CMC TELECOM
Aspire to Inspire the Digital World

# RANSOMWARE TRENDS REPORT Q3 | 2024

*with comparison Q2 | 2024*

CMC TELECOM
Aspire to Inspire the Digital World

# Executive Summary

Our Ransomware Trends Report is a comprehensive retrospective report on cybercrime activity worldwide. The report includes various sections with statistics on the size of the ransomware attack by industries, countries, ransomware groups, and company sizes. We aim to help security leaders infer the size trends of companies targeted in the ransomware sector and understand the scale of data for which threat actors have planned their attacks based on over 1218 studied incidents.

This report covers the recorded attacks in the 3rd quarter of 2024 and compares them to the 2nd quarter of 2024. CMC Telecom Cyber Threat Intelligence Team (CyberTI - CMC Telecom) Cyber tracked 58 active threat groups in July, August and September 2024. Along side current statistics, significant news stories about ransomware attacks in the past three months have been compiled and included in the report to refresh the reader's memory.

Our analysts have identified staggering ransomware incidents across 27 industry subsectors with devastating consequences. The statistical distribution of these events shows that 20.5% of them were related to Manufacturing, while 14.9% of the events were in the Business Services. Additionally, 11.6% of the events were related to the Retail sector.

The report also provides insights into various ransomware groups' tactics and techniques during attacks regarding vulnerabilities. Overall, our Ransomware Trends Report provides valuable information for security leaders to understand current trends in ransomware attacks and take proactive measures to protect their organizations from future threats.

***Sincerely,***
***CyberTI - CMC Telecom***

**1218**
VICTIMS

**80**
COUNTRY

**27**
INDUSTRY

**58**
RANSOMWARE GROUP

# Methodology

CMC Telecom analysts have identified a staggering number of ransomware incidents in the third quarter of 2024, surfacing across the deep and dark web. They meticulously collected valuable details, including the organizations targeted, the countries impacted, the specific data stolen during the attacks, and the ransom payouts demanded. These details have been compiled into a comprehensive retrospective report that encapsulates the global cybercrime activity during this period.

In preparing this report, the primary focus has been on meticulously analyzing the attacks carried out by various cybercriminal groups, which have been under close surveillance by our analysts from July to September. Within this scope, an attempt has been made to meticulously derive the 3 month trends of the attacking groups, taking into account various factors such as the countries targeted, the industries affected, the ransom amounts demanded, and the annual revenue of the targeted companies.

Additionally, to provide a comparative perspective, statistics from the RTR2024-Q2 report have been utilized, allowing for a detailed analysis of thetrends in the third quarter of 2024 compared to the previous quarter.

Furthermore, alongside the current statistics, the report also compiles significant news stories about ransomware attacks that have occurred in the pastthree months. This section aims torefresh the reader's memory and provide a narrative context to the raw datapresented. By gathering the most compelling and noteworthy news stories, wehope to offer industry leaders insightfuland visionary perspectives that will aidin understanding the broader implications of these cyber incidents and assist inshaping their strategic responses to thee volving cyber threat landscape

CMC TELECOM
Aspire to Inspire the Digital World

# Key Insights

- Ransomware attacks in Q3 2024 were marked by a fragmented threat landscape, with smaller actors comprising44.1% of attacks, while major players like RansomHub(16%) led, highlighting the increasing need for diverse andregion-specific cybersecurity strategies.

- In Q3 2024, ransomware attacks were highly concentratedin the U.S. (54.2%), but smaller and developing countries, represented by the 22% "Other" category, also faced significant threats, underscoring the global and diverse natureof cyber vulnerabilities.

- In Q3 2024, ransomware attacks primarily targeted manufacturing (20.5%), followed by business services (14.9%) andretail (11.6%), reflecting the vulnerability of critical infrastructure, customer data, and operational continuity acrossdiverse sectors.

- In Q3 2024, ransomware attacks were predominantly focused on North America (60.3%), followed by EMEA (25.9%)and APAC (8.8%), with Latin America (5%) facing the leastbut potentially increasing threat, indicating a strong focuson developed economies.

- Sixteen members of Evil Corp were sanctioned by the UK, and their links to the Russian state were revealed. After USsanctions in 2019, the group continued its operations by developing new malware and collaborating with othercriminal groups like LockBit.

- Ruslan Magomedovich Astamirov and Mikhail Vasiliev pleaded guilty to being members of the LockBit ransomware group and conducting cyberattacks globally. The two defendants targeted numerous victims between2020-2024, extorting millions of dollars in ransom.

- Cencora, a major U.S. pharmaceutical distributor, paid arecord $75 million ransom in Bitcoin following a ransomware attack by the Dark Angels group, which initiallydemanded $150 million. This marks the largest known ransomware payment, highlighting the growing threat andfinancial impact of cybercrime.

- Following the takedown of the Qakbot botnet, BlackBasta has adapted its strategy by developing custommalware and using new tools like "SilentNight" and "Cogscan" for rapid ransomware deployment. This shift highlights the group's increasing complexity and speed in carrying out attacks, moving away from traditional phishingmethods.

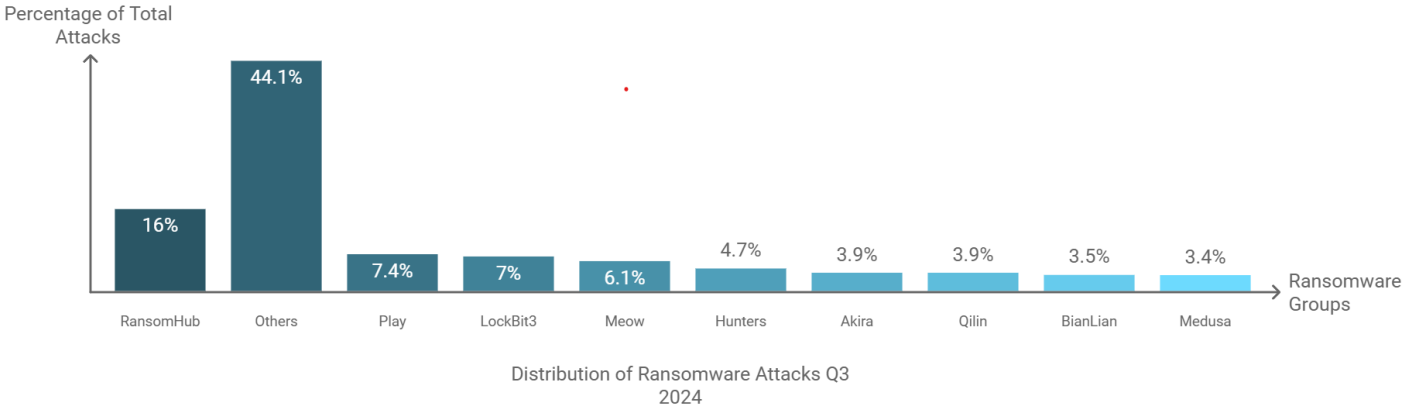
CMC TELECOM
Aspire to Inspire the Digital World

# Statistics on Ransomware Attacks

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

CMC TELECOM
Aspire to Inspire the Digital World

# Ransomware Attack Distributions by Group: Q3/2024




Distribution of Ransomware Attacks Q3 2024

The global distribution of ransomware attacksin the third quarter of 2024 revealed thatmany small actors are increasingly making their presence felt. The "Others" category, representing 44.1% of attacks, consists of a varietyof smaller groups, highlighting the diverse and fragmented nature of ransomware threats.

The leading ransomware group was RansomHub, responsible for 16% of all attacks, making it the largest individual actor. Following closely were Play with 7.4% and LockBit3 with 7%. The Meow group continued its activities, accounting for 6.1% of the attacks, while Hunters posed a significant threat at 4.7%. Additionally, both Akira and Qilin were active players, each contributing 3.9% of the total attacks. Moreover, BianLian and Medusa were responsible for 3.5% and 3.4% of the attacks, respectively. This diversity complicates defense strategies, as each group employs differenttactics, techniques, and procedures (TTPs).

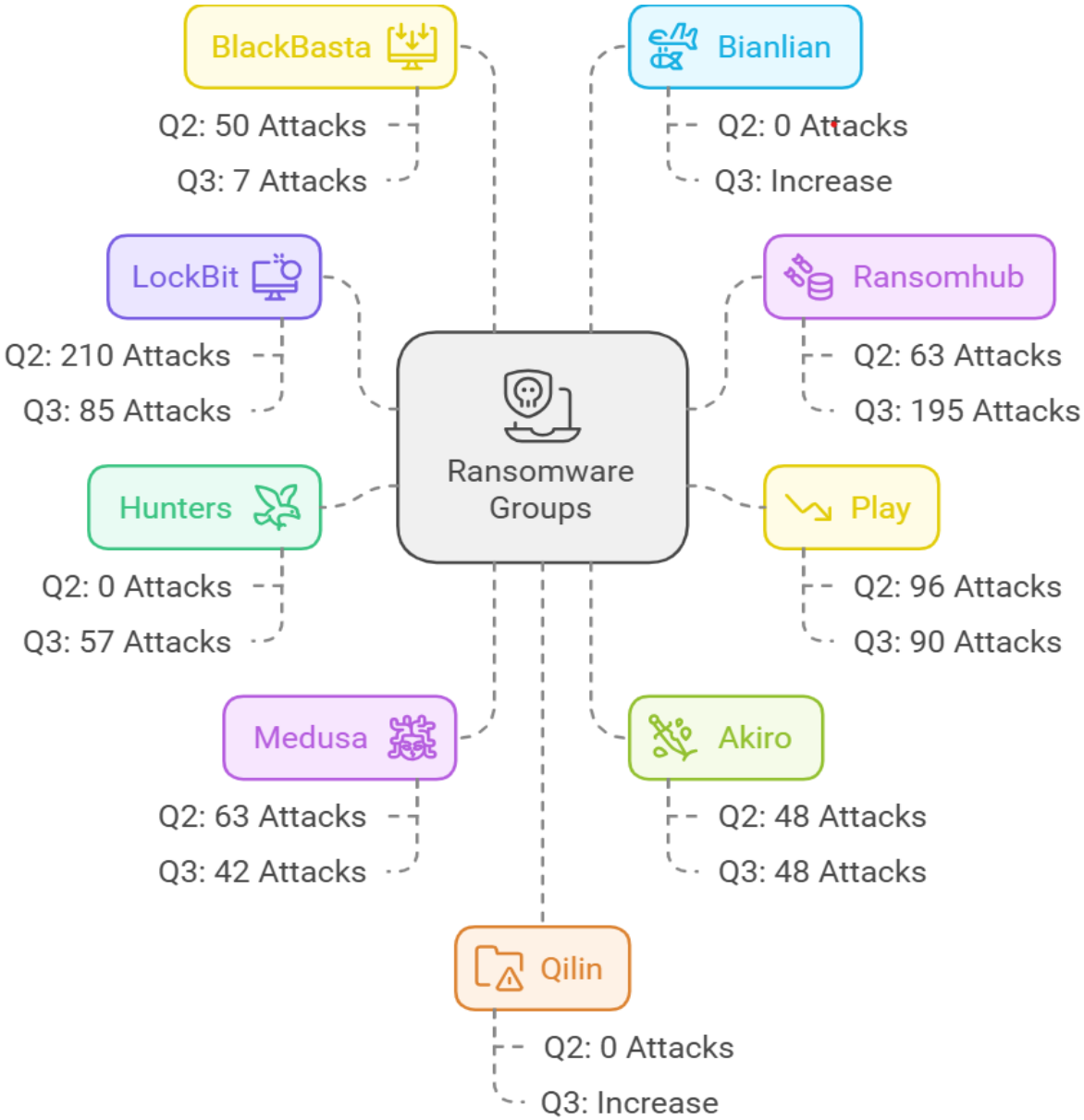
During this period, the most targeted regionswere the Americas, Europe, and the Asia Pacific. Countries such as the United States, the United Kingdom, Canada, and Germany were significantly affected, underscoring the need for regional cybersecurity strategies and stronger defense mechanisms. The ransomware eco system must develop more resilient and faster response solutions to keep up with the everevolving threats.

Top of the list

**Ransomhub, Play, LockBit**

CMC TELECOM
Aspire to Inspire the Digital World

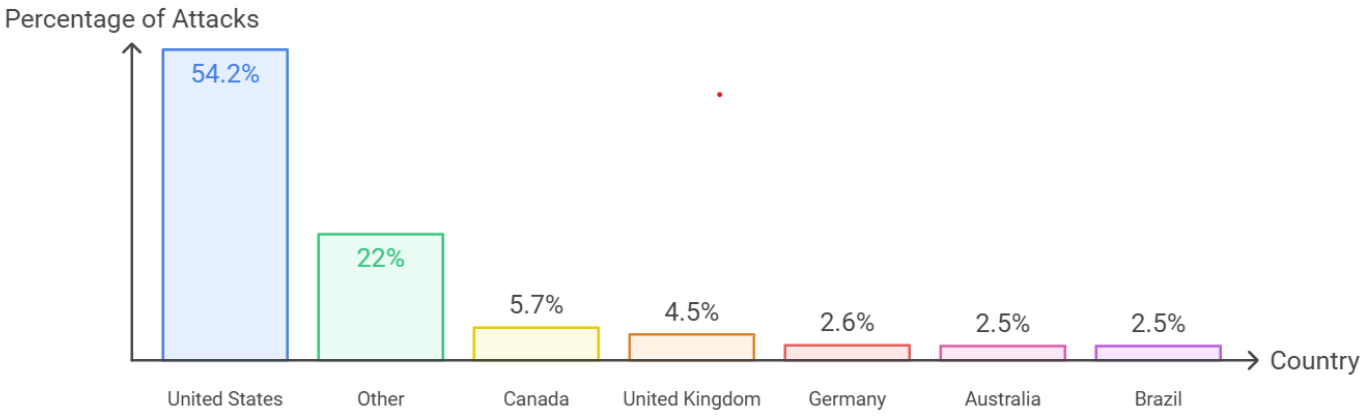
# Ransomware Attacks Comparison Across Group: Q2/2024 - Q3/2024




This chart compares ransomware attacks between Q2/2024 and Q3/2024. **LockBit**, while remaining one of the leading groups in both quarters, saw a significant drop from 210 attacks in Q2 to 85 in Q3. In contrast, **Ransomhub** experienced a sharp increase, rising from 63attacks in Q2 to 195 in Q3. **The Play** group saw a slight decline, dropping from 96 attacks inQ2 to 90 in Q3. Hunters increased its activity, reaching 57 attacks in Q3, while Medusa drop-ped from 63 in Q2 to 42 in Q3. **Akira** remained stable across both quarters, with 48 attacks. **BlackBasta** saw a steep decline, falling from 50 attacks in Q2 to just 7 in Q3. Both **Bianlian** and **Qilin** showed slight increases. Overall, while some ransomware groups gained strength, others experienced noticeable declines, with large fluctuations in attack dynamics.

CMC TELECOM
Aspire to Inspire the Digital World

# Ransomware Attack Distributions by Country: Q3/2024




Distribution of Ransomware Attacks by Country Q3 2024

The chart showing the distribution of ran-somware attacks by country in the third quar-ter of 2024 clearly shows how widespreadcyber threats are on a global scale. **The United States** is the most attacked country with 54.2%. This high rate shows that the digital infrastructure and economic power of the USmakes it an attractive target for ransomwaregroups. Stronger cybersecurity measures inthis area could be critical to reducing attackrates.

Countries in the **"Other"** category rankedsecond with 22%. This shows that ransomwa-re attacks are concentrated not only in largeeconomies, but also in smaller or developingcountries. **Canada (5.7%)**, **the United King-dom (4.5%)** and **Germany (2.6%)** are undersignificant threat. Countries such as **Australia(2.5%)**, **Brazil (2.5%)**, **Italy, France** and **Spainhave** also been targeted by ransomware attacks.

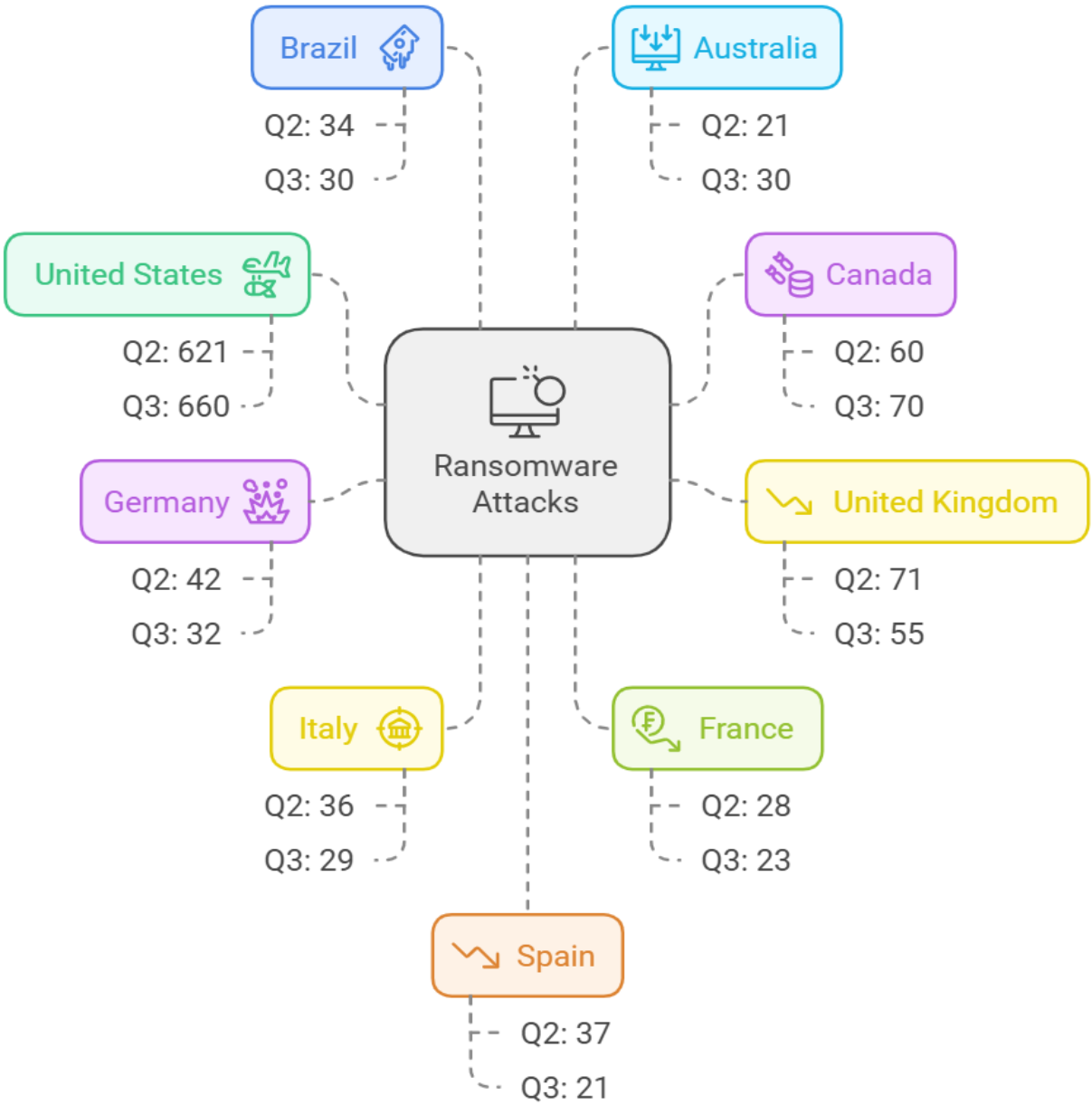
This distribution highlights that ransomwarethreats are geographically widespread andthat each country needs to strengthen itsown cyber defense strategies. In particular,the high percentage in the "Other" categoryindicates that smaller countries should alsotake more precautions against such cyberthreats. Overall, this graph reveals that globalransomware attacks are diversifying and thatevery country needs to take proactive steps toenhance its digital security.

Top of the list

**United States, Canada, United Kingdom**

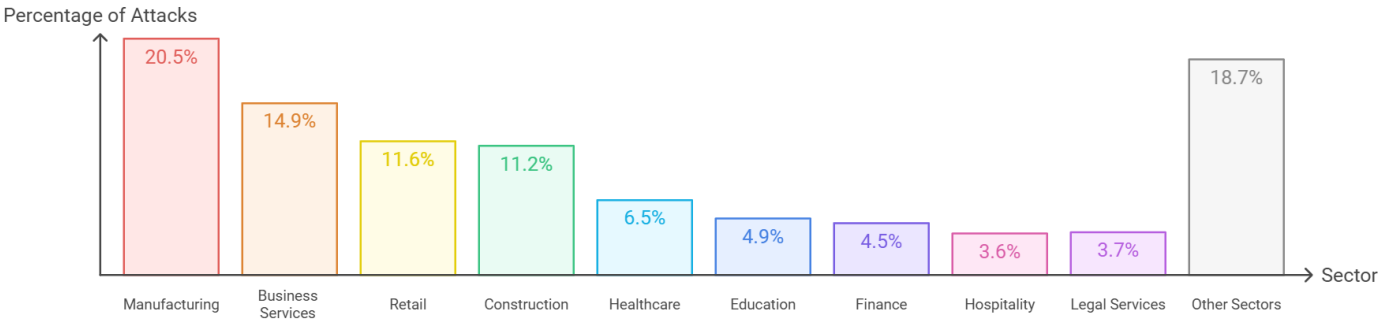
CMC TELECOM
Aspire to Inspire the Digital World

# Ransomware Attacks Comparison Across Countries: Q2/2024 - Q3/2024




The United States continues to experience the highest number of ransomware attacks,increasing from 621 in Q2 to 660 in Q3. **Canada** saw a significant rise from 60 to 70 attacks,while **the UK** dropped from 71 to 55 attacks. **Germany** and **Italy** witnessed declines, with **Germany** falling from 42 to 32 and **Italy** from 36 to 29. **France** also saw a decrease from 28 to23 attacks. **Brazil** decreased from 34 to 30, while **Australia** rises from 21 to 30. **Spain's** attacksdecreased from 37 to 21, while India saw a drop from 24 to 17. Overall, ransomware attacksshifted geographically, with some regions stabilizing and others seeing reductions.

# Ransomware Attack Distributions by Sectors: Q3/2024




Ransomware Attack Distribution by Sector in Q3-2024

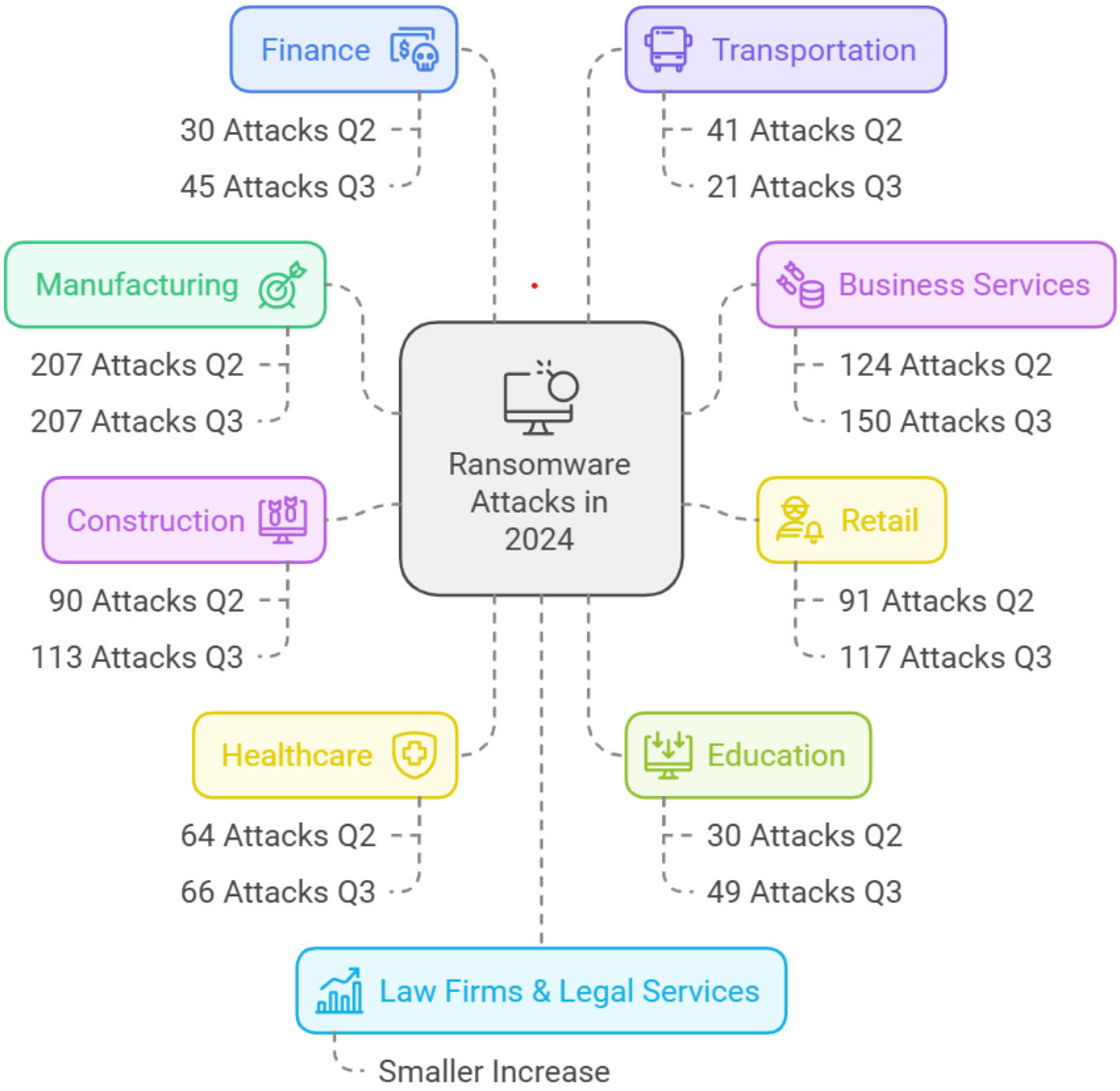
The ransomware attack distribution for Q3-2024 reveals significant threats targetingvarious sectors. The most affected sector is **Manufacturing**, which accounts for **20.5%** ofall attacks. This indicates that ransomwaregroups see the critical infrastructure of manufacturing facilities as an attractive target. Thedisruption of production processes and thecompromise of sensitive data highlight theimportance of comprehensive cybersecurity measures in this sector. In particular, operational disruptions in manufacturing can havesevere financial consequences.

**Business services** rank second with **14.9%** ofattacks. This sector continues to attract attac-kers due to its sensitivity in protecting custo-mer data. Businesses need to implementstrong security policies to ensure operationalcontinuity. **The Retail** sector is third with **11.6%** of attacks. Protecting digital infrastructureshas become critical, especially to safeguardcustomer data and payment systems. A databreach in the retail sector could erode custo-mer trust and lead to significant financiallosses.

**The Construction** sector accounts for **11.2%** ofattacks, while the Healthcare sector, with6.5%, emphasizes the importance of securingpatient data. Any disruption in the healthcaresector could directly jeopardize patient safety. **Education (4.9%), Finance (4.5%),** and **Hospi-tality (3.6%)** sectors also face notable threats. **Law firms and legal services** make **up 3.7%** ofattacks, while **other** sectors, with **18.7%**, expe-rience a broad share of attacks. This demonst-rates the diversity of ransomware targets andemphasizes that no sector is fully immunefrom these threats.

CMC TELECOM
Aspire to Inspire the Digital World

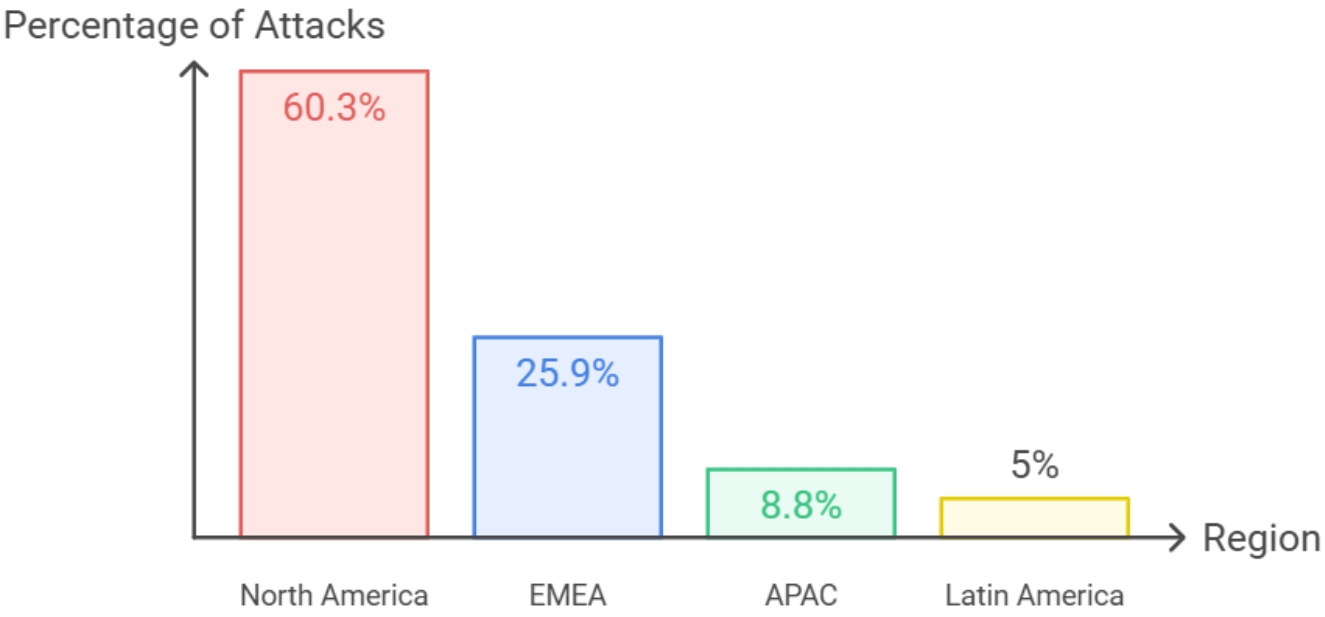
# Ransomware Attacks Comparison Across Sectors: Q2/2024- Q3/2024




In comparing ransomware attacks between Q2 and Q3 of 2024, most sectors saw increases. **Manufacturing** remained the highest-targeted sector, stable at 207 attacks in both quar-ters. **Business Services** surged from 124 to 150 attacks, while **Retail** saw a rise from 91 to 117. **Construction** also experienced growth, increasing from 90 to 113. **The Healthcare** sector sawa slight rise, from 64 to 66 attacks. **Education** had a notable jump from 30 to 49, and **Finance** spiked from 30 to 45.

Meanwhile, **Law Firms & Legal Services** and **Hospitality** saw smaller increases. **Transportation** was the only sector to see a major decrease, dropping from 41 to 21 attacks.
Overall, the data shows rising ransomware threats across most industries, with **Business Services** and Retail being the most impacted.

# Ransomware Attack Distributions by Region: Q3/2024




Regional Distribution of Ransomware Attacks Q3 2024

The chart shows the regional distribution ofransomware attacks carried out by groups inthe third quarter of 2024. According to thedonut chart, the majority of attacks targeted **North America (NA)**, accounting for 60.3% ofall incidents. This indicates that **North America** has become a major target, with ran-somware groups focusing heavily on busines-ses and individuals in this region.

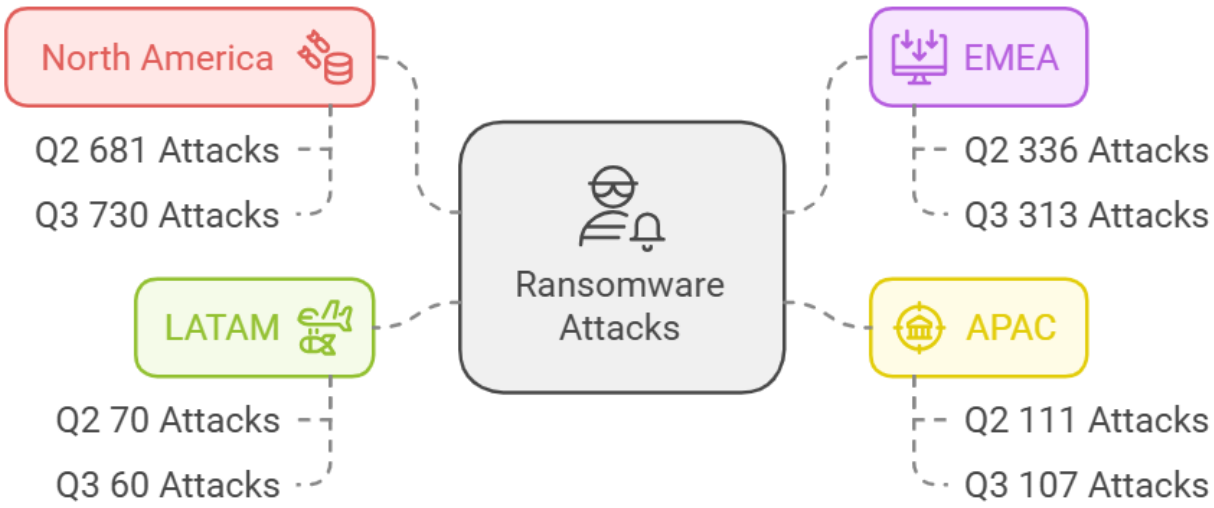
The second largest share of attacks is in the **EMEA** region **(Europe, the Middle East, and Africa)**, representing 25.9% of the attacks. **EMEA**, which includes both developed anddeveloping economies, is vulnerable to a widerange of sectors being targeted by ransomware. Large European economies are atsignificant risk from these threats.

**The APAC (Asia-Pacific)** region accounts fo r8.8% of the attacks, a lower share comparedto other regions. However, considering theeconomic strength of the region, this percen-tage is still significant. Lastly, **Latin America (LATAM)** shows the lowest attack rate at 5%.While the percentage is small, this regioncould see an upward trend due to weaker cybersecurity measures.
Overall, ransomware groups appear to beconcentrating their attacks on developedeconomies, highlighting the critical impor-tance of robust digital infrastructure in these areas.

Top of the list
NA, EMEA, LATAM

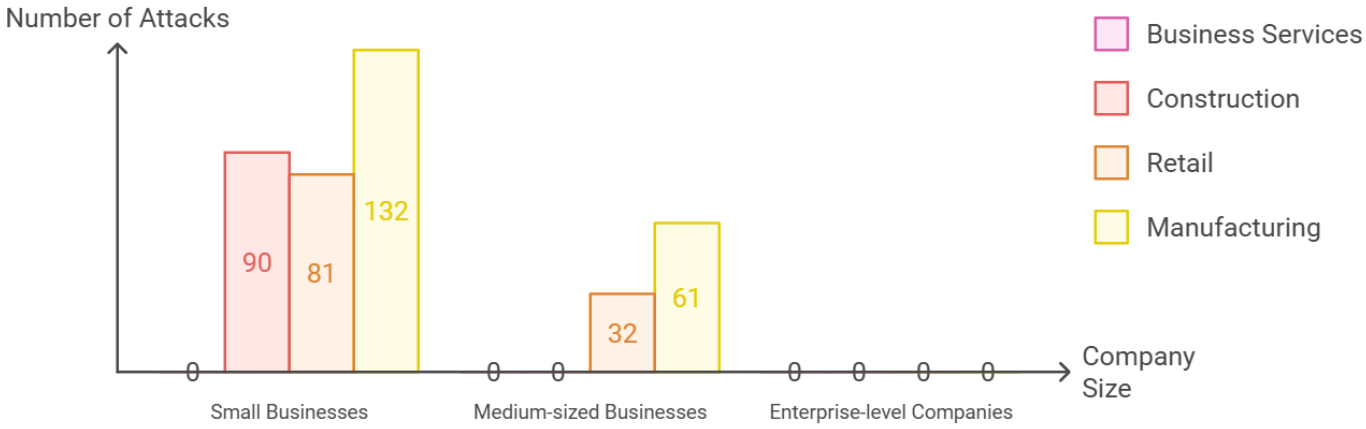
# 08

# Ransomware Attacks Comparison Across Region: Q2/2024- Q3/2024




The chart illustrates the distribution of ransomware attacks across different regions between Q2 2024 and Q3 2024. The highest number of attacks occurred in **North America (NA)**, with730 attacks in Q3, compared to 681 in Q2. This indicates an increase in ransomware activity inthe region. **EMEA (Europe, Middle East, and Africa)** follows, with 313 attacks in Q3, downslightly from 336 in Q2, showing a minor decrease. In the **APAC (Asia-Pacific)** region, thenumber of attacks is relatively lower, with 107 in Q3 and 111 in Q2. **Latin America (LATAM)** hasthe fewest attacks, with 60 in Q3 and 70 in Q2. Overall, while other regions have seen a decrease or stabilization in attack numbers, **North America** has experienced a significant rise. This suggests that ransomware groups are adopting different strategies in various regions.

# Ransomware Attack Distributions by Company Revenue: Q3/2024




Distribution of Companies Targeted by Ransomware Groups in Q3-2024

This chart illustrates the distribution of companies targeted by ransomware groups in Q3-2024, categorized by their size. The chart clearly shows that small businesses are themost targeted group. In each sector, small businesses represented by the blue color domi-nate the chart, for instance, 132 attacks in **Manufacturing**, 81 in **Retail**, and 90 in **Construction**. Medium-sized businesses are also significantly at risk, especially in the manufacturingand retail sectors, with 61 and 32 attacks, respectively. Enterprise-level companies are theleast targeted, but they still face some threats, particularly in **manufacturing** and **business services**.

These results suggest that cybercriminals frequently target small businesses, likely due totheir lower investments in cybersecurity. However, large businesses should also remainvigilant, as enterprise-level targeting persists across key industries.

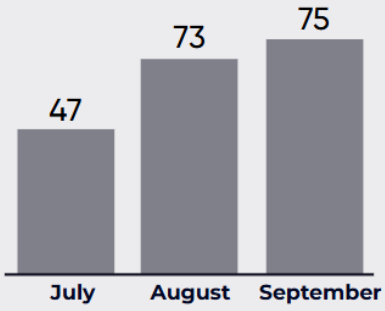
CMC TELECOM
Aspire to Inspire the Digital World

# Ransomware Groups: Q3/2024 Analysis

*Ransomware attacks in Q3 2024 were marked by a fragmented threatlandscape, with smaller actors comprising 44.1% of attacks, whilemajor players like RansomHub (16%) led, highlighting the increasingneed for diverse and region-specific cybersecurity strategies.*

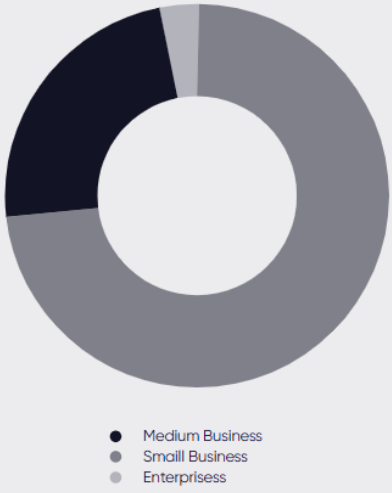
10

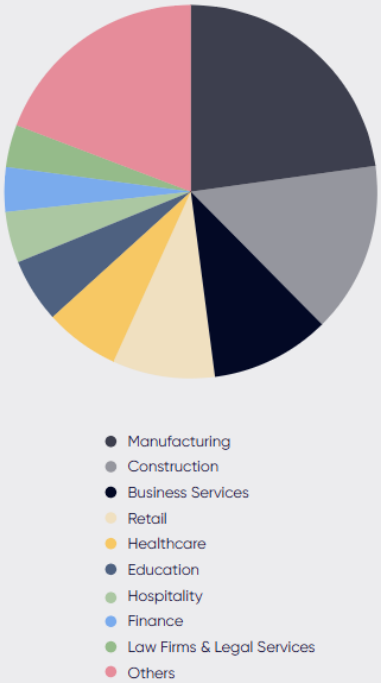
# Ransomhub




## Who is Ransomhub?

*RansomHub, a ransomware-as-a-service(RaaS) platform, has rapidly become one ofthe largest and most dangerousransomware groups in 2024. Likely anupdated version of Knight ransomware(formerly Cyclops), RansomHub hasexpanded its operations. While it sharesroots with Knight, it's unlikely the originalcreators are involved, as the Knightransomware source code was sold onunderground forums in February 2024,suggesting a change in leadership.*




Since its launch in February 2024, RansomHub hasquickly gained notoriety by attacking over 280 victims, including critical sectors like water sys-tems, IT, government services, healthcare, andemergency services. Its focus on high profileindustries has made it one of the most dangerous Ransomware-as-a-Service (RaaS) groups.

RansomHub's growth may be linked to recruitingformer affiliates from the defunct Noberus ran-somware group, including an affiliate known as Notchy. Tools associated with another Noberus affi-liate, Scattered Spider, were also used in recentattacks, increasing its impact.

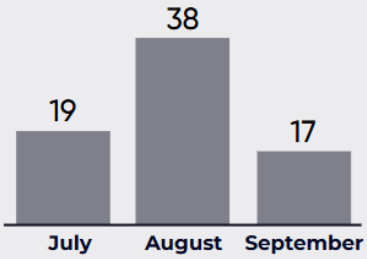
RansomHub employs double extortion tactics, encrypting data and threatening to release itunless ransoms are paid. Its ability to exploitzero-day vulnerabilities and use social engineeringallows it to bypass even strong security measures.With experienced operators and connections inthe cyber criminal underground, RansomHub hasrapidly become a major threat in 2024.

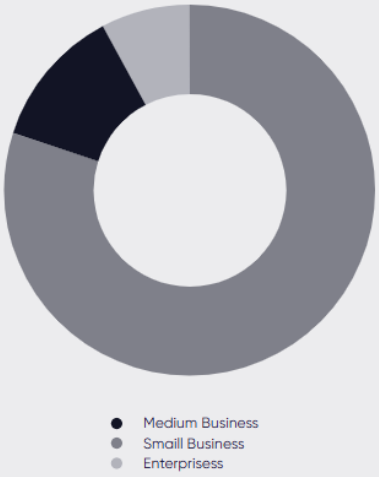
11

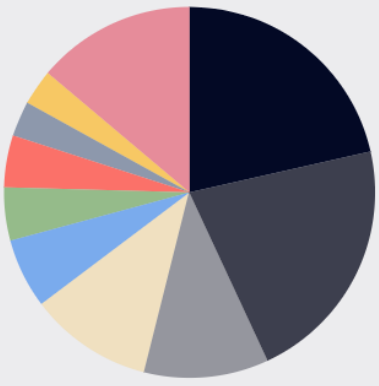
# Meow

## Who is Meow?

*Meow ransomware has gained a prominentplace among ransomware threats in 2022 and has been identified as a variant of the Conti family. While Meow continues to utilizemany of Conti's core functionality andencryption techniques, it is uniquely characterized by prominent elements such asthe phrase “MEOW! MEOW! MEOW! MEOW!” and “meowcorp2022” in its ransom notes.*



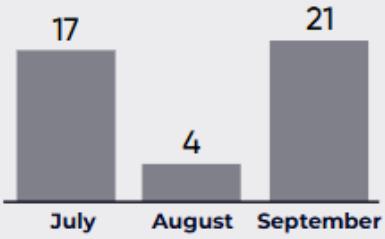



This group, which continued its attacks with 86 victims in 2024, is considered a major threat, espe-cially in ransomware operations. The Meow groupinfiltrates systems through known vulnerabilitiesand zero-day exploits, encrypts its victims' files anddemands ransom. After infecting systems, Meowencrypts files by appending the .meow extensionto them and prompts victims for payment instruc-tions via Telegram accounts meow2022 and meo-w123. The group is known to operate on a Ran-somware as a Service (RaaS) model and usuallydelivers post-encryption ransom demands viaemail or Telegram. Meow's effective operation wasdisrupted for a while by a decryption tool releasedin 2023, and some victims were able to recovertheir data. However, during this period, a groupcalled Meow Leaks emerged, and this new threat differed from Meow's previous encryption and datatheft tactics by focusing solely on data leakage.

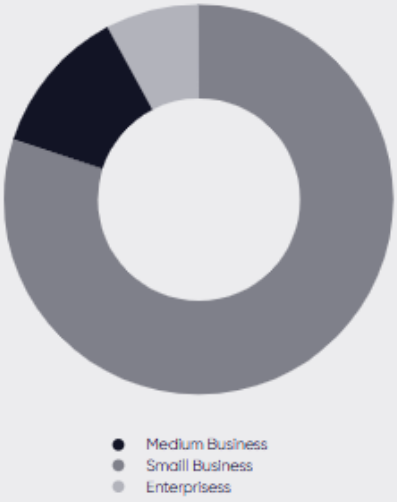
Meow's attacks spread to many countries, inclu-ding the US, the UK, Nigeria and Italy, and targeteda wide range of organizations. Especially with theMeow Leaks operations in 2023, data leakage-o-riented threats have become more prominent. Inaddition to Meow's encryption structure, this newvariant, which only leaks data instead of encrypti-on, has also been observed to be a major threat.

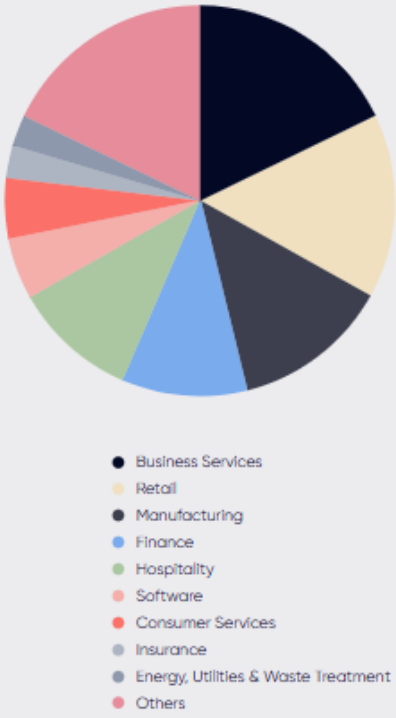
# Medusa




## Who is Medusa?

*Medusa ransomware, active since June 2021,operates as Ransomware-as-a-Service(RaaS) and targets vulnerabilities in RemoteDesktop Protocols (RDP) and phishingcampaigns. Known for double extortion, itencrypts data using RSA and AES256encryption, demanding ransoms fordecryption keys and to prevent data leaks.Key indicators include the ".MEDUSA" fileextension and ransom notes named"!!!READ_ME_MEDUSA!!!.txt".*



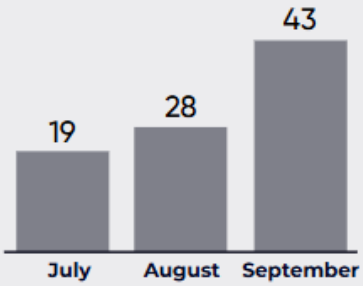



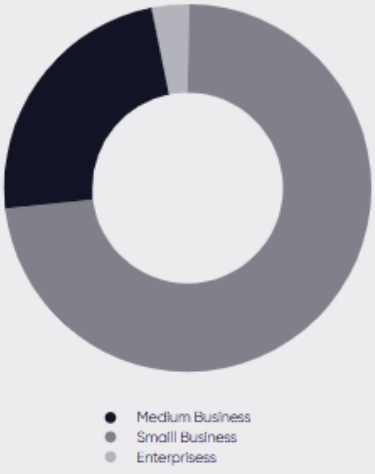

Medusa Ransomware employs a variety of tacticsto infiltrate systems, including phishing emails,malicious attachments, and exploiting softwarevulnerabilities. Once inside, it encrypts critical dataand systems, rendering them unusable until aransom is paid. This method disrupts businessoperations and forces victims into a difficult positi-on, often requiring significant resources to resolve.

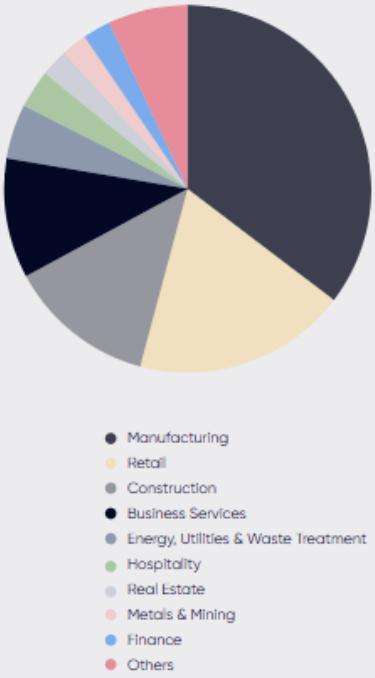
Notably, Medusa also engages in data theft priorto encryption, exfiltrating sensitive information.This double extortion tactic means victims facethe dual threat of losing access to their data andthe potential public release of stolen information ifthe ransom is not paid. The ransomware's opera-tors tailor their attacks to the specific environ-ments of their targets, using advanced techniquesto evade security measures and ensure effectiveexecution within the network. Beyond data encr-yption, Medusa can disrupt entire networks, cau-sing significant operational downtime and financi-al losses, making it particularly devastating fortargeted organizations.

# 13

# Play




## Who is Play?

*Ransomware attributed to the PLAY group,also known as PlayCrypt, has been observedin active campaigns since at least mid-July2022. In mid-August of the same year, thefirst public instance of PLAY Ransomwarecame to light when a journalist uncoveredits impact on Argentina's Judiciary ofCórdoba.*

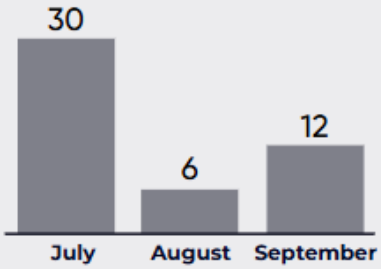
Play has been linked to multiple notable breaches andis recognized for its focus on exploiting vulnerabilitiesin Microsoft Exchange. Additionally, Play is among theinitial ransomware organizations to utilize periodic encryption, facilitating the rapid encryption of targetedsystems.

The operators behind these campaigns employcommon big game hunting (BGH) tactics. They utilizethe SystemBC Remote Access Trojan (RAT) for establishing persistence and Cobalt Strike for post-compromise tactics. Additionally, they are known to leveragecustom PowerShell scripts along with AdFind fornetwork enumeration. For privilege escalation, theyutilize WinPEAS. Inside a target network, the groupemploys RDP or SMB for lateral movement. In April 2023, it was detected that the Play ransomware grouphad developed two custom tools in .NET named "Grixba" and "VSS Copying Tool.“

To mark encrypted files, the threat actors append the ".play" extension, and their ransom note includes onlythe word "PLAY" and an email address for communica-tion. Unlike some other BGH ransomware campaigns, PLAY Ransomware operators do not operate a Tor dataleak site to exfiltrate stolen files. Instead, they have beenobserved using WinSCP for file exfiltration.

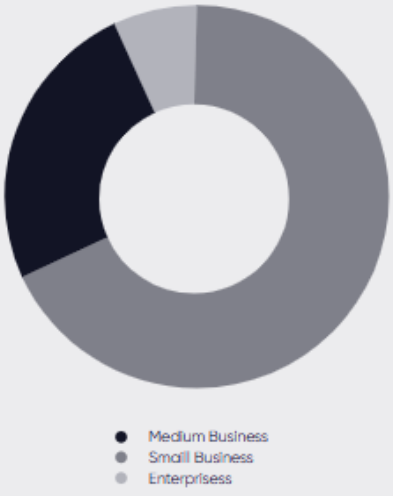
14

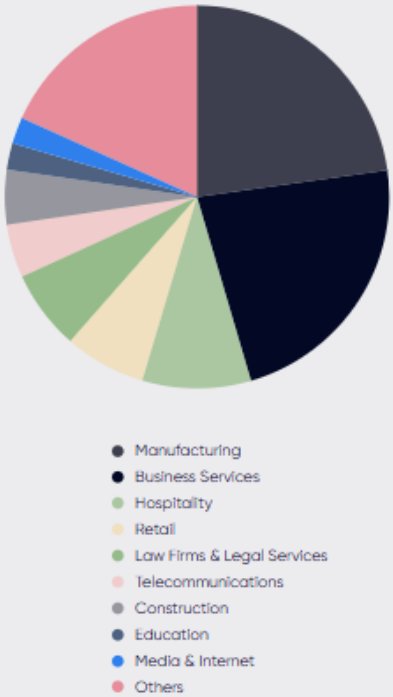
# Akira




## Who is Akira?

*Akira is a ransomware group that emerged in2023. Similar to other prominent RaaS(Ransomware as a Service) groups, itexfiltrates data from target devices beforeencrypting them, leveraging this data fordouble extortion. In this tactic, the attackersdo not compel victims to pay for bothdecryption assistance and data deletionseparately. Instead, Akira offers victimsthe option to choose which services they wantto pay for. However, if a victim refuses to paythe ransom, their name and data arepublished on Akira's leak site.*




The initial version of Akira was written in C++ andappended the ".akira" extension to files while leaving a ransom note named "akira_readme.txt.“ However, shortly thereafter, a new version was released on July 2, 2023, correcting a decryption flaw. Since then, a new version of Akira has emerged,developed in the Rust language, known as "mega-zord.exe," at the end of August 2023, appending the ".powerranges" extension to encrypted files. Theransomware operates by deleting Windows Shadow Volume Copies to hinder data recovery.Akira employs various tactics to infect its victims, including sending email attachments with macros,malvertising, torrent websites, and pirated softwa-re. Weaknesses in multi-factor authentication (MFA) are often targeted, as well as known vulnerabilities in VPN software. The attackers attempt toobtain credentials through LSASS dumps for lateral movement and privilege upgrades when necessary. Akira attempts to scan the target network todiscover target systems and network configurations. Additionally, it may use the AdFind tool toaccess information in Active Directory, employ an SFTP client like FileZilla to steal and exfiltrate sensitive data from posts of targets and the targeted servers, and use tools like SystemBC for persistent access after the initial attack.

CMC TELECOM
Aspire to Inspire the Digital World

# Q3/2024 Spotlight Uncovering the Significant News Surrounding the Quarter's Top

# Q3/2024 Important Ransomware News

## Identities of Several Evil Corp Members Revealed:
Lockbit Affiliate Among Them


**Source:** https://www.nationalcrimeagency.gov.uk/images/Oct2024/AF_social_1.png

Sixteen members of the Evil Corp cybercrime group, once considered one of theworld's largest cyber threats, have faced sanctions in the United Kingdom. These members were found to have links to the Russian state and other prominent ran-somware groups such as LockBit.

A comprehensive investigation conducted by the UK's National Crime Agency (NCA)revealed the history and activities of Evil Corp. Initially a family-centered financialcrime group based in Moscow, the group transitioned into cybercrime, extorting atleast $300 million globally.

In 2019, this investigation led to the indictment and sanction of Evil Corp's leaderMaksim Yakubets and group administrator Igor Turashev in the United States, alongwith several other members. Yakubets, Turashev, and seven others sanctioned bythe US in 2019 have now been sanctioned by the UK's Foreign, Commonwealth &Development Office, along with an additional seven individuals previously not expo-sed for their support of the group.

Among those newly sanctioned is Alek-sandr Ryzhenkov, Yakubets' right-hand man. Ryzhenkov played a significant rolein developing some of the group's mosteffective ransomware strains. As part of Operation Cronos, Ryzhenkov was identified as a LockBit affiliate involved in ransomware attacks against several organizations. The US Department of Justicealso unsealed an indictment against Ryzhenkov for using the BitPaymer ransomware against US victims.

In the UK, others sanctioned includeYakubets' father Viktor Yakubets, his father-in-law Eduard Benderskiy, aformer high-ranking FSB official, andother key figures who supported EvilCorp's criminal activities. The latest sanctions were said to expose more members of Evil Corp, including a LockBit affiliate, as well as individuals supportingthe group's activities.

Evil Corp was officially formed as a crimegroup in 2014 and developed and distributed ransomware such as BitPaymer and Dridex, targeting banks and financial institutions in over 40 countries, stealing over $100 million. The group held aprivileged position, with some membershaving close ties to the Russian state.Benderskiy played a key role in strengthening Evil Corp's relationship with Russian Intelligence Services, which reportedly tasked the group with conducting cyberattacks and espionage operationsagainst NATO allies before 2019.

After the US imposed sanctions and indictments in December 2019, Benderskiyused his influence to provide protectionfor the group's leaders, ensuring they were not pursued by Russian authorities,thereby securing the group's operations.These 2019 actions significantly weake-ned Evil Corp's ability to demand ransompayments and forced the group to rebuild and adopt further measures to conceal their activities from law enforcement.

The group adapted by developing additional malware and ransomware strains, including Wasted Locker, Hades, PhoenixLocker,PayloadBIN, and Macaw. They shifted their focus from widespread attacks to targeting highvalue organizations. Some members abandoned their own tools and instead adopted ransomware developed by other criminal groups, such as LockBit.

The NCA continues to monitor the illegal activities of former Evil Corp members, particularly their involvement in ransomwareattacks. The international investigation intoLockBit is also ongoing, with the group's original leak site, now under NCA control,coming back online this week. The site details actions taken by the Cronos Taskforce,including the arrests of two individuals in August, suspected of being associated witha LockBit affiliate, on charges of Computer Misuse Act violations and money laundering.

That same month, French authorities arrested a LockBit developer, and Spanish police detained a primary facilitator of LockBit's infrastructure and seized nine servers used by the group.

*over*

**40 countries**

*stealing over*

***$100 million***

# Arrested LockBit Ransomware Group Members Plead Guilty

Ruslan Magomedovich Astamirov and Mikhail Vasiliev have pleadedguilty to being members of the LockBit ransomware group, one ofthe most widespread ransomware operations globally, and tocarrying out LockBit attacks against victims in the United Statesand around the world.

Ruslan Magomedovich Astamirov and Mikhail Vasiliev have pleaded guilty tobeing members of the LockBit ransomware group, one of the most widespread ransomware operations globally, and to carrying out LockBit attack sagainst victims in the United States andaround the world. Ruslan Magomedovich Astamirov, 21, from the Chechen Republicof Russia, and Mikhail Vasiliev, 34, a dualcitizen of Canada and Russia, were both members of the LockBit group. Between January 2020 and February 2024, LockBit became one of the most active and destructive ransomware groups, targeting over 2,500 victims in 120 countries, 1,800 of whom were in the United States.

Victims included individuals, small businesses, hospitals, schools, multinational corporations, nonprofit organizations,critical infrastructure, and law enforcement agencies. LockBit extorted approximately $500 million in ransom from its victims and caused billions of dollars in additional damages, including lost revenue and incident response costs.

As affiliates of LockBit, Vasiliev and Astamirov illegally accessed vulnerable computer systems, stealing and encrypting data through ransomware. They demanded ransom from victims in exchange for decrypting the data and claimed that they would delete the stolen data. If victims refused to pay, the attackers leftthe data encrypted permanently and published the stolen information on apublic website. Between 2020 and 2023, Astamirov deployed LockBit ransomware against 12 victims, including organizations in Virginia, Japan, France, Scotland, and Kenya, extorting $1.9 million. He operated under various aliases such as "BET-TERPAY" and "offtitan."  Astamirov has agreed to forfeit assets, including 350,000 in crypto currency. Vasiliev, using aliases like "Ghostrider" and "Digitaloce-an90," attacked 12 victims between 2021 and 2023. These victims included businesses in the United States, the United Kingdom, and Switzerland. He also targeted an educational facility in England anda school in Switzerland, causing $500,000in damages. Vasiliev was arrested in Canada in November 2022 and extraditedto the United States in June.

REWARDS OF UP TO $15 MILLION

LOCKBIT 3.0

**NAME:** LockBit Ransomware as a Service (RaaS)
**NATIONALITY**: Various (Unknown)
**CITIZENSHIP:** Various (Unknown)

The U.S. Department of State is offering **a reward of up to $10,000,000** for information leading to the identification or location of any individual(s) who hold a key leadership position in the Transnational Organized Crime group behind the LockBit ransomware variant. In addition, **a reward offer of up to $5,000,000** is offered for information leading to the arrest and/or conviction in any country of any individual conspiring to participate in or attempting to participate in LockBit ransomware activities.

**Source:** https://www.justice.gov/usao-nj/media/1361001/dl?inline

Astamirov pleaded guilty to conspiracy to commit computer fraud andabuse and conspiracy to commit wire fraud, facing up to 25 years inprison. Vasiliev pleaded guilty to four charges, facing up to 45 years inprison. Sentencing dates have not yet been set, and a federal districtcourt judge will determine their sentences, considering the U.S. Sen-tencing Guidelines and other statutory factors.

The guilty pleas follow an operation conducted by the UK's NationalCrime Agency (NCA) in February, in cooperation with the U.S. Depart-ment of Justice, FBI, and other international partners. This operationtargeted the LockBit infrastructure, seizing public-facing websites andservers used by LockBit administrators, significantly disrupting theirability to carry out attacks and extort victims.

Dmitry Yuryevich Khoroshev, alleged to be the creator of LockBit, wascharged in May 2024. He allegedly recruited new members, operatedunder the alias "LockBitSupp," and maintained the infrastructure usedfor ransomware attacks. Khoroshev is also accused of taking a 20%share of each ransom, amassing at least $100 million.

Other individuals charged include Artur Sungatov and Ivan Kondrat-yev, who are accused of using LockBit ransomware against U.S. victimsand others globally. Mikhail Matveev is also charged with using variousransomware variants to attack U.S. victims. Rewards of $10 million havebeen offered for information leading to their arrests.

# Record $75 Million Ransom Paid in Recent Ransomware Attack

Ransomware attacks are becoming increasingly frequent and severe, with a recent incident setting a new record in cyber extortion. Cencora, one of the largest pharmaceutical distributors in the United States, paid an unprecedented $75 millionin Bitcoin after falling victim to a sophisticated ransomware attack in February. This record-breaking ransom, coupled with a growing number ofsimilar attacks, signals a worrying trend in the rise of cybercrime, particularly ransomware.

The attack, believed to have been orchestrated by the notorious Dark Angels group, initially came with a ransom demand of $150 million. After negotiations, Cencora managed to reduce the demand by 50%, but the final payout still far surpassed any previously known ransom settlement.This event marks a grim milestone in the escalation of ransomware attacks, underscoring the increasing financial stakes and boldness of cybercriminals.

The ransomware attack on Cencora led to the theft of highly sensitive patient data, including names, addresses, dates of birth, and medical records. While the company assured stakeholders that the incident would not significantly disrupt its operations, the breach has already hadnotable consequences. News of the ransom payment sent Cencora’s stock prices tumbling, reflecting investor concerns over the potential longterm fallout from the attack.

Experts are particularly alarmed by the scale of the ransom payment, warning that such substantial payouts could embolden other cybercriminal groups to adopt similar tactics. Last year alone, ransomware payments exceeded $1 billion, highlighting the growing financial impact ofsuch cybercrimes. As cybercriminals becomemore organized and sophisticated, the threat of ransomware continues to escalate, posing significant risks to organizations across all industries.

CMC TELECOM
Aspire to Inspire the Digital World

# KARAKURT

## Ransomware Suspect Extradited to U.S.

Deniss Zolotarjovs, a suspectedmember of the Russian Karakurt ransomware gang, is being charged in aU.S. court with money laundering, wirefraud, and extortion under the HobbsAct. The 33-year-old Latvian national, residing in Moscow, was arrested in Georgia in December 2023 and extradited to the United States earlier this month. According to court documents, Zolotarjovs is accused of stealing datafrom at least six U.S. companies between August 2021 and November 2023,and subsequently demanding crypto currency ransom payments, leakingvictims' sensitive information online insome cases. Zolotarjovs, who used thealias "Sforza," was responsible for negotiating with victims, particularly thosewho initially refused to pay the ransom.

The U.S. Department of Justice alleges that Zolotarjovs and his associates harassed company employees and pressured them to make ransom payments by contacting them directly viaemail or phone. In one instance, a victim paid $1.3 million in Bitcoin toprevent the gang from publishing theirdata. Court documents reveal that "Sforza" was sometimes successful inreviving stalled extortion cases. It was also noted that he discussed hiring paid journalists to publish news about victims in order to intimidate other targets. Zolotarjovs is the first suspected Karakurt member to be arrested and extradited.

# BLACK BASTA

## Black Basta Adapts Strategy Post-Qakbot Takedown

The Black Basta ransomware group hasshifted its strategy following the takedown of the Qakbot botnet, now employing new custom tools and initial access techniques. Previously, the group usedQakbot through phishing campaigns togain access to target systems. However, after the U.S. government's "OperationDuck Hunt" disabled Qakbot, Black Bastabegan developing their own custom malware and using access brokers. Aspart of this shift, the group resumed using the "SilentNight" backdoor and deployedit through malvertising campaigns, moving away from phishing methods.

nce gaining access to target systems, the group employs "living-off-the-land"(LotL) techniques along with custommalware to maintain persistence and perform lateral movement. A new tool, "Cogscan," is used to map out target networksand collect system information, replacingearlier opensource tools like Bloodhound. Another tool, "Knotrock," facilitates rapid ransomware deployment across network shares, accelerating the encryption process. These tools allow BlackBasta to conduct larger-scale and fasterattacks.

Black Basta's innovative approaches demonstrate the group's adaptability andresilience. Moving away from popular methods like phishing, the group has developed more complex and targeted tactics to carry out their attacks quickly and extort victims through data leaks.These developments indicate that ransomware attacks are becoming morerapid and complex, underscoring the need for strengthened defense measures.

CMC TELECOM
Aspire to Inspire the Digital World

# Most Used CVEs by Ransomware Groups Q3/2024 Analysis A Study of Prevalent Vulnerabilities

CMC TELECOM
Aspire to Inspire the Digital World

# Critical Vulnerabilities Analysis Over Q3/2024

Throughout Q3 2024, ransomware attacks have continued to exploit both new and old vulnerabilities. A particularly dangerous flaw, CVE-2024-4577, affects certain PHP versions on Windows servers using Apache and PHP-CGI, allowing attackers to execute arbitrary PHP code. Meanwhile, an older vulnerability, CVE-2020-1472, known as "Zerologon," has resurfaced, with a new threat actor utilizing it to gain domain administrator access by exploiting the Netlogon protocol. This combination of new andold exploits has contributed to the increasing sophistication of ransomware campaigns.

Other significant vulnerabilities include CVE-2024-23897 in Jenkins, which allows attackers to read arbitrary files and potentially execute remote code, and CVE-2024-37085 in VMware ESXi, which grants unauthorized access to ESXi hoststhrough authentication bypass. These vulnerabilities are actively being targeted byransomware groups, making it crucial for organizations to strengthen their defenses.

CMC Telecom Threat Intelligence Service can help you stay proactive by providing immediate alerts on new exploits and community intelligence on popular CVEs and related GitHub repositories. By utilizing resources like CMC Telecom and implementing security best practices, you can significantly reduce the risk of falling victimto ransomware attacks and ensure the safety of your data and systems.

| | | |
|---|---|---|
| 10 - Critical<br>Netlogon<br>**CVE-2020-1472**<br>**Group:** Ransomhub | 9.8 - Critical<br>SonicWall SonicOS<br>**CVE-2024-40766**<br>**Group:** Akira | 9.8 - Critical<br>Jenkins<br>**CVE-2024-23897**<br>**Group:** RansomEXX |
| 9.8 - Critical<br>PHP-CGI Argument<br>**CVE-2024-4577**<br>**Group:** TellYouThePass | 9.8 - Critical<br>Fortinet FortiClientEMS<br>**CVE-2023-48788**<br>**Group:** Medusa | 7.8 - High<br>Microsoft Windows Kernel<br>**CVE-2024-21338**<br>**Group:** Mallox |
| 7.5 - High<br>Microsoft Office and Windows HTML<br>**CVE-2023-36884**<br>**Group:** Underground Ransomware | 7.5 - High<br>Veeam Backup & Replication<br>**CVE-2023-27532**<br>**Group:** Phobos, Estate Ransomware | 7.2 - High<br>VMware ESXi<br>**CVE-2024-37085**<br>**Group:** BlackByte |

# Deep Dive in Tactics, Techniques and Procedures

Cybercriminals leverage a variety of tactics, techniques, and procedures (TTPs) to exploit system vulnerabilities and deploy ransomware attacks. These malicious actors often target specific security weaknesses to gain unauthorized access, using tools such as remote code execution to infiltrate systems. Once inside, they bypass authentication and exploit privilege escalation vulnerabilities to deepen their control. With full access, the ransomware is deployed, encrypting critical files and making them inaccessible to the victim until a ransomtypically in cryptocurrency is paidfor the decryption key.

As these attacks grow more sophisticated, cybersecurity professionals must remain alert and adopt effective defense strategies. Regular software updates, strong cybersecurity practices, comprehensive risk assessments, and user trainings are key to reducing vulnerabilities. Additionally, organizations must implement rigorous backup and recovery plans to mitigate the damage caused by ransomware attacksand ensure ongoing operations. By staying informed and adopting proactive security measures, organizations can better protect their systems and critical data from the constantly evolving tactics of cybercriminals, reducing the impact of ransomware threats.

## 1.TTP Exploiting Remote Code Execution Vulnerabilities

**CVE-2024-4577:** This vulnerability affects PHP versions 8.1 before 8.1.29, 8.2 before 8.2.20, and 8.3 before 8.3.8 when using Apache and PHP-CGI on Windows. When the system is configured to use certain code pages, Windows may employ "Best-Fit" behavior to replace characters in the command line. These changes can cause the PHP CGI module to misinterpret command line characters, treating them as PHP options. This misinterpretation allows attackers to pass malicious options to the PHP binary, potentially executing arbitrary PHP code on the server and exposing sensitive information.

**CVE-2023-48788:** This vulnerability in Fortinet FortiClientEMS versions 7.2.0 through 7.2.2 and 7.0.1 through 7.0.10 allows attackers to execute unauthorized code or commands via specially crafted packets due to improper neutralization of special elements used in an SQL command.

**CVE-2024-23897:** This vulnerability allows attackers to read arbitrary files on the Jenkins controller file system through the command line interface (CLI). By leveraging a feature in the command argument parser, attackers with sufficient permissions can read entire files, potentially gaining access to sensitive information like cryptographic keys. In certain cases, this vulnerability can lead to remote code execution (RCE), particularly if the attackers obtain keys that allow further exploitation.

**CVE-2023-36884:** This vulnerability allows an attacker to evade Mark of the Web (MOTW) defenses by planting a malicious file, which can lead to code execution on the victim system. Successful exploitation of this vulnerability involves winning a race condition and requires user interaction, such as convincing the target to open a specially crafted file sent via email or instant message. If successful, it can lead to a high loss of confidentiality, integrity, and availability on the affected system.

## 2.TTP Bypassing Authentication and Exploiting Pre-Authentication Vulnerabilities

**CVE-2024-40766:** This vulnerability involves improper access control in SonicWall SonicOS management access, potentially leading to unauthorized access to resources and, under specific conditions, causing the firewall to crash. This issue affects SonicWall Firewall Gen 5 and Gen 6 devices, as well as Gen 7 devices running SonicOS 7.0.1-5035 and older versions.

**CVE-2024-37085:** This vulnerability in VMware ESXi allows an attacker with sufficient Active Directory (AD) permissions to bypass authentication and gain full access to an ESXi host. The attacker can exploit this vulnerability by re-creating the previously configured AD group ('ESXi Admins' by default) after it was deleted from AD, effectively bypassing authentication and taking control of the system.

## 3.TTP Exploiting Privilege Escalation Vulnerabilities

**CVE-2020-1472:** This vulnerability allows an attacker to connect to a domain controller using the Netlogon protocol and gain domain administrator access, effectively exploiting privilege escalation.

**CVE-2024-21338:** This vulnerability resides in the IOCTL dispatcher within appid.sys, which is the core driver behind AppLocker, Windows' application whitelisting technology. The vulnerable control code (0x22A018) is used to compute a smart hash of an executable image file. Due to improper handling of kernel function pointers from the input buffer, an attacker who can exploit this vulnerability may gain SYSTEM privileges, effectively escalating their privileges on the affected system.

## 4.TTP Vulnerabilities in Backup and Recovery Solutions

**CVE-2023-27532:** This vulnerability in a Veeam Backup & Replication component allows an unauthenticated user within the backup infrastructure network perimeter to obtain encrypted credentials stored in the configuration database. Exploiting this vulnerability may enable an attacker to gain unauthorized access to the backup infrastructure hosts, compromising the security of the backup and recovery environment.

CMC TELECOM
Aspire to Inspire the Digital World

# Final Words

*Strengthening Cybersecutiy Against Ransomware Attacks:*
*To mitigate risks, adopt multi-layer security approaches andproactive and comprehensive solutions.*

# Conclusion

*In the third quarter of 2024, ransomware attacks continued unabated globally, with a particular focus on critical infrastructure and small and medium-sized enterprises. There were 1218 ransomware attacks in this period, with 58 active threat groups.*

***The following summarizes the key findings and takeaways from this period:***

**Regional Distribution**
The majority of attacks (60.3%) occurred in North America, with the EMEA region, which covers Europe, the Middle East and Africa, suffering 25.9% of attacks. Developed economies in particular have become the primary target of ransomware groups, highlighting the need for stronger cybersecurity measures to protect digital infrastructures.

**Sectoral Targets**
Manufacturing was the most targeted sector (20.5%), followed by business services (14.9%) and retail (11.6%). The increase in attacks on critical infrastructures shows that ransomware groups are continuing their strategy of generating large ransom demands by causing operational disruptions.

**Tactics and Techniques of Ransomware Groups**
RansomHub was the most active ransomware group with 16%, while Play, LockBit3 and Meow groups were also among the major threats. Most attacks used double-sided blackmail tactics (data encryption and data exfiltration threats), and attacks focused on zero-day vulnerabilities made defense strategies more complex.

**Increased Threat to Small and Medium Enterprises**
Small businesses have been the most targeted group in ransomware attacks. With more limited cybersecurity resources, these businesses have been seen as easy targets for ransomware groups.

**Target Countries**
The United States was the most attacked country with 54.2%, while Canada, the United Kingdom and Germany also faced serious threats. Digital infrastructures and economic assets in these countries were found to be attractive targets for ransomware groups.

Ransomware threats are evolving rapidly, following different strategies across sectors, regions and business sizes. Countries and sectors must take more proactive cyber security measures against these threats. The diversification of the ransomware ecosystem once again demonstrates the need for more flexible and regionally focused security strategies.

CMC TELECOM
Aspire to Inspire the Digital World

# Recommendation

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

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

### Strengthening Cybersecurity Infrastructure

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

### Enhancing Security in Critical Sectors

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

### Focusing on Small and Medium-Sized Enterprises (SMEs)

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

## Defending Against Ransomware Group Tactics

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

## Developing Region-Specific Defense Strategies

Given that North America and EMEA regions face the highest number ofattacks, it is essential to tailor security strategies to the specific threatmodels and risks of each region. Implementing cybersecurity measuresaligned with local regulations and sector-specific requirements will create amore effective defense framework.

## Raising Cybersecurity Awareness and Training

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

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

CMC TELECOM
Aspire to Inspire the Digital World

# Thank you!