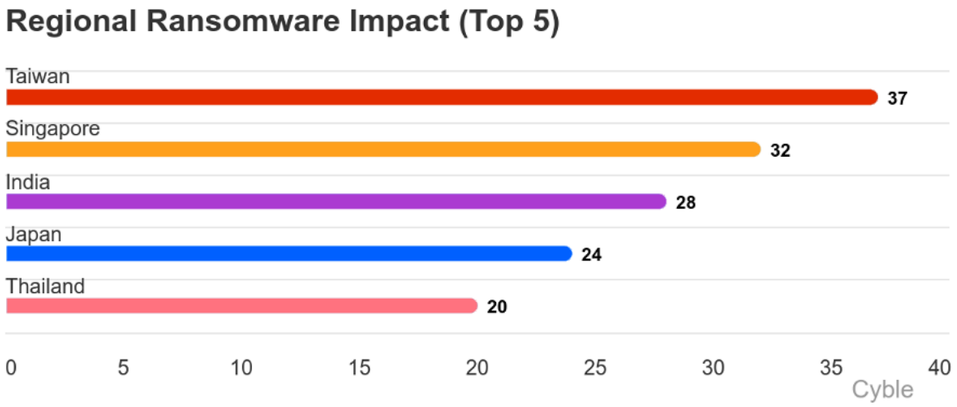
### Top 10 Industry Wise Attacks by - Ransomware Groups






## APAC

In Asia and Pacific, Taiwan was the most targeted country with 37 recorded incidents followed by Singapore (32), India (28), and Japan (24). The geopolitical tension in the South-East Asian countries seems to being leveraged by opportune ransomware actors in this region. A total of 219 attacks were recorded here.





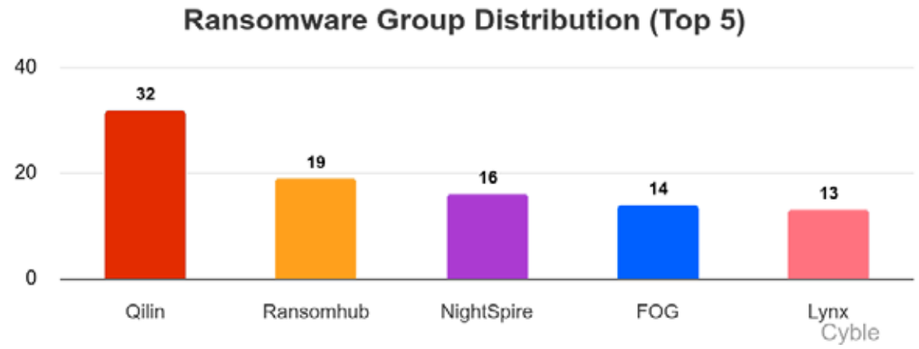


The LockBit Team was the most active in Taiwan and targeted its Healthcare and Technology sectors. NightSpire, Akira and Lynx were the other actors targeting the island nation.

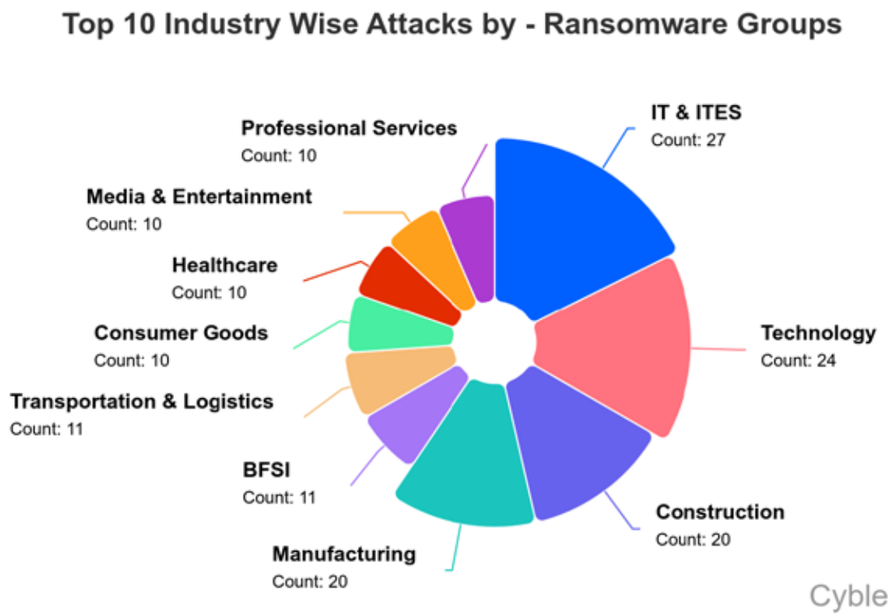
In India, Qilin, RansomHub and Medusa were the most active actors with IT, BFSI, and Manufacturing being the top three target sectors.

Qilin was the most prolific threat actor in this region with 32 attacks and most of them were targeted at Singapore, India, and Japan. Second on the list is Ransomhub (19) and NightSpire (16).

Qilin was the most active ransomware actor in the region in April with 11 attacks.

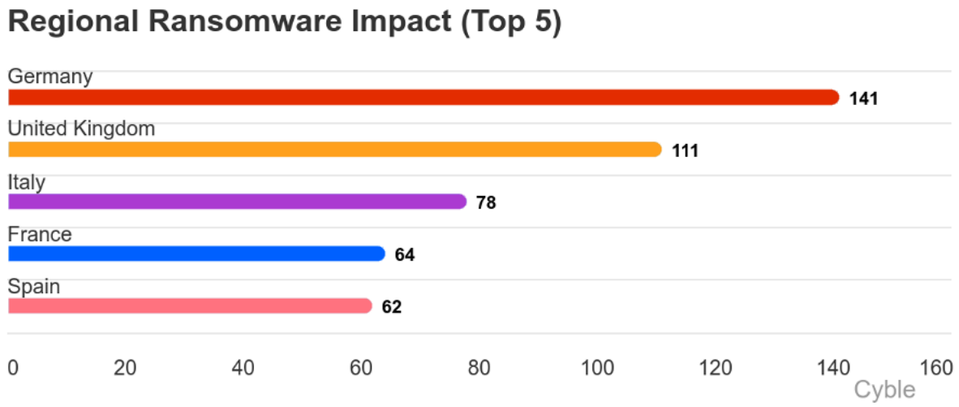



Sector-wise, IT and Technology were the most targeted, but RansomHub also concentrated on the Construction and Manufacturing sectors which form the backbone of the region where most of the countries fall under the developing countries bracket.



## Europe and United Kingdom

Being the second most targeted region after North America, Germany, the U.K., followed by Italy, France and Spain were the most targeted countries of the region. A total of 663 ransomware attacks were recorded in this region in H1 2025.

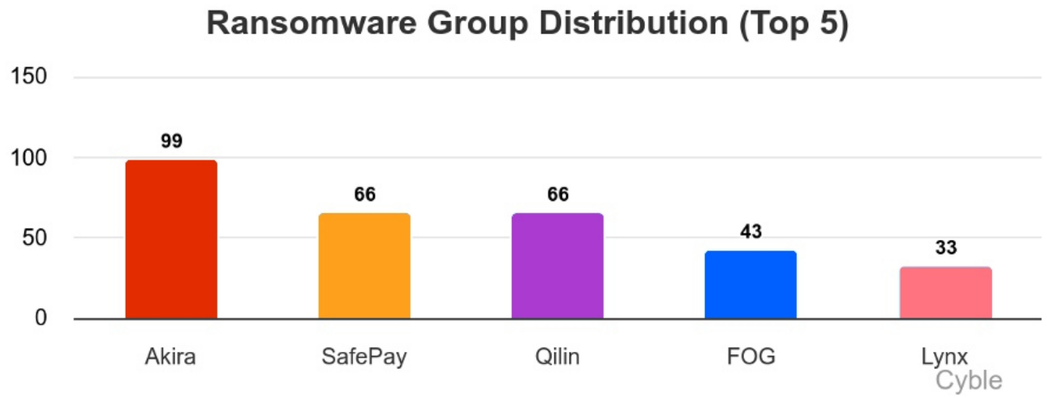



SafePay ransomware actor was the most active (45 attacks) in Germany with 32% of the attacks attributed to this ransomware group. Their primary targets: Professional Services and Construction. Germany being an automotive hub, this sector, along with manufacturing was also on the target list of several ransomware actors.

In the United Kingdom, Medusa (14) and Qilin (11) were the most prolific ransomware actors who targeted Professional Services (20), Manufacturing (15) and Construction (13) sectors. Other notable sectors that saw targeted attacks in U.K. were Healthcare, BFSI and Transport and Logistics.

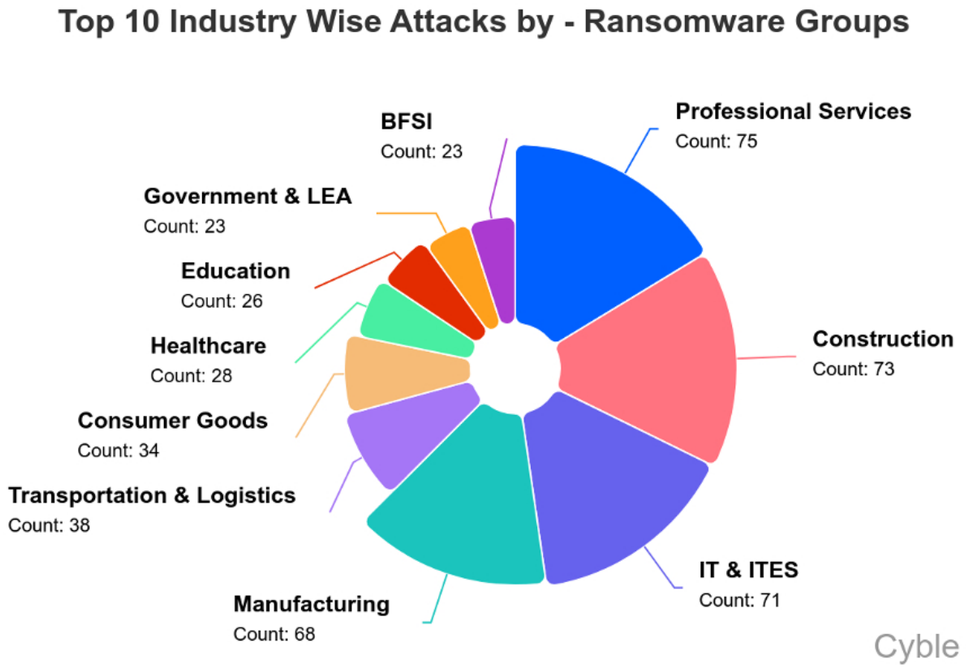
In Italy, Akira was the most active group whereas in France Qilin and 8Base led the list.

Akira was the most active ransomware group in the region with nearly 100 attacks that were primarily targeted at the Professional Services and the Construction sector.





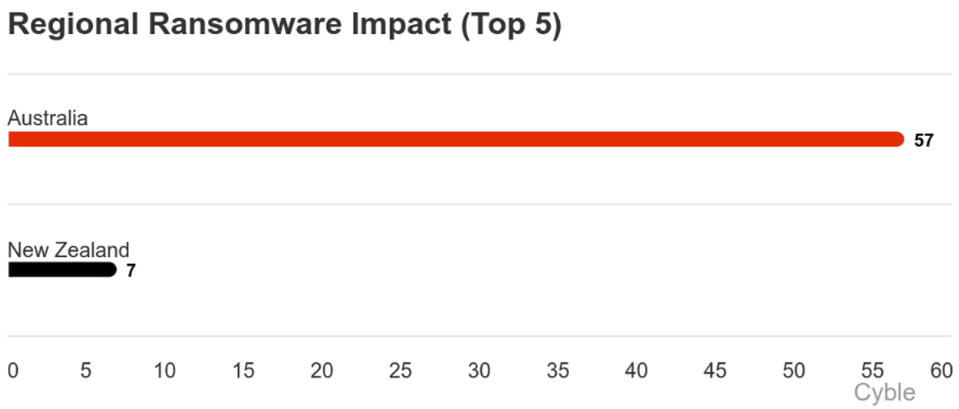

Overall, the Professional Services, Construction, and IT & ITES sectors were the most targeted in Europe and the U.K. as they accounted for nearly 50% of all the attacks.



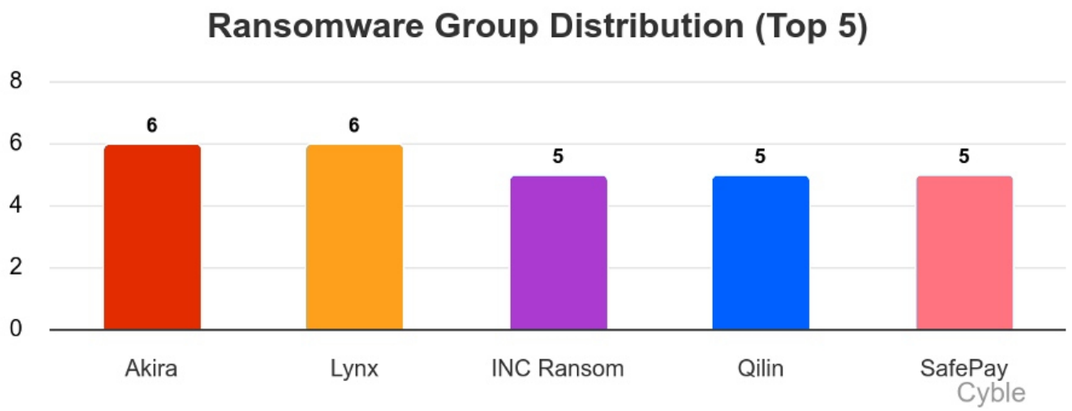

The transport sector in the region has also been under severe pressure since the last quarter. A cyberattack on the city's transportation in London, had resulted in a severe impact on its online ticketing system for weeks. Apparently, a 17-year-old teenager was behind the attack who siphoned some customer details in the process. The teenager was arrested 10 days after the attack.

## Australia and New Zealand (ANZ)

The ransomware threats "Down Under" doubled in the first six months of the year as compared to the last year. Australia saw 57 ransomware attacks whereas the Kiwi land further down south registered seven attacks – taking the total number of ransomware attacks in the region to 64.



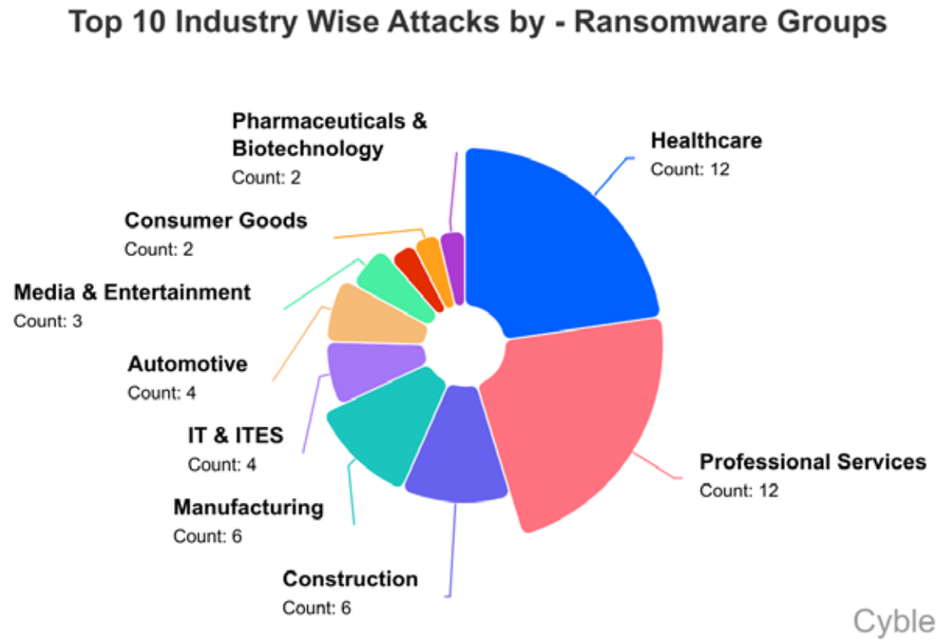

The prevalence and sophistication of ransomware campaigns have escalated significantly. While Sarcoma and Safepay were the prominent active threat actors in the region for the first quarter, Akira, Lynx and INC Ransom actors dominated the region in the second half. In fact, the latter (INC Ransom) primarily targeted the healthcare sector in this region including a devastating attack on Tonga's Ministry of Health.




Healthcare and professional services, and small to medium-sized enterprises (SMEs) were the most targeted sectors here. The region also saw an increase in payment demands, with averages exceeding USD $750,000.

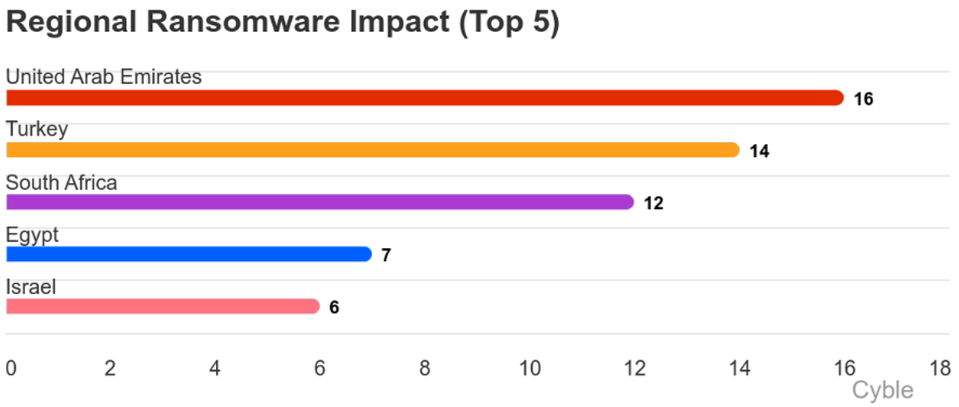
Also, While Akira concentrated on the targeting of the Manufacturing sector, Healthcare (12) and Professional Services (12) remained the primary targets, followed by Construction (6).



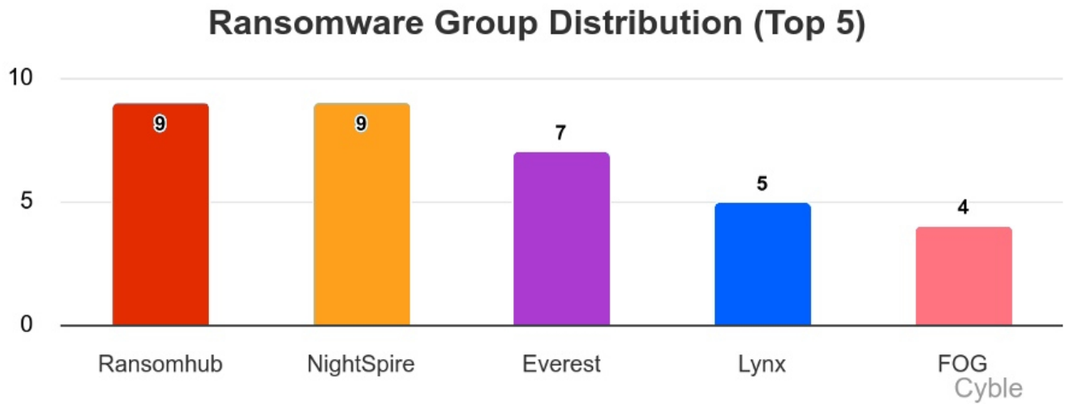




## Middle East and Africa

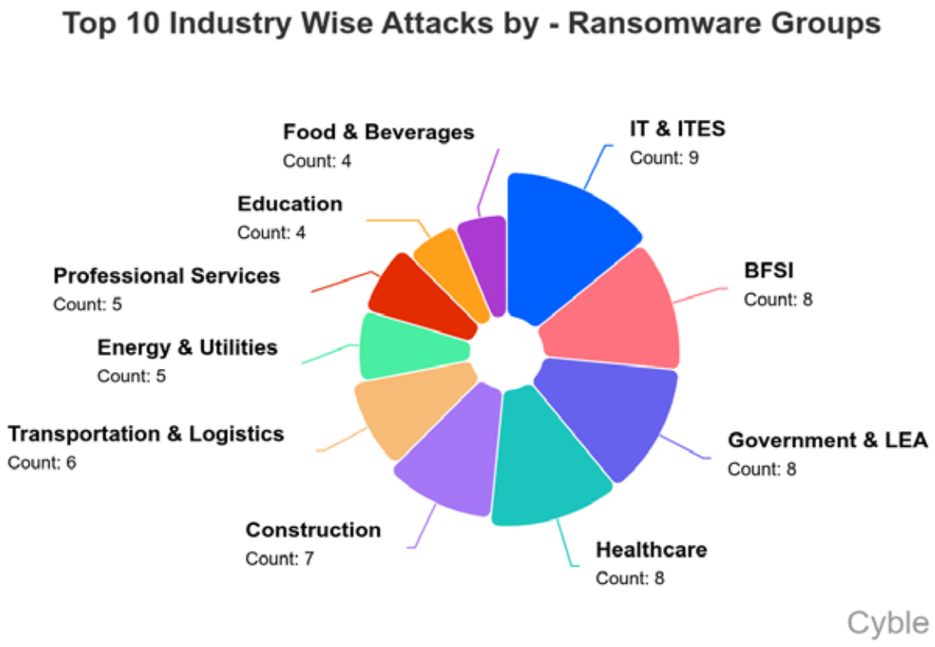
Middle East saw the UAE take the top slot  while South Africa remained the focus of ransomware actors in Africa.




Everest group was the primary threat actor in the UAE. While RansomHub (9) and NightSpire (9) targeted the region equally with nine attacks each, Everest (7) and Lynx (5) were the most active in Q2 2025.




As UAE sees rapid development owing to the policies for growth, ransomware actors continued to focus on the critical infrastructure sectors like Healthcare, Construction, and Energy and Utilities, of the Emirates. But overall, the IT landscape is one of the fastest evolving in the region which remained the prime focal point of ransomware actors followed by the BFSI sector that keeps the money flowing into the rest of the sectors.




# New Ransomware Groups

## Dire Wolf

Among new ransomware groups that have emerged recently, “Dire Wolf” launched an onion-based data leak site (DLS), listing six victim organizations, primarily across Asia, Australia and Italy. For each organization, Dire Wolf posted a file tree, sample files, and descriptions of the allegedly stolen data.

## DATACARRY

A new ransomware group named DATACARRY was observed actively targeting European companies through a newly established onion-based data leak site. The group has listed seven victims from diverse sectors and countries, leaking parts of allegedly stolen data. The group communicates with victims via Session messenger and has circulated a ransom note, though no locker has been yet observed.

## “J”

A newly emerged ransomware group calling itself “J” has launched an onion DLS, following earlier signs of activity observed in March 2025. In its initial disclosure, J listed multiple organizations across South America, Australia, Europe, the U.S. and Asia. The group has shared file trees of allegedly compromised data of victim organizations in support of their claims.

## Silent Team

Silent Team surfaced with an onion data leak site (DLS), claiming two victims: a U.S.-based engineering company and a Canadian aerospace manufacturer. According to the leak site, the group allegedly exfiltrated 2.85 TB of data across 597,028 files and posted multiple samples showing internal documents, ID scans, technical schematics, database structures, engineering blueprints of aircraft, and other sensitive documents. The Silent Team DLS design mimics that of Hunters International. No known encryptor samples have yet surfaced.

## Gunra

A newly identified ransomware group, tentatively named Gunra by the threat intelligence community, has also surfaced with an onion data leak site. The group has listed three victims so far: a Japan-based real estate company; a medical firm in Egypt; and a Panama-based beverage and distribution company.

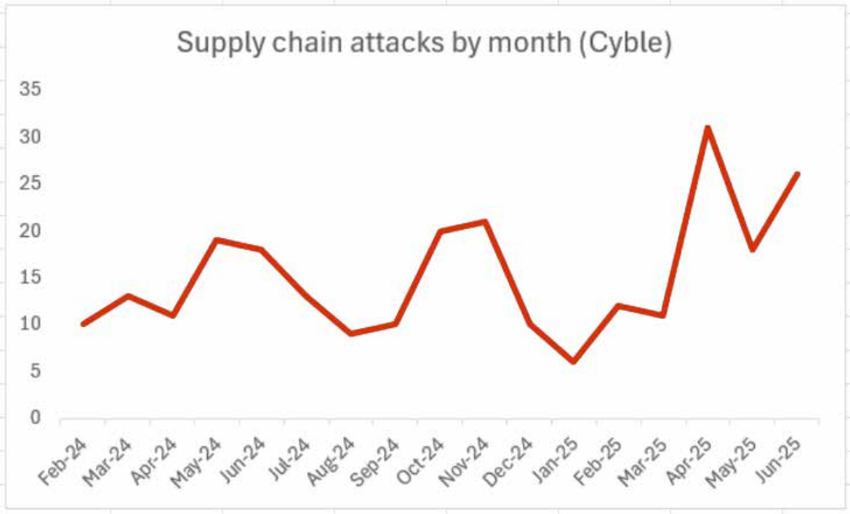



© 2025 Cyble Inc. All rights reserved.

# Software Supply Chain Attacks Surged in the Second Quarter

IT and software supply chain incidents have been trending higher in recent months, as threat actors have become more adept at exploiting the interconnected hardware, software, and services that comprise modern IT environments.

An analysis of Cyble data reveals that software supply chain attacks have increased from an average of just under 13 a month during the eight-month period of February-September 2024 to just over 17 a month from October 2024 to June 2025, an increase of more than 30% in the most recent nine-month period. The three months that comprised the second quarter of 2025 averaged 25 cyberattacks with supply chain impact, which would represent a near-doubling of supply chain attacks if the recent trend continues (chart below).




However, monthly variations in supply chain attacks tend to be quite large, ranging from a low of 6 attacks in January 2025 to a high of 31 attacks in April 2025, so some variability should be expected even as supply chain attacks generally trend higher.

What follows is an analysis of software supply chain attack trends, including targeted industries and countries, a closer look at 10 significant incidents.

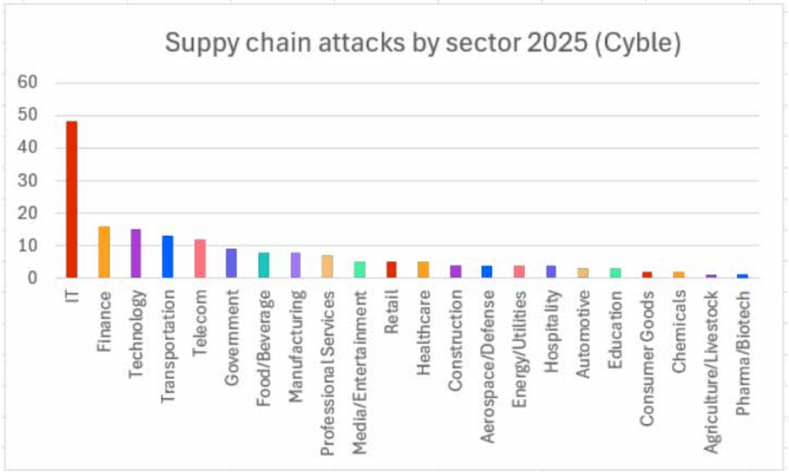



## Software Supply Chain Attacks: Targeted Industries and Countries

Looking at the 105 cyberattacks with supply chain implications documented by Cyble in the first six months of 2025, the majority (65, or 62%) directly targeted IT, technology, and telecommunications companies, which are rich potential targets for threat actors hoping to exploit downstream users.

Damage from a single successful exploit in those areas can be widespread, as happened with the hundreds of CL0P ransomware victims from a single vulnerability.

Supply chain attacks hit 22 of the 24 sectors tracked by Cyble in the first six months of 2025 (chart below). Only the Mining and Real Estate industries remained untouched.




Within non-tech industries, supply chain attacks often stem from third parties and service providers, including industry-specific solutions.

Among targeted countries, the U.S. was a target in 42 of the 105 incidents. European countries were targeted in 32 incidents, with France (10 incidents) experiencing the highest number of European attacks.

36 of the incidents targeted APAC countries, led by India (13 incidents) and Taiwan (4). The Middle East and Africa were targets in 14 incidents, including five each in the UAE and Israel.

## Notable Supply Chain Incidents

Here are details of 10 supply chain incidents documented by Cyble in recent months.

- Everest Ransomware claimed a ransomware attack on a Swiss banking technology solutions and services company. Included in the exfiltrated data were login credentials to various banking applications.
- An IT services subsidiary of a large international conglomerate confirmed that it was impacted by a ransomware incident believed to be the responsibility of the Akira ransomware group. The incident may have impacted multiple projects tied to government entities.
- A threat actor (TA) on the English-language cybercrime forum DarkForums offered for sale a large dataset allegedly pertaining to a high-throughput telecommunications satellite for Indonesia and some ASEAN countries. The TA claimed that the entire dataset is 92 GB in size and includes technical documents related to propulsion tests, launch analyses, ground systems, site vulnerabilities, and more.
- The Hellcat ransomware group allegedly compromised a China-based company specializing in display technologies and electronic solutions. The threat actor claimed to have exfiltrated 166 GB of data, including blueprints, financial records, and internal correspondence.
- The DragonForce extortion group claimed responsibility for an attack on a U.S. company specializing in biometric recognition and identity authentication solutions, from which the group claimed to have exfiltrated more than 200 GB of data.
- The VanHelsing ransomware group claimed responsibility for compromising a U.S.-based company specializing in enterprise security and identity access management (IAM) solutions. The nature of the exposed files suggests they may contain sensitive information linked to the company's customers, potentially affecting sectors such as Banking, Financial Services, and Insurance (BFSI).
- A threat actor on the cybercrime forum Exploit claimed to offer unauthorized access with administrative privileges to the cloud infrastructure of an India-based fintech company specializing in SaaS-based payment service solutions.
- The extortion group Crypto24 claimed responsibility for a cyberattack on a Singapore-based technology company, alleging the theft of 3TB of data. According to the group, the compromised information includes customer records, database content, technical and project documentation, and other internal files from the company's servers and NAS systems.
- Killsec hacking group claimed responsibility for compromising an Australia-based company that offers IT and telecom solutions. While the group did not disclose the volume of data exfiltrated, leaked content included backup data, licensing and application configuration files, software license types, hashed credentials, and other critical infrastructure-related datasets.
- The Medusa ransomware group claimed responsibility for compromising a U.S.-based technology solutions provider specializing in IT infrastructure, cloud services, cybersecurity, and systems integration for public sector and enterprise clients.



© 2025 Cyble Inc. All rights reserved.

# Hacktivism Gets More Sophisticated

Hacktivism is typically associated with DDoS attacks and website defacements, but in the first half of 2025, hacktivists became significantly more sophisticated, with some groups moving into ransomware and critical infrastructure attacks. As hacktivist groups often work together, that growing sophistication will likely spread to other groups over time.

Hacktivism in 1H 2025 tended to follow conflicts, with Ukraine-Russia, Israel-Iran, India-Pakistan, Thailand-Cambodia, and Morocco-Algeria among the flashpoints for hacktivist activity that has also targeted other countries perceived as allies. Vietnam has also been a target of significant hacktivist activity this year.

## Critical Infrastructure Hacktivism

Among groups targeting critical infrastructure, Russia-linked Z-Pentest has emerged as the leading hacktivist group, with 38 ICS attacks in the second quarter after notching 15 in the first quarter of 2025. Z-Pentest's consistent targeting of energy infrastructure across multiple European countries reflects a structured and sustained campaign approach. A frequent Z-Pentest tactic is to post screen recordings of members tampering with ICS controls.

Two other Russia-linked groups have also actively targeted industrial control system (ICS) environments. **Dark Engine** – a new group – accounted for 26 ICS-targeted incidents in the second quarter, with a significant operational surge in June, while Sector 16 – which first emerged in January – was linked to 14 attacks in the most recent quarter.

The groups have aligned messaging, coordinated timing, and shared targeting priorities, suggesting deliberate collaboration in support of Russian strategic cyber objectives.

The Energy & Utilities sector has emerged as the primary focus of ICS attacks, highlighting a strategic emphasis on infrastructure tied to national resilience. Additional targeting has been observed in the Manufacturing, Transportation, and Telecommunications Sectors, including attempts to compromise control systems within national networks.

Italy was the most frequently targeted in ICS attacks by hacktivists, followed by other NATO-aligned states, including the U.S., Czech Republic, France, and Spain.

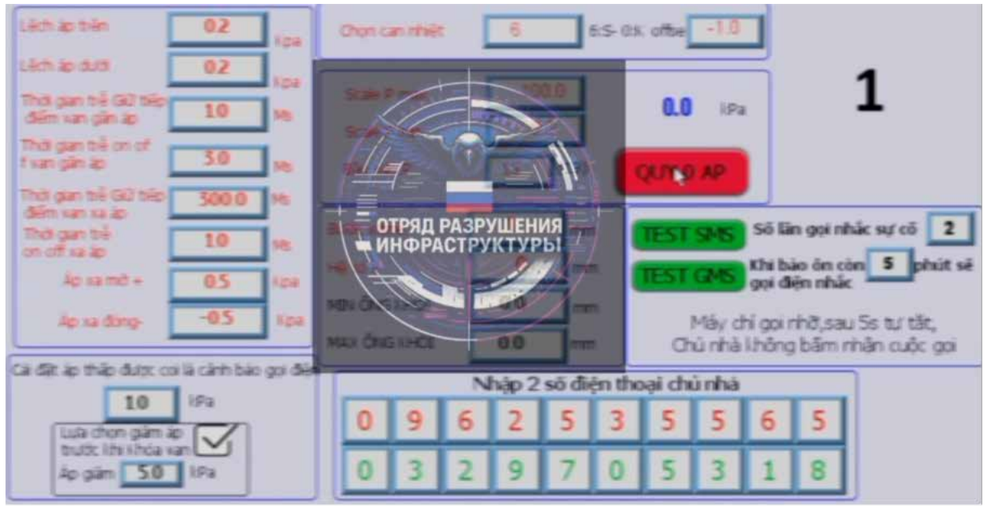


## New Hacktivist Groups

**Dark Engine** has operated across multiple continents, with confirmed activity in the EU, Asia and Latin America. The group has engaged in a range of tactics—access-based intrusions, data breaches, and ICS attacks—demonstrating both strategic breadth and technical depth. The group's targeting has spanned critical infrastructure, notably the Energy and Utilities sector, along with Food & Beverages, Education, and Manufacturing, indicating a deliberate focus on national resilience sectors.

In a recent incident, Dark Engine – also known as the "Infrastructure Destruction Squad" – claimed unauthorized access to a HMI/SCADA interface used in Vietnamese industrial operations. As observed from the leaked screenshots of the compromise (sample below), the breached system controls a high-temperature furnace likely used in sectors such as metallurgy, ceramics, cement, or food processing.

The group's justification for the attack references its stance against any nation perceived as hostile to China. Dark Engine frames its activity as part of a cyber campaign in geopolitical alignment with the Eastern bloc, reinforcing its ideological commitment through targeted industrial disruption.




*A screenshot of a Dark Engine SCADA compromise*

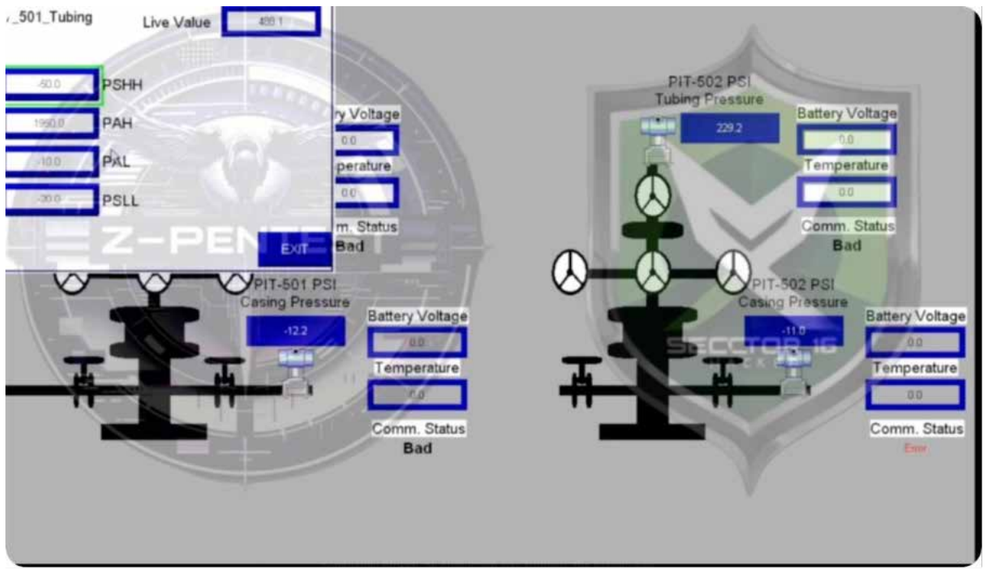
**APT IRAN** is an emerging group that has maintained a highly focused operation during the Iran-Israel conflict. With observed activity in the U.S., the group has executed ICS-specific operations against the energy sector. The group's selectivity, timing, and infrastructure targeting suggest alignment with national strategic interests and OT-centric intrusion capabilities.

**BL4CK CYB3R**, a Cambodian politically motivated collective, has mainly targeted Thailand. The group has employed both access and DDoS attacks, impacting a wide range of sectors, including IT & ITES, government, and consumer goods. BL4CK CYB3R were extremely active during the Thailand-Cambodia border conflict that began in late May.

## Hacktivist Attacks Against ICS/OT Environments

Sector 16 first emerged in January in a teamed attack with Z-Pentest on a SCADA system managing oil pumps and storage tanks in Texas. The groups shared a video showcasing the system interface, revealing real-time data on tank levels, pump pressures, casing pressures, and alarm management features.

Both groups put their logos on the video, suggesting a close alliance between the two (image below).




Sector 16 also claimed responsibility for unauthorized access to the control systems of a U.S. oil and gas production facility, releasing a video purportedly demonstrating their access to the facility's operational data and systems. Displayed systems include shutdown management, production monitoring, tank level readings, gas lift operations, and Lease Automatic Custody Transfer (LACT) data, all critical components in the facility's operations. Additionally, the group was also able to access valve control interfaces, pressure monitoring, and flow measurement data, highlighting the potential extent of access.

In one February incident, Z-Pentest claimed to gain unauthorized access to a fuel refinery management system in the United States. The attackers stated that they accessed the SCADA system responsible for monitoring and controlling fuel storage, distribution, and operational parameters.

The group shared images of their unauthorized access, displaying system dashboards with fuel tank levels, pressure readings, temperature data, and alarm statuses (example below). The images do not contain the name and location of the Refinery, but Z-Pentest said it is located in the U.S.





*Z-pentest tampering with fuel refinery controls*

In one incident, Sector 16 collaborated with the Russian group **OverFlame** to claim unauthorized access to the control systems of a hydroelectric facility operated by Dynelec in the southern region of France. As revealed through shared images, the control interface suggests a system designed for managing critical operations such as water level regulation, pressure control, and turbidity monitoring. The accessed interface also showed advanced tools for monitoring and controlling various parameters tied to the facility's hydroelectric operations.

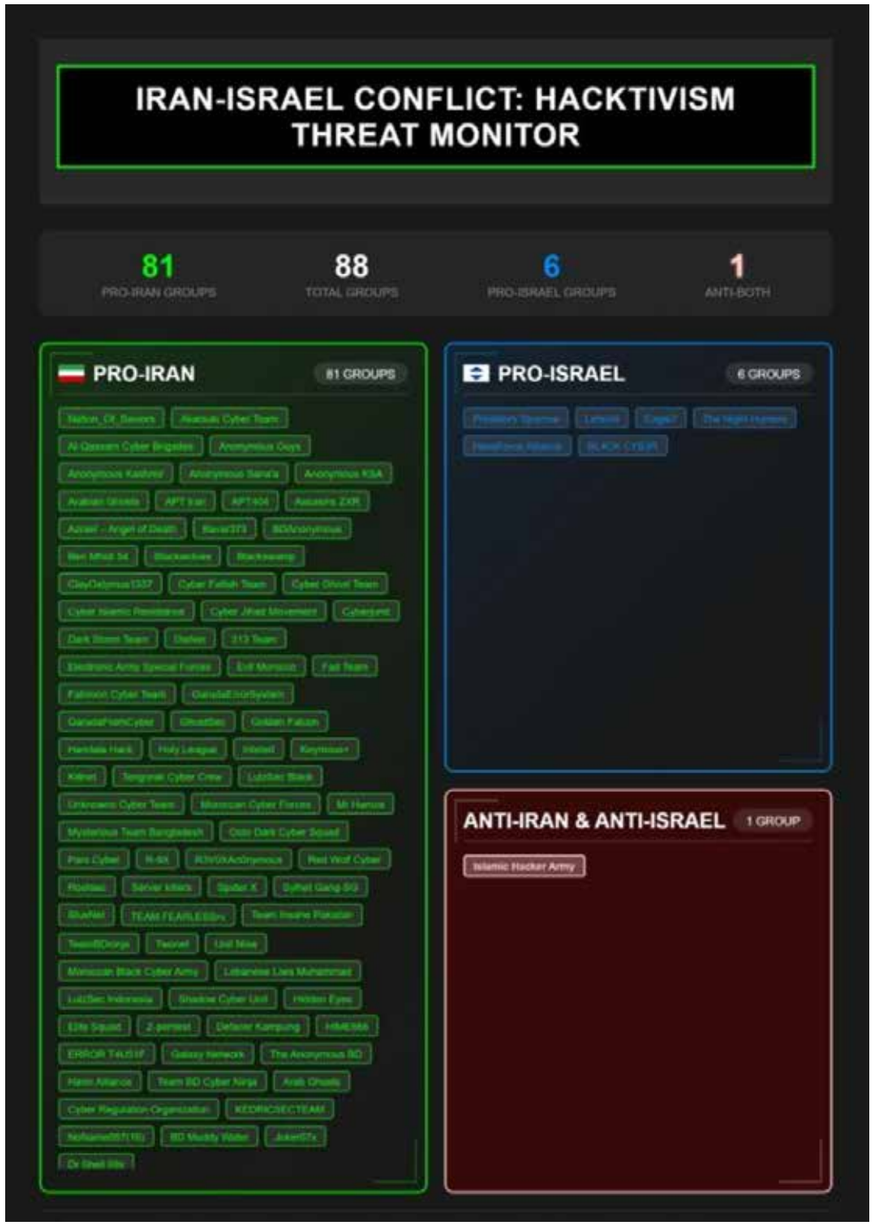
Pro-Palestinian hacktivist group **Golden Falcon Team** claimed unauthorized access to the AuditEAU system, an application developed by Fondation Rivières for monitoring municipal wastewater sanitation works in France, belonging to an unnamed client. The group released screenshots indicating alleged access to the system. The compromised interface controls metrics such as pH levels, temperature, conductivity, and water distribution processes, which are essential for managing wastewater treatment and public sanitation operations. The identity of the affected client and the location were not shared by the hacktivist group.

Golden Falcon also claimed unauthorized access to fuel station management software and a fuel station retail management system. These platforms are deployed across the fuel retailing and petroleum distribution sectors, including fuel stations, depots, and fleet fueling sites. Screenshots shared by the group appeared to indicate access to a real-time panel of an undisclosed location and the threat group navigating across various tabs and settings in the panel. It is notable that several panels are exposed over the internet and hacktivists tend to gain illicit access to them by use of default credentials or brute forcing.

## Hacktivists Turn to Ransomware, Extortion

The list of hacktivist groups embracing ransomware as a tool for ideological disruption is also growing – and played a significant role in the Iran-Israel conflict too.

Cyble documented 88 hacktivist groups active in the Iran-Israel conflict, the vast majority aligned with Iran (image below).




Of the scores of active groups and cyberattacks observed in the conflict, the **Handala** group appears to have been one of the more effective attackers, with at least 15 claims of ransomware/extortion incidents, and data samples offered as evidence in most of those alleged attacks. All of the group's victims have been based in Israel.

Russia-linked groups were mainly absent from the Iran-Israel cyber conflict, although Z-Pentest claimed to have compromised an industrial control system (ICS) at an Israeli energy and utilities target, and **NoName057(16)** claimed a DDoS attack on an Israeli transportation organization.

Ukraine-aligned group **BO Team** conducted a ransomware attack on a Russian industrial manufacturer allegedly linked to the Ministry of Defense. The operation encrypted over 1,000 hosts and 300TB of data, culminating in a $50,000 Bitcoin ransom payment. The incident highlights the growing overlap between hacktivist motivation and cybercriminal methodology.

The pro-Ukrainian hacktivist group known as **C.A.S.** carried out a coordinated cyber operation against a Russian technology firm. The attackers claim to have exfiltrated approximately 3 terabytes of internal corporate data, including source code, accounting records, employee documents, and internal network documentation. The group reported that they partially destroyed the company's infrastructure, targeting Windows and Linux Mint workstations, database servers, development environments, and backup systems.

The **Ukrainian Cyber Alliance** (UCA) claimed responsibility for a cyberattack on Carmoney, an entity specializing in secured loans and reportedly linked to Lyudmila Putina, the ex-wife of Russian President Vladimir Putin. According to UCA, the attack resulted in the destruction of Carmoney's infrastructure, including virtual machines and terabytes of data. UCA also reported the acquisition of sensitive borrower data, which allegedly includes information connected to various Russian military units, the GRU, and the FSB. Notably, the data is said to involve employees from the 16th FSB Center, known for its cyber activities under the aliases "Energetic Bear" and "Dragonfly." However, these claims regarding intelligence-related data could not be independently verified.

**Moroccan Dragons** announced the development of a proprietary ransomware program named M-DragonsWare. The statement was shared via their Telegram channels, though no technical specifications or intended deployment targets were disclosed.

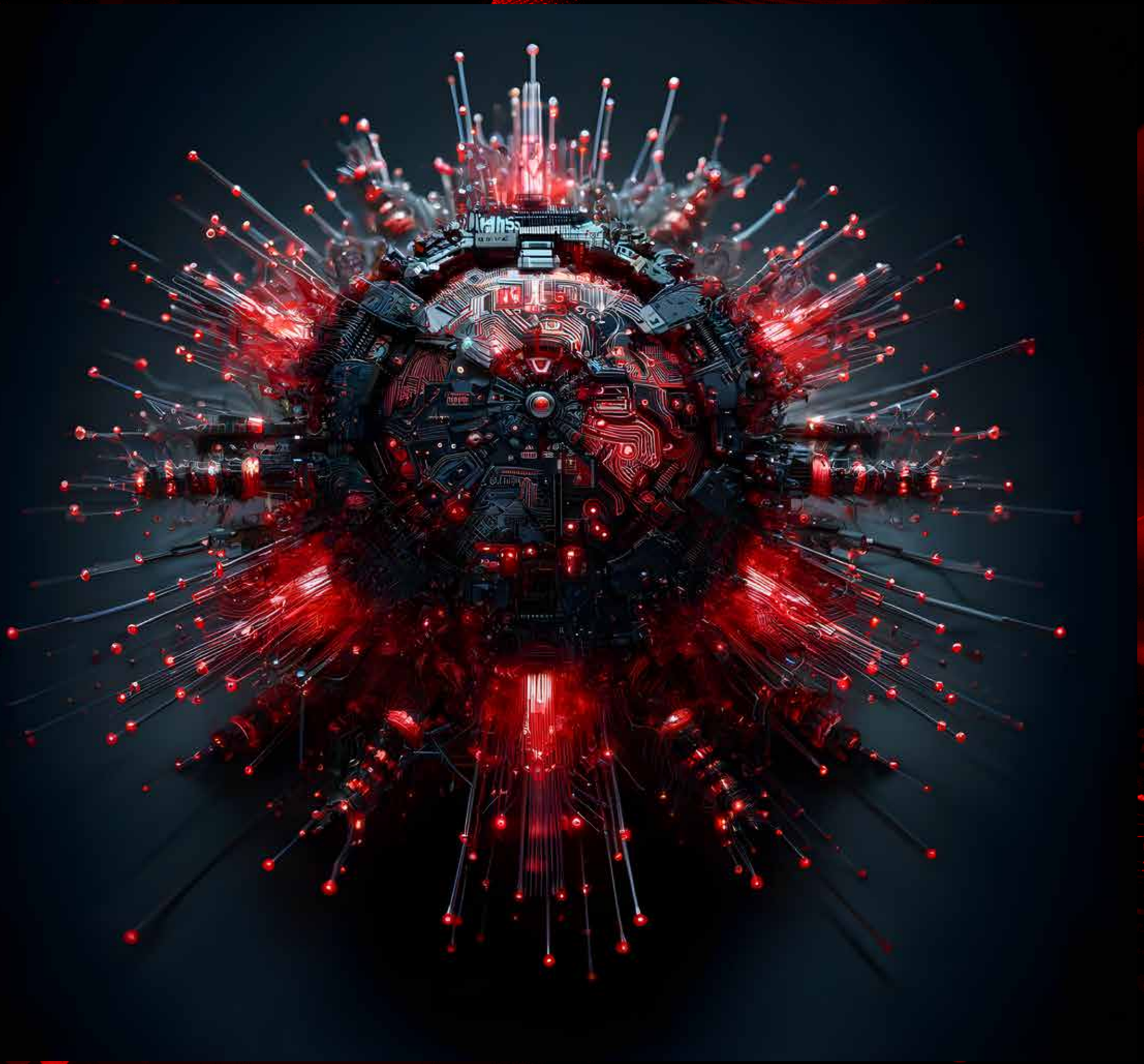
Cyble also observed several hacktivist groups engaged in more sophisticated website attacks, including SQL Injection attacks, brute forcing internet-exposed web panels to gain illicit access to data, exploiting OWASP vulnerabilities in web panels to steal data, and Dorking to discover misconfigured or internet-exposed databases. **ParanoidHax, THE ANON 69, Indohaxsec,** and **Defacer Kampung** were observed promoting data leaks on their Telegram channels.

# Conclusion

The first half of 2025 was marked by a significant increase in ransomware attacks, with an unprecedented 54% rise compared to the same period in 2024. This escalation in volume was accompanied by a notable increase in the sophistication of attacks. North America remained the most targeted region, accounting for 65% of all attacks, and the United States alone experienced 57% of the global total. The Construction and Professional Services sectors were the most targeted globally. A small number of dominant ransomware operators, namely CL0P, Akira, and Qilin, were responsible for 34% of all attacks.

Beyond ransomware, the first half of 2025 also saw other significant trends in the threat landscape. A 30% rise was observed in software supply chain attacks. Hacktivism also evolved, with groups becoming more sophisticated and targeting critical infrastructure and industrial control systems (ICS). These trends, along with the exploitation of zero-day vulnerabilities, highlight a complex and challenging environment for organizations.

In light of these findings, organizations must adopt a proactive and comprehensive approach to cybersecurity. This includes strengthening their threat intelligence capabilities, ensuring robust patching hygiene, and implementing cross-sector cyber resilience strategies to defend against the escalating and evolving threats of ransomware, supply chain attacks, and sophisticated hacktivism. The report underscores the need for continuous vigilance and adaptation to a threat landscape that is becoming more complex and interconnected.



# Industry Recognition

Cyble's capabilities are highly praised by global analysts, industry critics, and cybersecurity leaders

## Gartner

Cyble Recognized in **Three Gartner® Hype Cycle™ Reports** for the **Second Consecutive Year 2025, TechScape 2025 & More**

## FORRESTER®

Cyble has been recognized in Forrester's Q1 2025 report on Extended Threat Intelligence Service Providers (ETISPs) and in the Q2 2024 Forrester Attack Surface Management Landscape report.

## FROST & SULLIVAN


Cyble Named Leader in Frost Radar™ Cyber Threat Intelligence 2024

## Y Combinator

Cyble Recognized in Y Combinator's

**Top 100 SaaS Startups 2025**

## QKS Group

SPARK Matrix™ 2025

**LEADER**

Cyble Named as a Leader in Digital Threat Intelligence Management

Forbes BEST STARTUP EMPLOYERS 2025

Recognized as one of America's Best Startup Employers by Forbes

Global Infosec Awards NOW OPEN Cyber Defense Magazine 2025

Cyble Secures Four Prestigious Honors at the 2025 Global Infosec Awards

Gartner Peer Insights.

**Ranked No. 1** among the top Security Threat Intelligence Providers.

**4.7/5**


Cyble Named in America's Greatest Startup Workplaces 2025, By Newsweek

TOP INFOSEC INNOVATOR WINNERS Cyber Defense Magazine 2023

Named Editor's Choice for Threat Intelligence by Cyber Defense Magazine

Named a leader in the G2 Grid for Dark Web Monitoring and Threat Intelligence

**Cyble shines bright** in **G2 Summer 2025 Crowned** as a **Leader** and **High Performer across 22 categories,** and **celebrated** for the **easiest setup** and **exceptional ease of use.**

SUMMER 2025 — Grid Leader

SUMMER 2025 — Easiest To Use

SUMMER 2025 — Grid Leader ENTERPRISE

SUMMER 2025 ASIA PACIFIC — Regional Leader ENTERPRISE

SUMMER 2025 — High Performer

## OUR INVESTORS

BLACKBIRD · KING RIVER · Xoogler.co · SUMMIT PEAK INVESTMENTS · Singtel innov8 · ADITYA BIRLA Bizlabs · Y · SPIDER CAPITAL

10080 North Wolfe Road, Suite SW3-200, Cupertino, CA 95014 | contact@cyble.com | +1 888 673 2067