CYBLE®

REPORT

RANSOMWARE THREAT LANDSCAPE JAN-APRIL 2025

Table of Contents

Executive Summary

Ransomware attacks spiked 86% globally between January and April 2025, with February alone recording 848 incidents—the highest monthly count and largely driven by Cl0P, which accounted for over 28% of all activity. Known for its exploitation of zero-day vulnerabilities, Cl0P led a wave of high-impact campaigns, particularly in North America.

The United States remained the most targeted country, experiencing nearly 1,400 attacks. Construction and manufacturing sectors faced the most pressure, followed by consumer goods and logistics. APAC saw a rise in attacks fueled by geopolitical tensions, with Taiwan, India, and Singapore most affected. Europe and the U.K. continued to face sustained attacks on IT, construction, and professional services, while ransomware incidents in Australia and New Zealand doubled compared to the previous quarter.

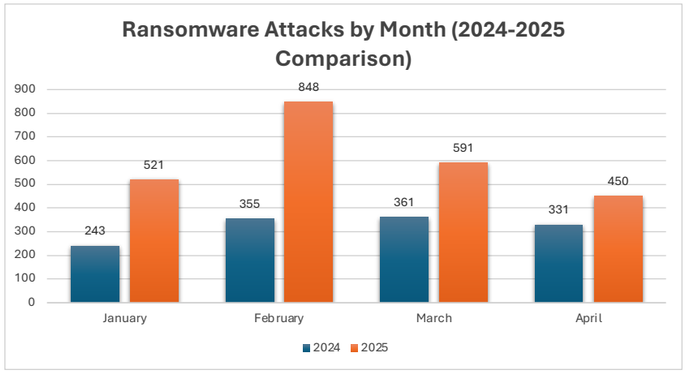
RansomHub, Akira, and Qilin were also highly active across regions, targeting IT, healthcare, and energy sectors. The Doge Big Balls campaign emerged as a standout operation—leveraging PowerShell scripts, BYOVD techniques, and psychological manipulation to evade detection and increase pressure on victims.

Threat actors exploited both new and legacy vulnerabilities, with MOVEit Transfer (CVE-2023-34362), NailaoLocker (CVE-2024-24919), and Akira-linked flaws topping the list.

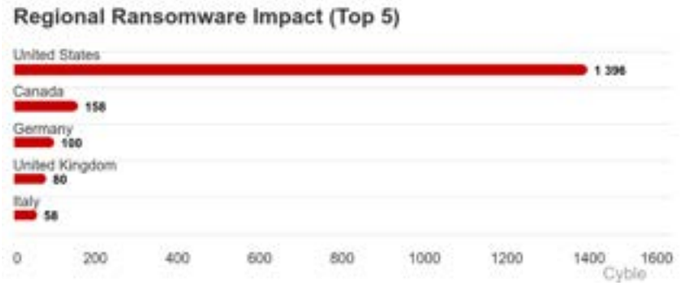
This report reinforces the need for proactive threat intelligence, patch management, and a holistic cybersecurity approach to mitigate the evolving ransomware threat landscape. Cyble remains committed to tracking these developments and providing strategic insights to help organizations stay ahead of ransomware actors.

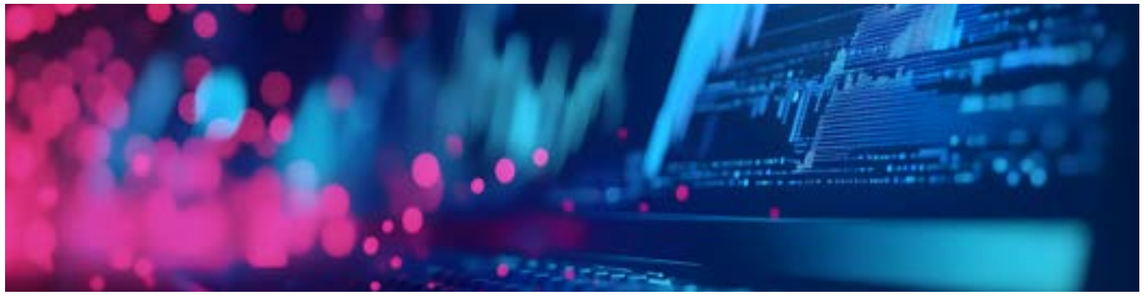
Key Statistics

86%
Ransomware attacks this year from Jan-Apr saw an 86% increase as compared to last year.



1400
U.S. remains key target with nearly 1400 ransomware incidents.

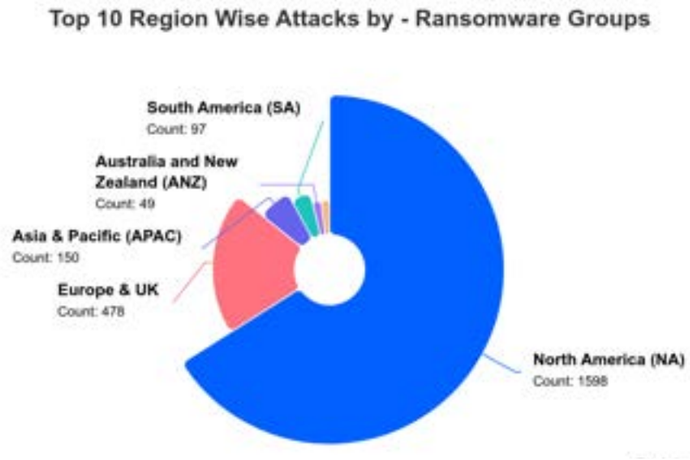


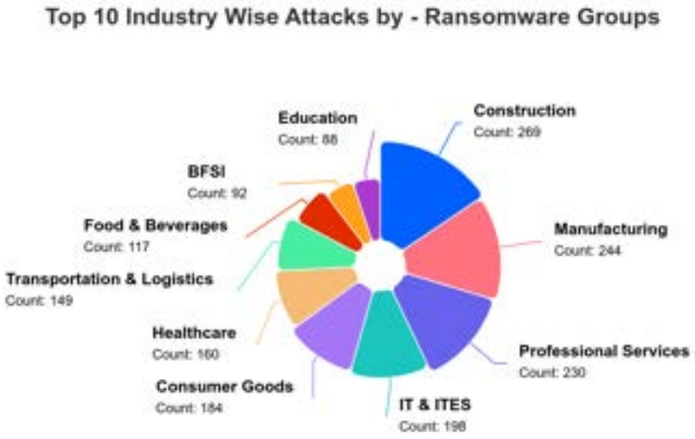


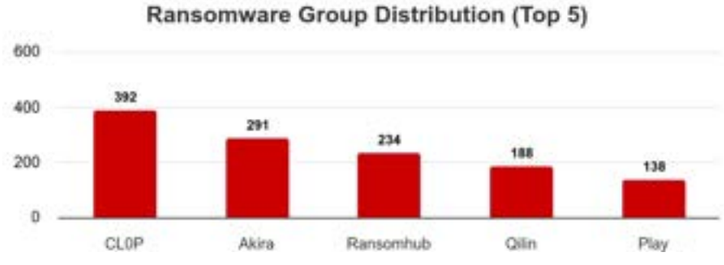
Feb.
February saw the highest number of ransomware incidents.

Construction and manufacturing
Construction and manufacturing were the most targeted sectors worldwide.

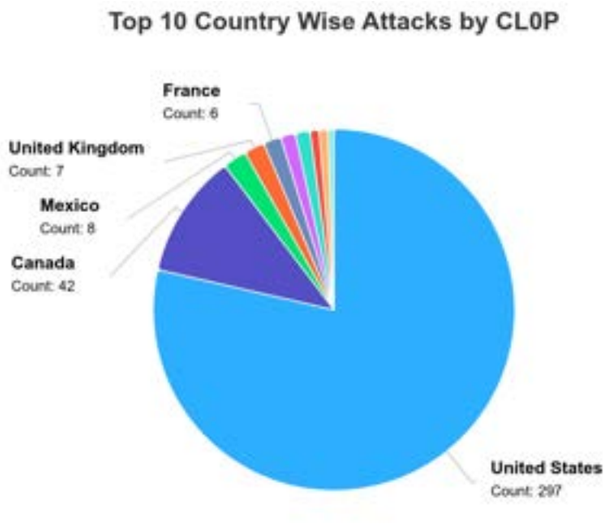
28%
CI0P accounted for more than 28% of all these ransomware incidents.



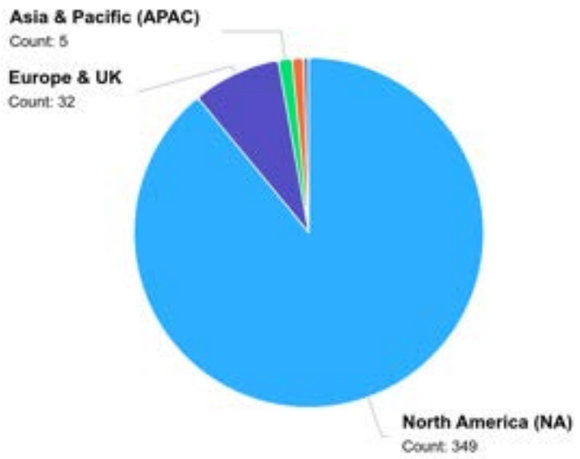




CL0P Ransomware:
The Highest Contributor with 28%



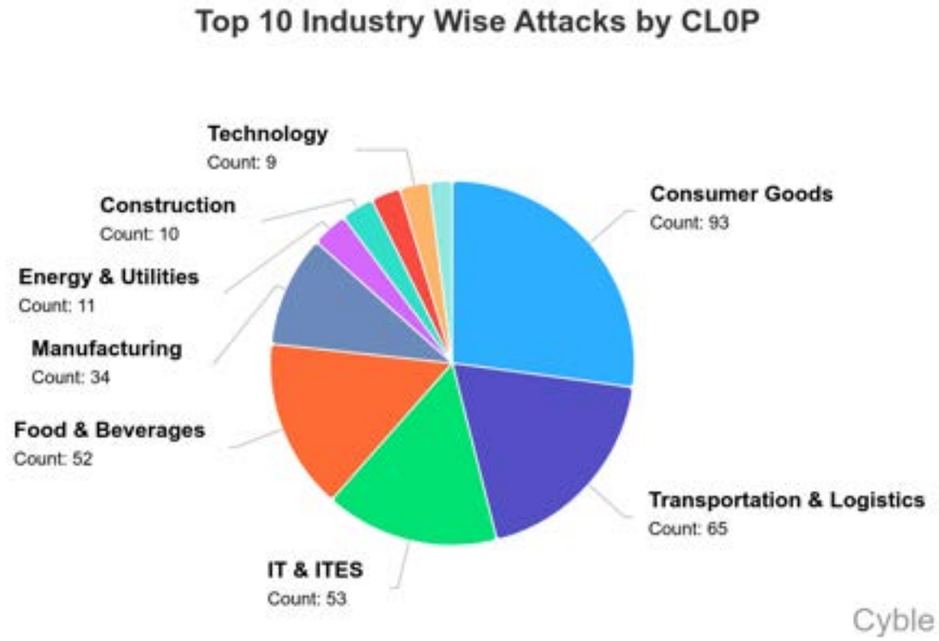
While Cl0P ransomware actors targeted organizations globally, their primary target was North America – particularly the Unites States and Canada which together accounted for 339 victims of the group. Cl0P also recorded 37% of all February ransomware attacks globally. February saw the highest number of 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.

Cl0P typically targets organizations in finance, education, healthcare, and government, often selecting victims based on their size and data value. 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.

List of

Weaponized Vulnerabilities

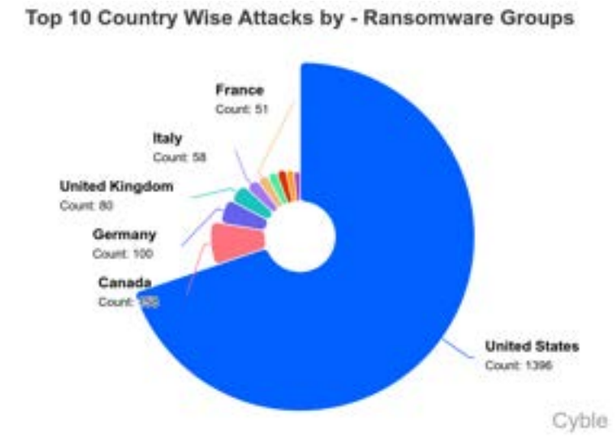
Several zero-days were exploited in this period but some of the vulnerabilities that Cyble observed where various ransomware groups exploited historical and latest flaws are listed below:

- CVE-2024-57726, CVE-2024-57727, and CVE-2024-57728 – Akira
- CVE-2018-13379, CVE-2010-2861, CVE-2009-3960, CVE-2021-34473, CVE-2021-34523, CVE-2021-31207 - Ghost (aka Cring)
- CVE-2024-24919 – NailaoLocker
- CVE-2023-22527 - LockBit (2024)
- CVE-2025-0289 – Unknown ransomware groups
- CVE-2024-55591 and CVE-2025-24472– Mora_001 (SuperBlack ransomware linked to LockBit 3.0)
- CVE-2022-24521 and CVE-2023-27532 – RansomHub
- CVE-2025-26633 - Water Gamayun

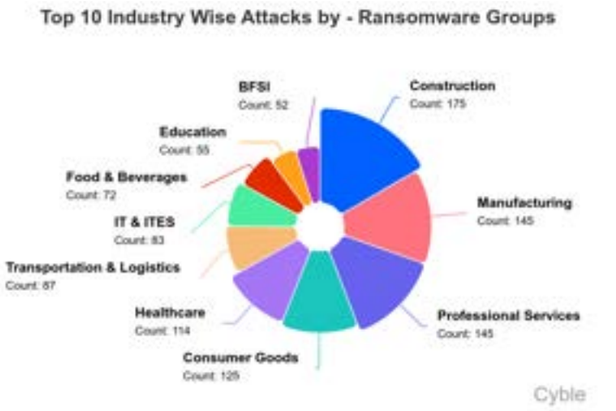
Region Wise

Ransomware Threat Landscape

United States

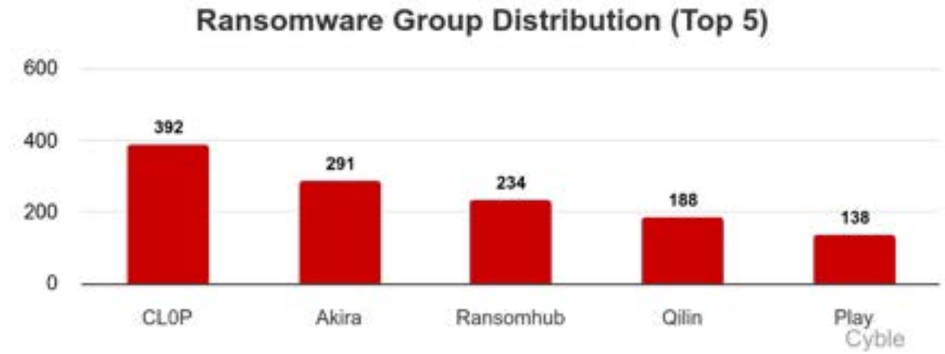


The U.S. once again led all countries in ransomware attacks, with 1396 attacks, or 58% of the global total, followed by a distant second Canada (158).



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

Following on global trends, CL0P most actively targeted organizations and businesses in the U.S. with 392 attacks under its name. Akira and RansomHub followed suit.

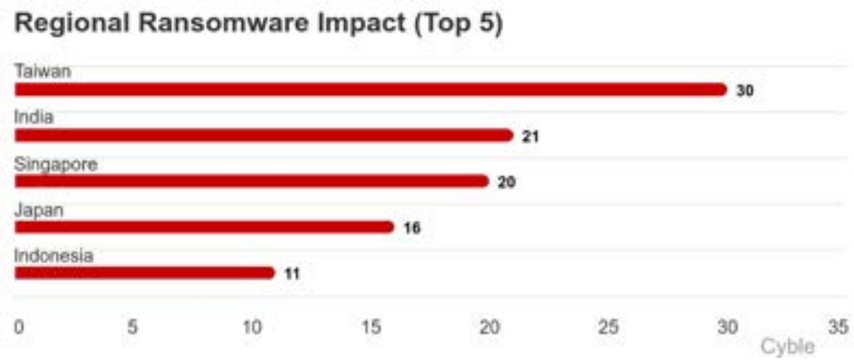


APAC

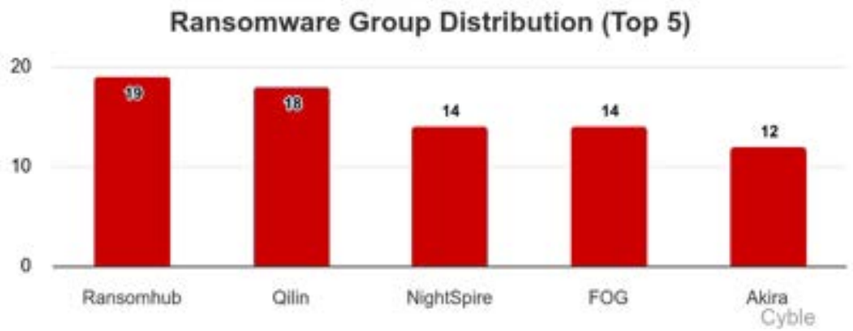
In Asia and Pacific, Taiwan was the most targeted country with 30 recorded incidents followed by India (21), Singapore (20), and Japan (16). The geopolitical tension in the South-East Asian countries seems to being leveraged by opportune ransomware actors in this region.

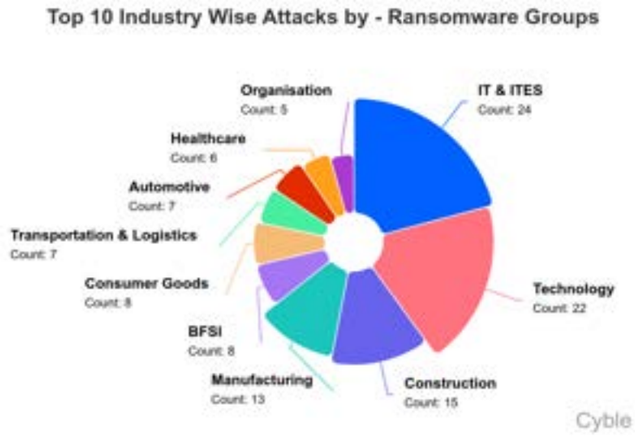
The CrazyHunter Team was the most active in Taiwan and targeted its Healthcare and Technology sectors. NightSpire, Akira and Lynx were the other actors targeting the island nation.

In India, Qilin, RansomHub and Cl0P were the most active actors with IT and Manufacturing being the prime target sectors.



RansomHub was the most prolific threat actor in this region with 19 attacks and most of them were targeted at India, Japan, and Thailand. It is closely followed by Qilin (18) and FOG (14). Qilin was also the most active ransomware actor in the month of 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.

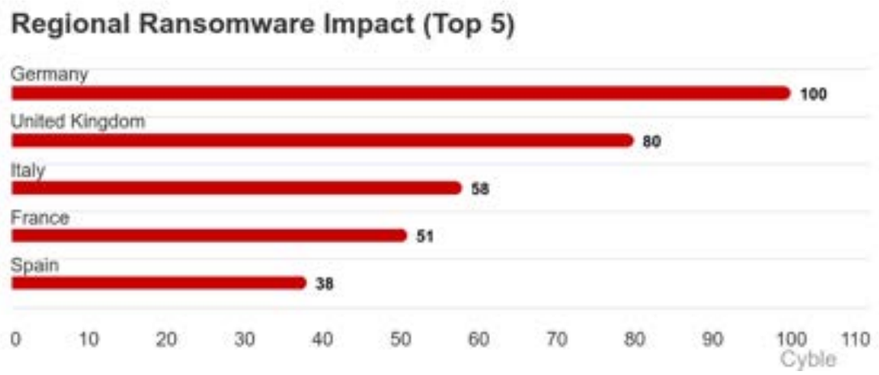
Europe and United Kingdom

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.

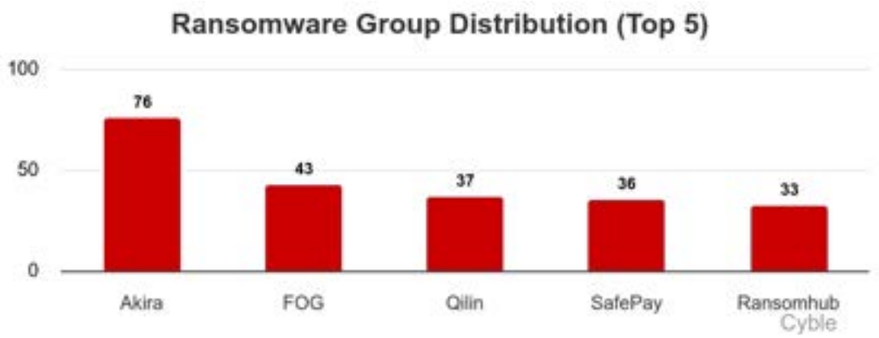
SafePay ransomware actor was the most active in Germany with one in every four attacks attributed to this ransomware group. Their primary targets: Construction and Professional Services. Germany being an automotive hub, this sector was also on the target list of several ransomware actors.

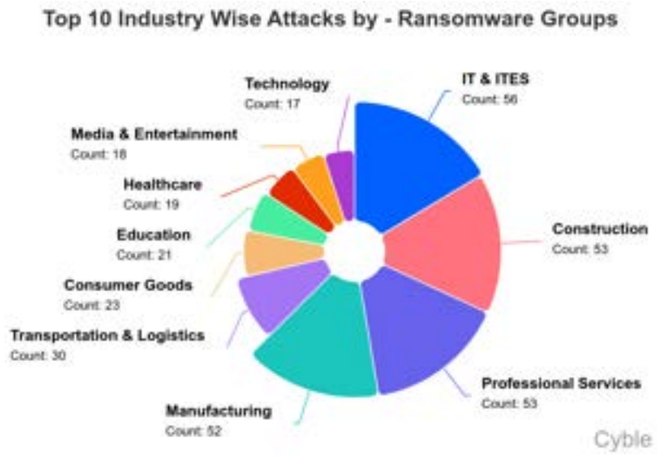
In the United Kingdom, Medusa and RansomHub were the most prolific ransomware actors who targeted Professional Services, Construction and Manufacturing services. Other notable sectors that saw targeted attacks in U.K. were Healthcare, BFSI and Media and Entertainment.

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



Akira was the most active ransomware group in the region with 76 attacks that were primarily targeted at the Construction sector.



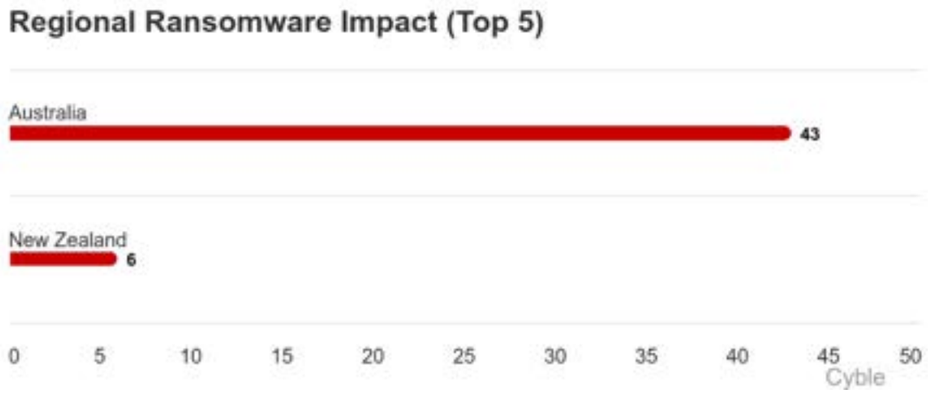


Overall, the IT & ITES and Construction and Professional Services sectors were the most targeted in Europe and the U.K.

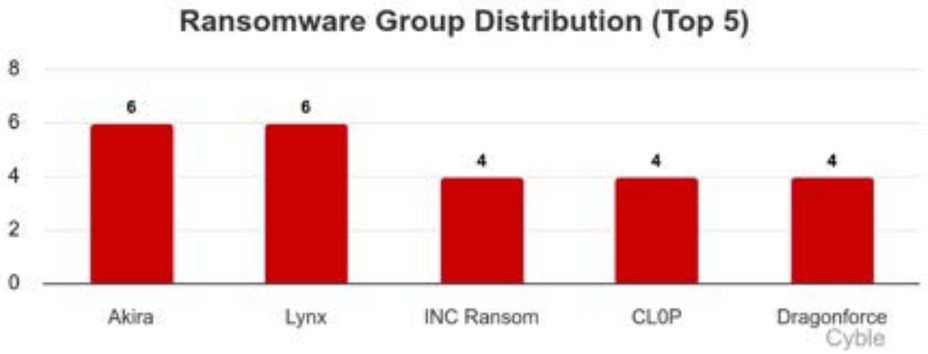
The transport sector in the region has also been under severe pressure since the last quarter. A cyberattack on the city's transportation in London, had resulted in a severe impact on its online ticketing system for weeks. Apparently, a 17-year-old teenager was behind the attack who siphoned some customer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

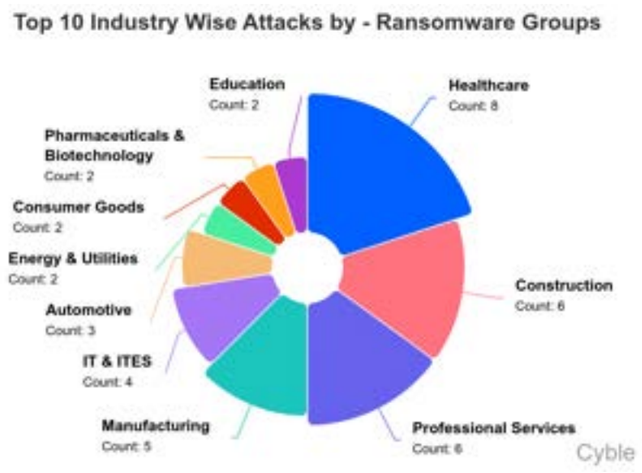
Australia and New Zealand (ANZ)

The ransomware threats down under doubled in the first four months of this year as compared to the last quarter which saw 26 ransomware incidents in Australia and just 3 in the Kiwi land.



While Sarcoma and Safepay were the prominent active threat actors in the region last quarter, Akira, Lynx and INC Ransom actors dominated the region this year. In New Zealand, DragonForce actor was a force to reckon with as 33% of the attacks were attributed to this actor.

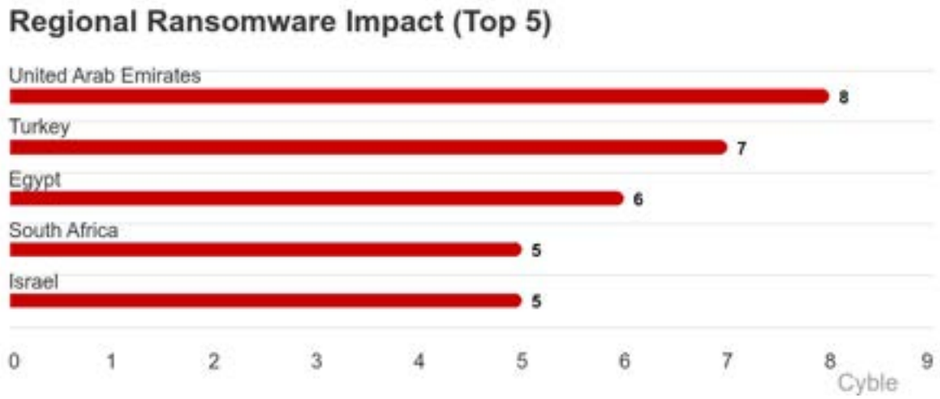




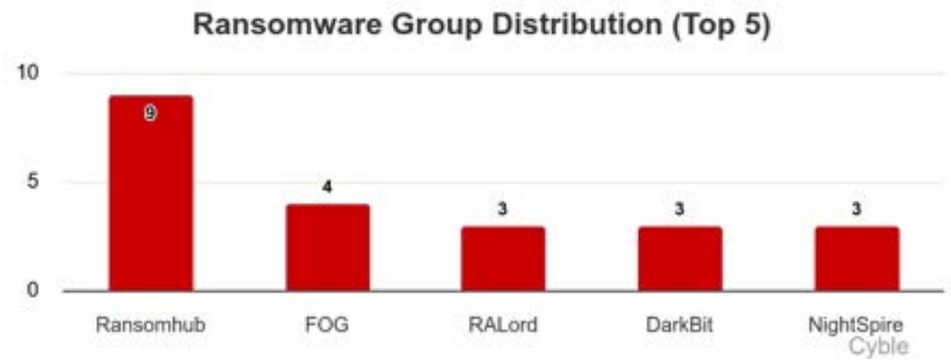
While Akira concentrated on the targeting of the Manufacturing sector, Healthcare remained the primary target, followed by Construction and Professional Services.

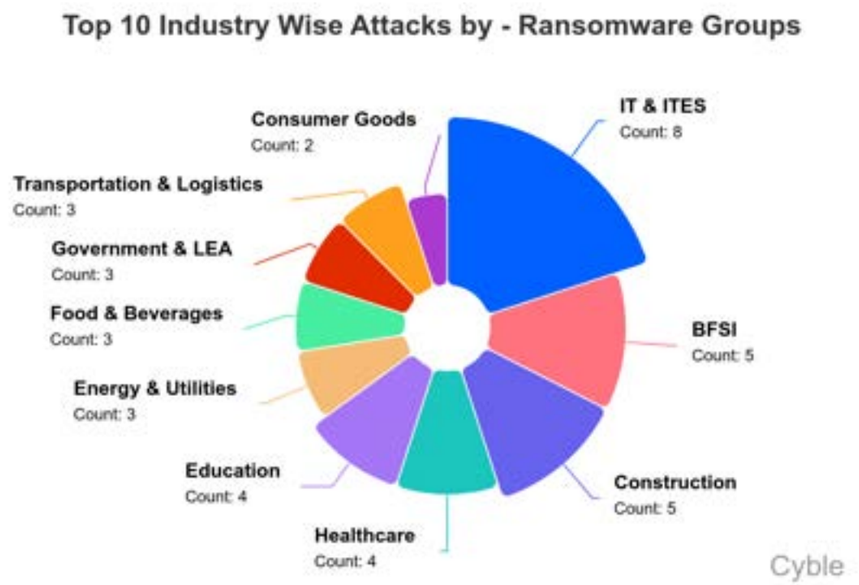
Middle East and Africa

UAE was the most targeted in the Middle East while South Africa remained the focus of ransomware actors in Africa.



There was no frontrunner as the primary threat actor in the UAE. All actors including Lynx Medusa, RansomHub and CL0P targeted the region equally with one attack each. However, when it came to the entire MEA region, RansomHub was the most active of them all with nearly double the number of attacks as compared to its closest competitor.





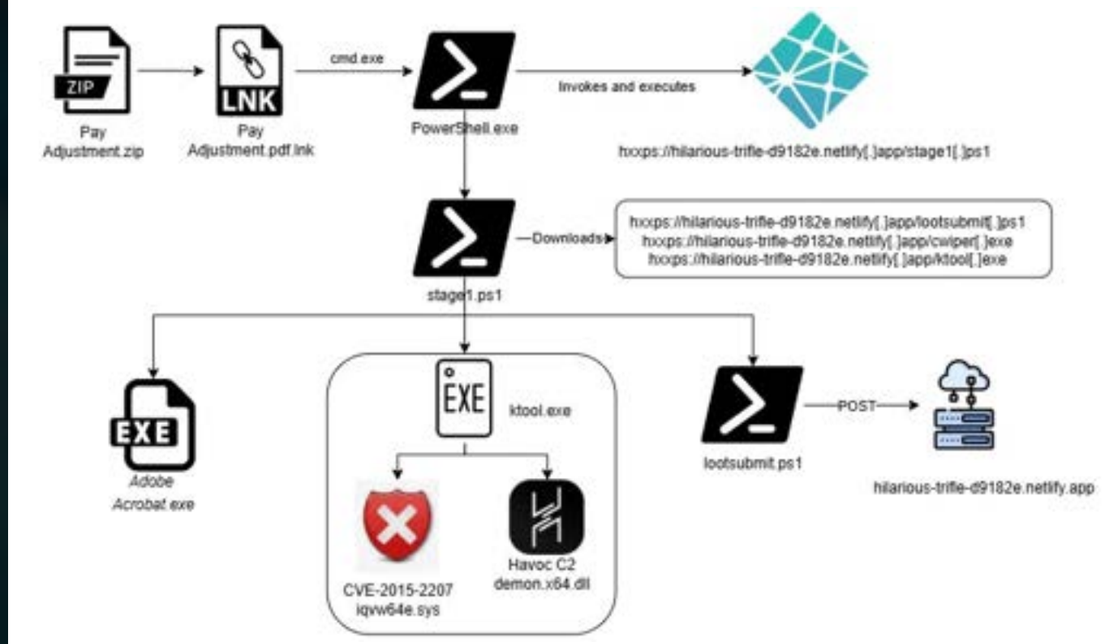
As UAE sees rapid development owing to the policies for growth, ransomware actors continued to focus on the Construction and Energy & Utilities sectors of the Emirates. But overall, the IT landscape is one of the fastest evolving in the region which remained the prime focal point of ransomware actors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

Doge Big Balls Ransomware Campaign:

Technical Summary

During the reporting period, Cyble Research and Intelligence Labs (CRIL) also analyzed a targeted ransomware campaign dubbed **"Doge Big Balls,"** linked to an individual named Edward Coristine. This operation showcases a technically sophisticated multi-stage infection chain, leveraging social engineering, privilege escalation, and evasion techniques, along with psychological manipulation to intimidate victims.

Infection Chain Overview:



Doge Big Balls ransomware campaign infection chain. (Source: CRIL)

1. **Initial Access:** The campaign begins with a malicious .LNK file that executes PowerShell commands to retrieve and run a script (stage1.ps1) from a Netlify-hosted URL.

2. **Privilege Check & Execution:** The script checks for administrator privileges. If present, it creates a hidden folder in the system startup directory and downloads a disguised Fog ransomware binary (cwiper.exe) and a kernel exploit tool (ktool.exe).

3. **Privilege Escalation (BYOVD):** Using the vulnerable iqvw64e.sys driver (CVE-2015-2291), ktool.exe elevates the ransomware process to SYSTEM privileges.

4. **Information Gathering:** A secondary script (lootsubmit.ps1) is executed to collect extensive system and network information, including BIOS serials, disk/CPU info, UUIDs, MAC/IP addresses, RAM, and OS details.

5. **Payload Execution:** The customized Fog ransomware encrypts files (adding the .flocked extension), deletes shadow copies, and drops a ransom note (readme.txt) in each directory.

6. **Ransom Demand:** The note claims authorship by Edward Coristine and demands payment of 4.721373 Monero (~$1,000) via a Monero wallet, threatening harsh consequences and offering a Tor-based chat link for negotiation.

Notable Characteristics:

- **Psychological Manipulation:** The PowerShell scripts include references to conspiracy theories and unrelated content, likely to confuse analysts and unsettle victims.

- **Evasion Techniques:** The campaign employs execution guardrails, such as checks for specific environment variables and PowerShell logs, alongside BYOVD for stealth and persistence.

- **Reputation Targeting:** The operation appears designed to malign Edward Coristine—a developer allegedly associated with Elon Musk's DOGE initiative—by falsely attributing the attack to him.

This campaign demonstrates the convergence of advanced persistence mechanisms with reputational smearing and misinformation, raising concerns about the increasingly multidimensional nature of ransomware threats.

For additional technical details on this new ransomware variant, read the blogpost here.

Industry Recognition

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

Gartner

Cyble Recognized in Gartner® Emerging Tech Report and Named a Sample Vendor in Three Gartner® Hype Cycle™ Reports: Managed IT Services 2024 and Cyber Risk Management 2024.

FROST & SULLIVAN

Cyble Named Leader in Frost Radar™ Cyber Threat Intelligence 2024

Y Combinator

Ranked in Y Combinator's Top 100 AI Startups for 2024

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.

QKS Group

SPARK Matrix™ 2025

LEADER

Cyble Named as a Leader in Digital Threat Intelligence Management

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

Earned nine awards at the Global InfoSec Awards during RSA

Gartner Peer Insights

Ranked among top 5 cyber threat intelligence providers

4.7/5

G2

Named a leader in the G2 Grid for Dark Web Monitoring

AMERICA'S BEST STARTUP EMPLOYERS Forbes 2024

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

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

Cyble shines bright in **G2 Spring 2025 Crowned** as a **Leader** and **High Performer across 16 categories,** and **celebrated** for the **easiest setup** and **exceptional ease of use.**

OUR INVESTORS

BLACKBIRD · KING RIVER · Xoogler.co · SUMMIT PEAK · 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