FALCONFEEDS.IO

QUARTERLY THREAT INTELLIGENCE REPORT

CYBER ATTACKS IN Q3 2024

(July -September)

Data sourced from FalconFeeds.io

PREFACE

In a world increasingly shaped by digital connections, the third quarter of 2024 underscored a sobering reality: cyber threats are not just rising—they're evolving. With over 9,300 incidents in three months, we witnessed a 14% surge in attacks that targeted every facet of modern society, from public institutions to private enterprises, disrupting lives and businesses alike. DDoS attacks, data breaches, and ransomware continue to headline these threats, particularly impacting essential sectors such as government, technology, and education.

This report, backed by the robust intelligence of FalconFeeds.io, offers more than numbers and charts—it's a narrative of today's cyber battleground. FalconFeeds.io has provided real-time insights into emerging attack patterns, helping to illuminate the expanding underground market and the rise in malicious tactics. From analysing shifts across regions like Europe, the Middle East, and Asia, to pinpointing the most relentless ransomware groups, this report delivers a clear, timely picture of the cyber threats at our doorstep.

Our aim is simple: to empower readers with the insights needed to confront these threats head-on. In this rapidly shifting landscape, proactive defense is the line between resilience and vulnerability. We hope this report serves as a valuable guide to staying ahead, protecting what matters, and strengthening defenses for the road ahead.

Nandakishore Harikumar,
CEO, FalconFeeds

TABLE OF CONTENTS

INTRODUCTION

The third quarter of 2024 saw a significant uptick in cyber attacks, with a total of **9,393 incidents** reported, representing a **14% increase** over Q2 2024. **DDoS attacks, data breaches**, and **ransomware** were the dominant attack vectors, with the **Government & Public Sector, Technology & IT Services,** and **Education** sectors being the most targeted.

FalconFeeds.io was instrumental in identifying and tracking these trends, offering real-time visibility into emerging cyber threats. Its comprehensive intelligence provided critical insights into the increase in **DDoS attacks** and the growing underground market for **access sales.**

This report offers a deep dive into the key incidents, trends, and affected sectors during Q3 2024, providing a comparative analysis with Q2 2024 and highlighting region-wise impacts across the **USA, Europe, ASEAN,** and other regions.

OVERVIEW OF KEY FINDINGS

Category-wise Incident Distribution (Q3 2024)

In Q3 2024, DDoS attacks accounted for the highest number of incidents, followed by **data breaches** and **ransomware:**

DDoS Attack:
3,748 incidents

Data Breach:
1,892 incidents

Ransomware:
1,246 incidents

Defacement:
1,235 incidents

Data Leak:
724 incidents

Access Sale:
548 incidents

Ransomware **13.3%**

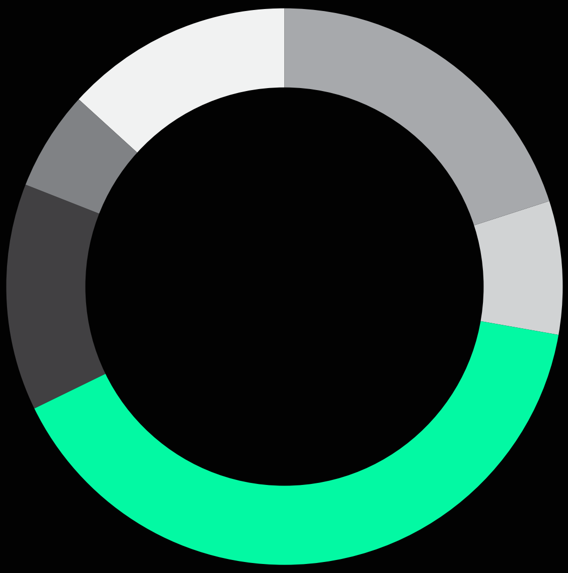
Access Sale: **5.8%**

Defacement: **13.1%**

Data Breach: **20.1%**

Data Leak: **7.7%**

DDoS Attack: **39.9%**

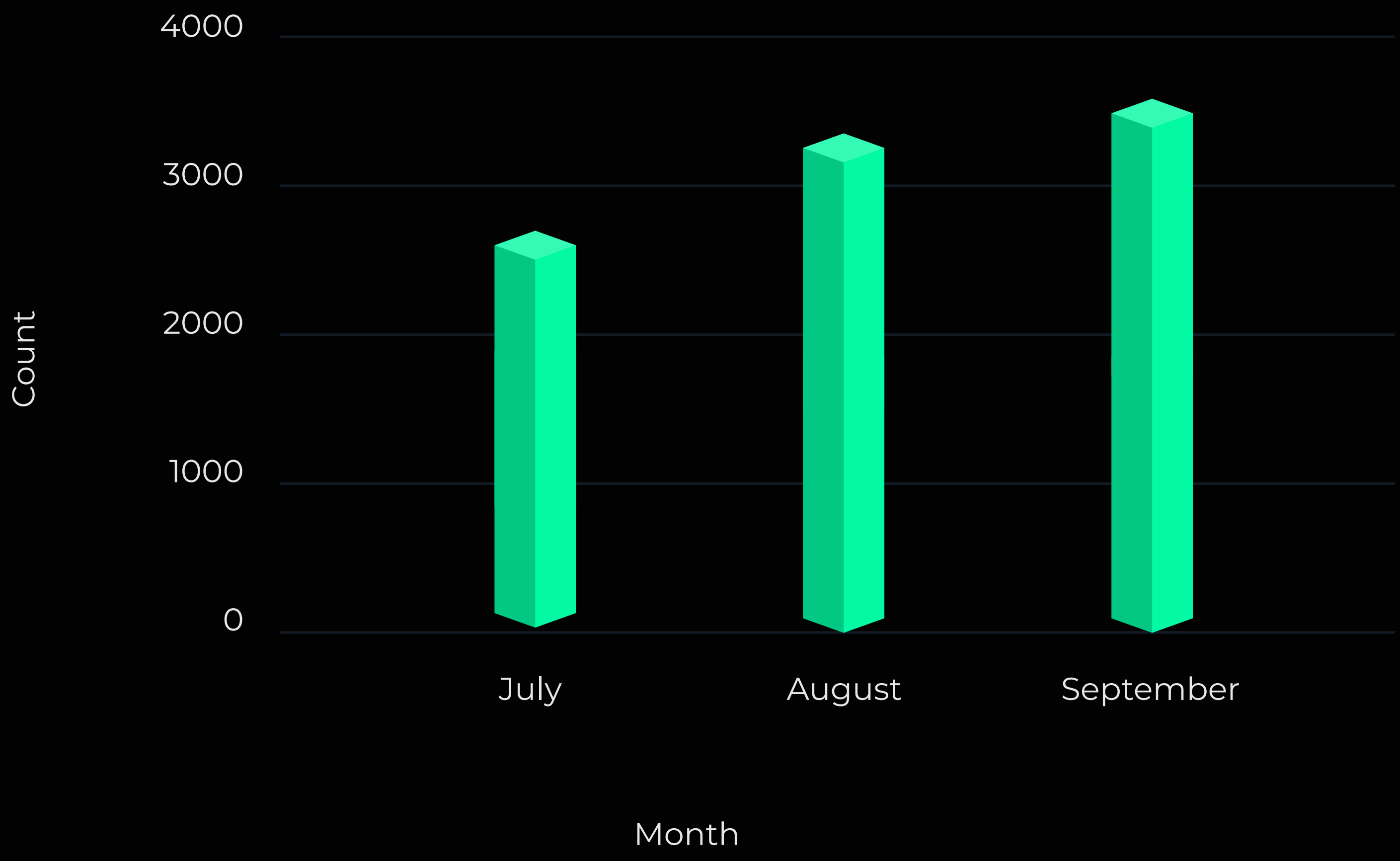


This highlights the critical importance of **disruption-based attacks**, such as DDoS, which continue to pose a significant threat to industries worldwide.

MONTH-WISE INCIDENT TRENDS

The number of incidents steadily increased from **July to September,** with the most significant rise in **DDoS attacks and defacements** in **August and September.**

July	August	September
2,749 incidents	**3,273 incidents**	**3,371 incidents**



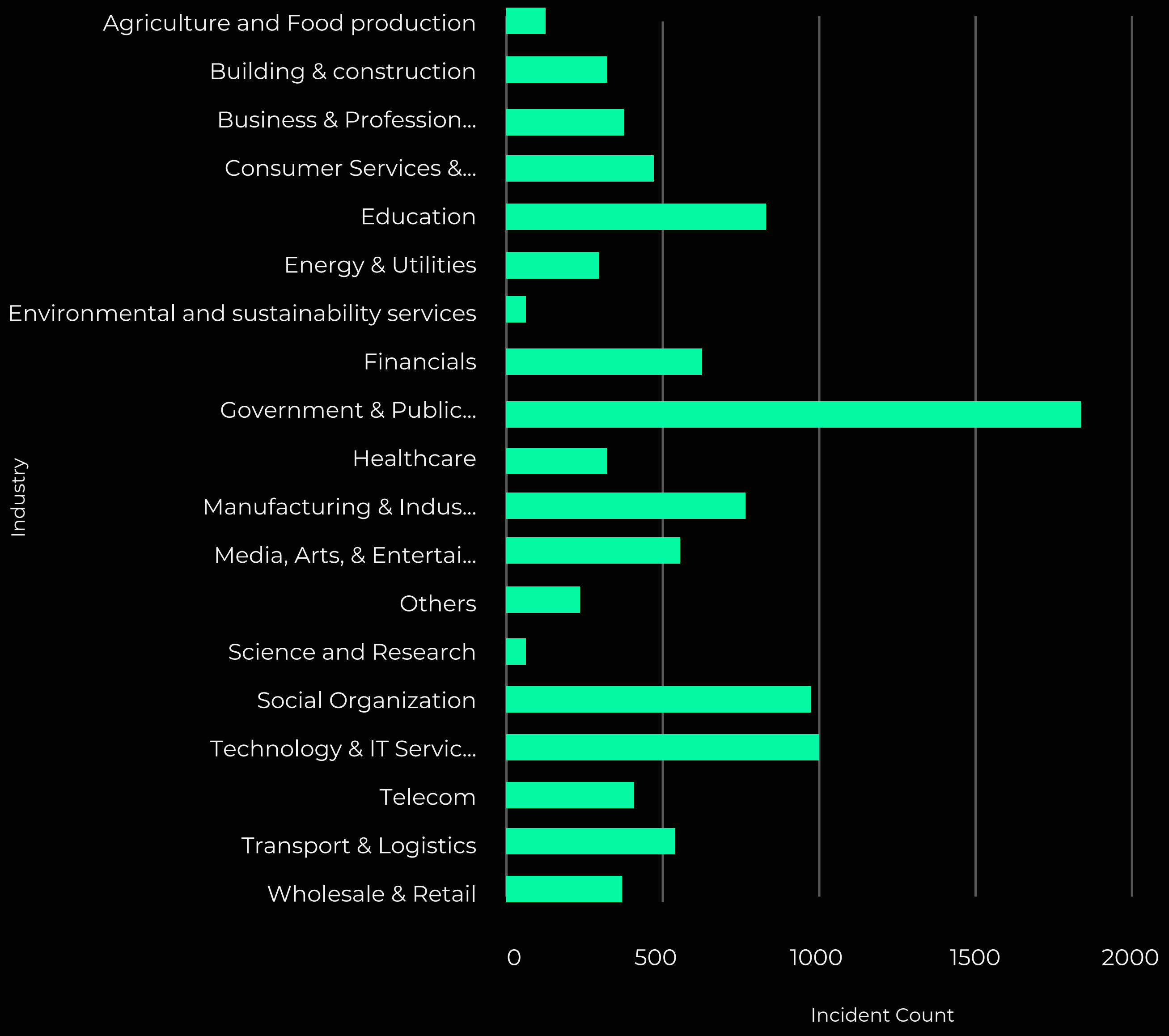
INDUSTRY-WISE IMPACT

The **Government & Public Sector** was the most heavily impacted industry, followed by **Technology & IT Services and Education**

Government & Public Sector **1,742 incidents**

Technology & IT Services **995 incidents**

Education **836 incidents**



COUNTRY-WISE IMPACT

The **USA** experienced the highest number of incidents in Q3 2024, followed by **India, Ukraine, Israel and Indonesia**

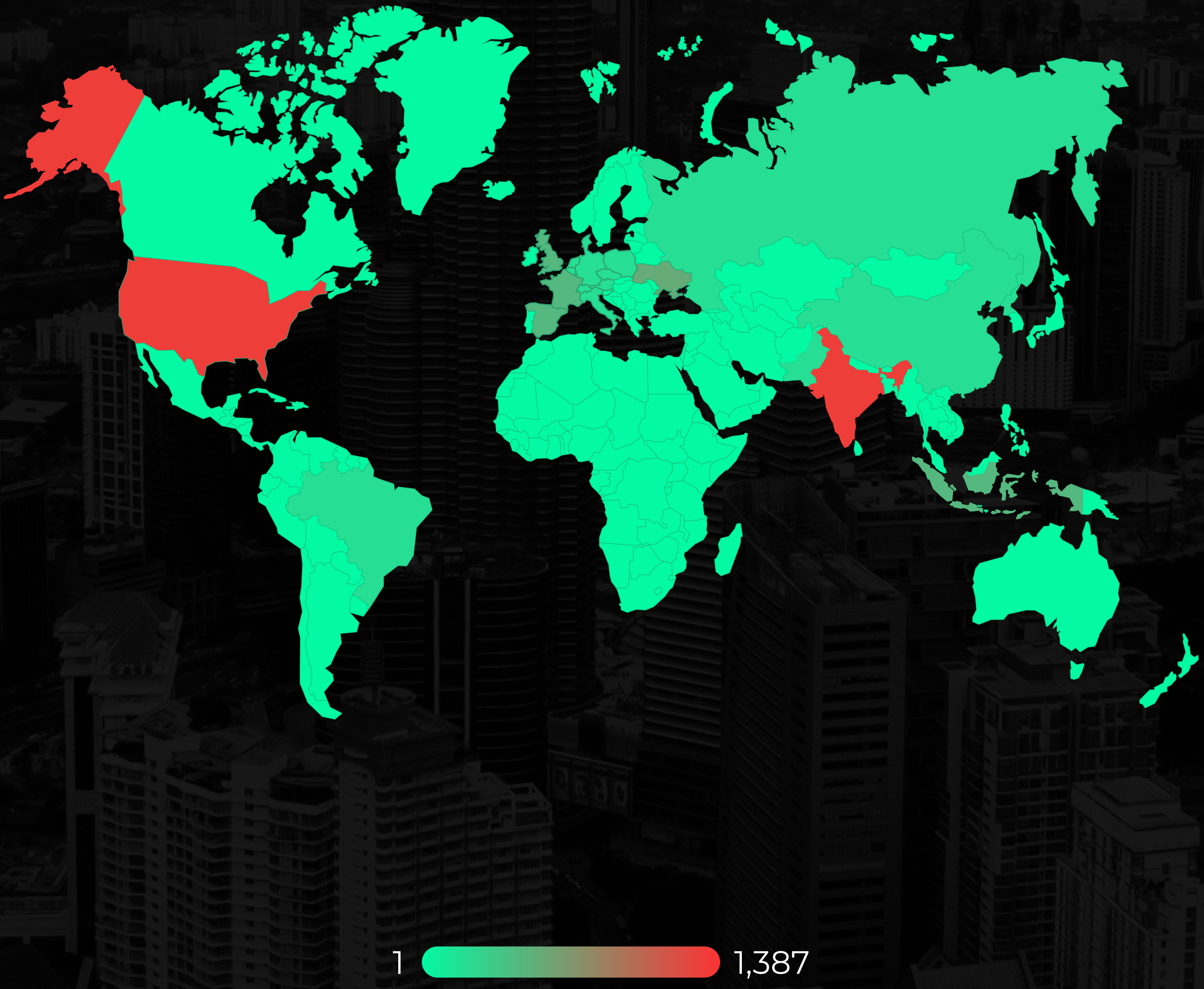
USA **1,387 incidents**

Ukraine **506 incidents**

India **1,223 incidents**

Israel **608 incidents**

Indonesia **512 incidents**



PLATFORM-WISE ACTIVITY

Underground forums remained active, with **Breach Forums** leading the way in cybercriminal activities, followed by **Exploit and Xss forums**

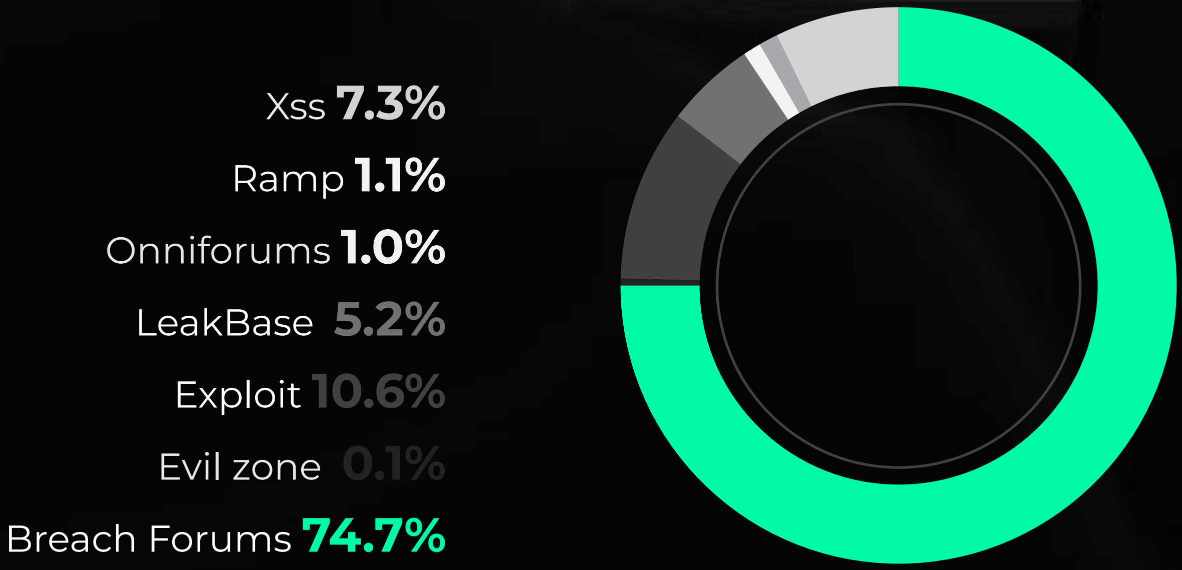
Breach Forums
1,953 incidents

Exploit
276 incidents

Xss
192 incidents

LeakBase
135 incidents

Ramp
28 incidents



COMPARATIVE ANALYSIS: Q2 2024 VS. Q3 2024

The comparison between Q2 and Q3 2024 reveals significant growth in cyber attack activity across key categories.

Category-wise Comparison

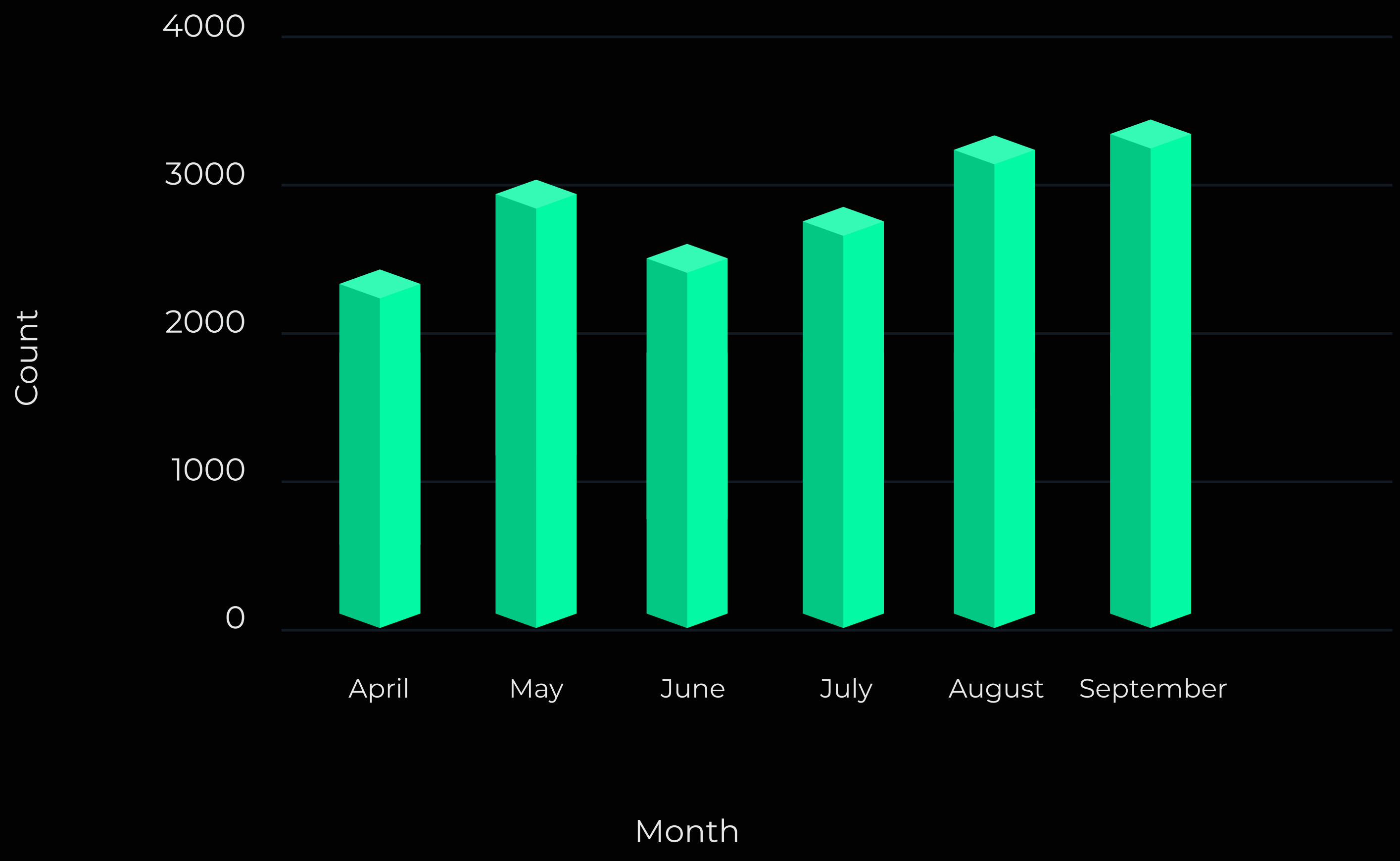
Category	Incident Count (Q3 2024)	Incident Count (Q2 2024)
DDoS Attack	3 ,748	2,977
Data Breach	1,892	1,596
Ransomware	1,246	1,231
Defacement	1,235	967
Data Leak	724	547
Access Sale	548	563

DDoS attacks saw the largest increase, with an additional **771 incidents** in Q3, underscoring the growing use of DDoS as a disruptive tool. **Defacements** also increased, particularly targeting **media** and **government websites** for political or ideological reasons.

MONTH-WISE COMPARISON

The total incident count rose sharply in Q3 compared to Q2, with a noticeable increase in **August** and **September** due to a rise in **DDoS attacks** and **data breaches.**

April **2,337 incidents**	May **3,033 incidents**	June **2,511 incidents**
July **2,749 incidents**	August **3,273 incidents**	September **3,371 incidents**



INDUSTRY-WISE COMPARISON

Category	Incident Count (Q3 2024)	Incident Count (Q2 2024)
Government & Public Sector	1,742	1,485
Technology & IT Services	995	1,006
Education	836	733
Manufacturing & Industrial	613	501
Financials	582	575
Healthcare	342	317

The **Government & Public Sector** saw the highest increase, reflecting the continued targeting of national institutions followed by the **Education and Manufacturing** sector, while **Technology & IT Services** remained consistently attacked.

COUNTRY-WISE COMPARISON

Country	Q2 Incident Count	Q3 Incident Count	Increase/ Decrease %
USA	1,390	1,387	0
India	852	1,223	44
Indonesia	334	519	55
Bangladesh	164	337	105
Brazil	138	149	8
Canada	141	141	0
China	112	117	4
Israel	515	608	18
France	151	348	130
Germany	182	118	-35
Ukraine	330	591	79
Mexico	68	57	-16
South Africa	31	22	-29
Japan	36	75	108

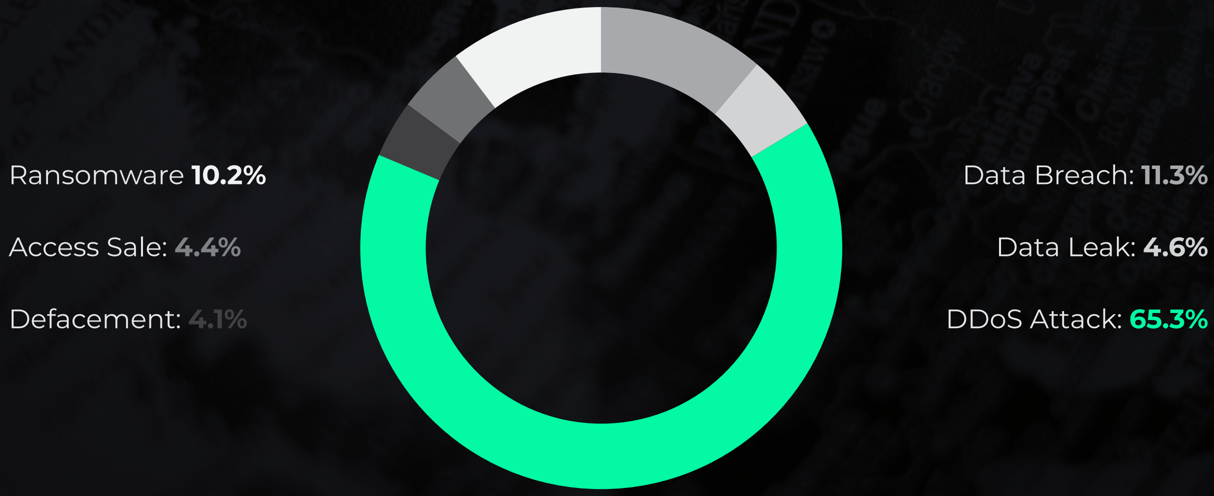
COUNTRY-WISE COMPARISON

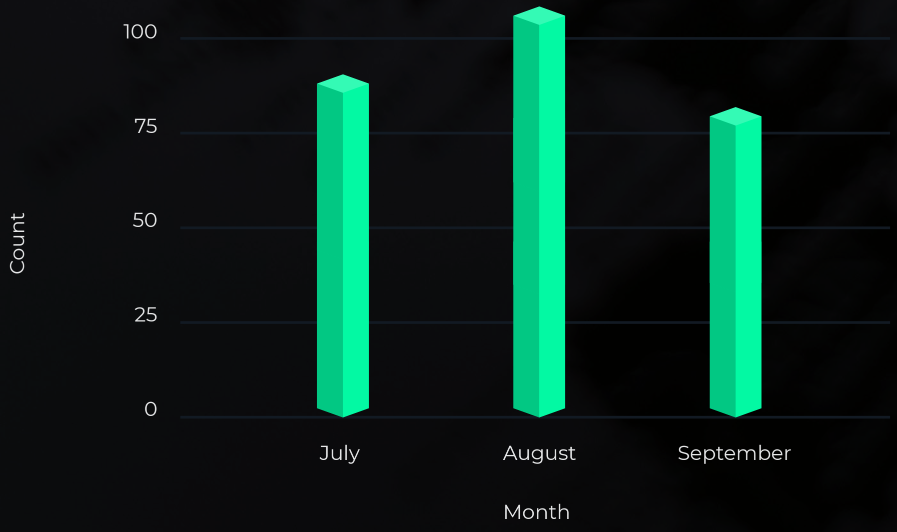
Key takeaways from the Q2 vs. Q3 country-wise comparison highlights significant increases in cyber attacks in India, Ukraine, and Israel, driven by DDoS attacks, ransomware, and defacements, often linked to geopolitical tensions. Indonesia was heavily targeted due to the opportunist nature of threat actors after the ransomware attack that affected the national data center (KOMINFO). In contrast, countries like the USA and Canada saw stable threat levels, while Germany experienced a decline. France and Japan saw notable rises in data breaches and ransomware, indicating shifting focus within Europe and Asia.

REGION-WISE THREAT INTELLIGENCE
EUROPE

Total Incidents (Q3): 2,757

Key Observations: Europe experienced a surge in **DDoS attacks** and **data breaches**, with **Government**, **Transportation**, **Technology** and **Manufacturing** sectors frequently targeted. **Ukraine**, **France**, **Spain** and the **United Kingdom** were highly targeted during this period. Ransomware remains a persistent threat across the region with 282 incidents with heightened activity in august. RansomHub (54 incidents) and Lockbit 3.0 (26 incidents) were the most active ransomware groups in the region.



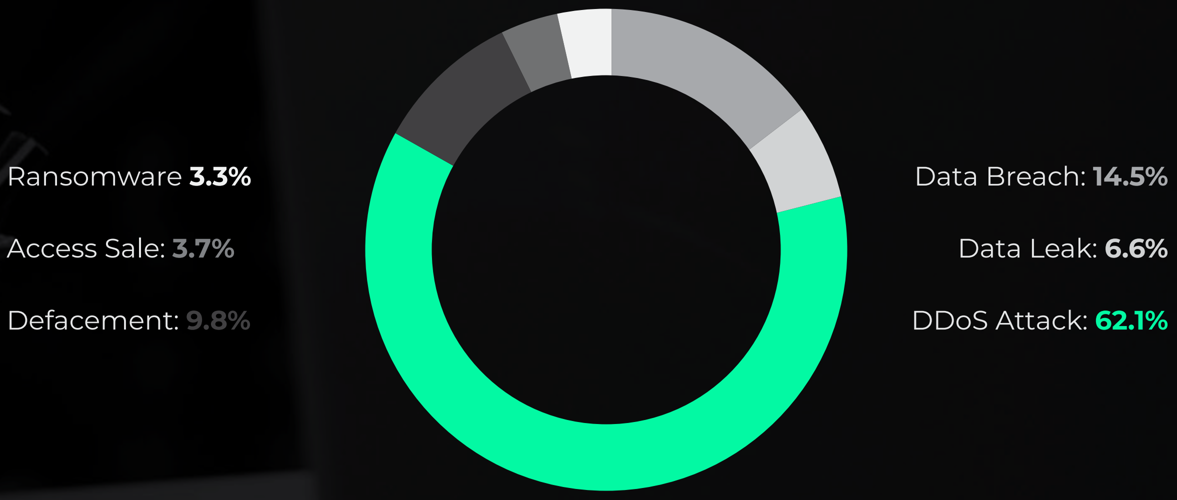


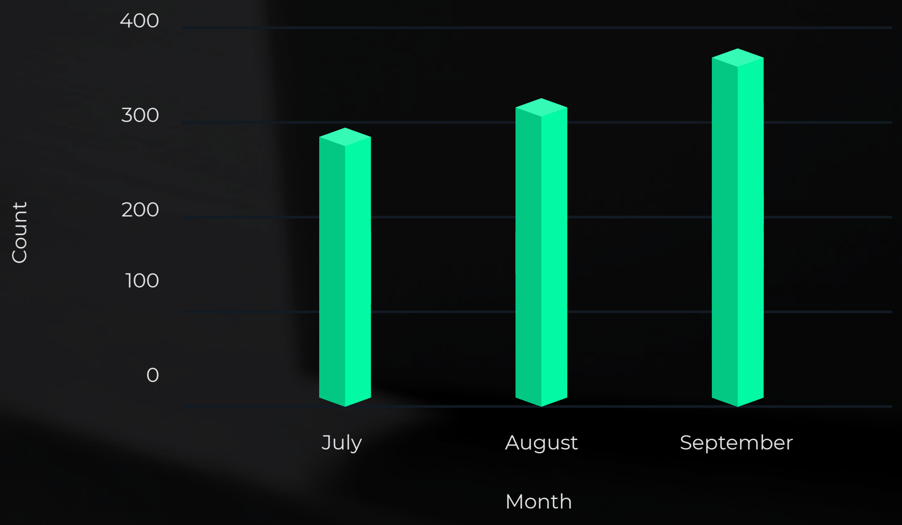
Countries analyzed : Albania,Andorra, Armenia, Austria, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia,Finland, France, Georgia, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Moldova, Netherlands, North Macedonia, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, UK and Ukraine

MIDDLE EAST

Total Incidents (Q3): 979

Key Observations: The **Middle East** faced numerous **DDoS attacks** and **data leaks**, targeting **Government**, **Technology**, **Financial**, **Education** and other **critical infrastructure**. **Israel**, **Turkey**, **UAE** and **Saudi Arabia** were highly targeted during this period. Ransomware has 32 incidents recorded in this region with increasing activity throughout the period. Meow (10 incidents) and RansomHub (9 incidents) were the most active ransomware groups in the region.



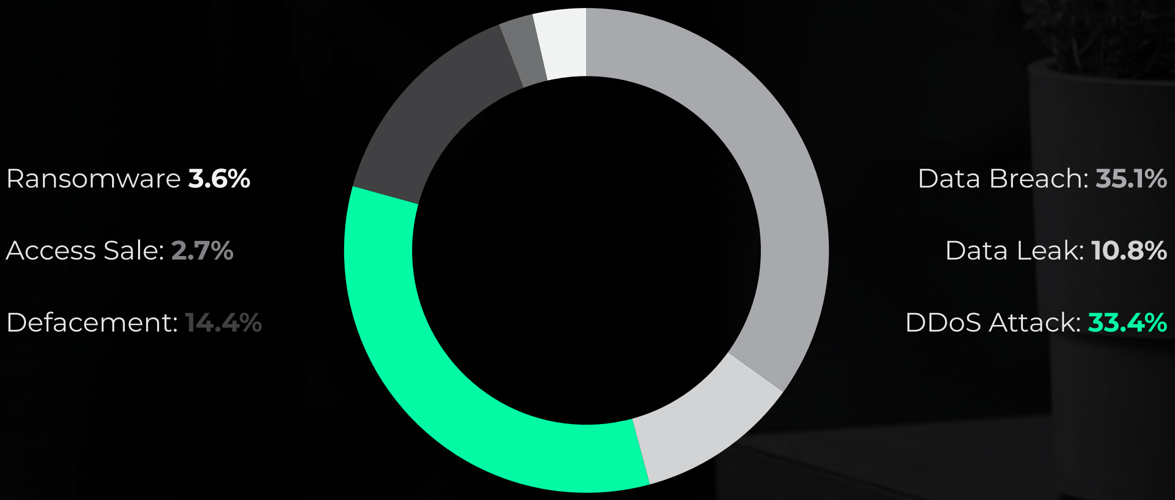


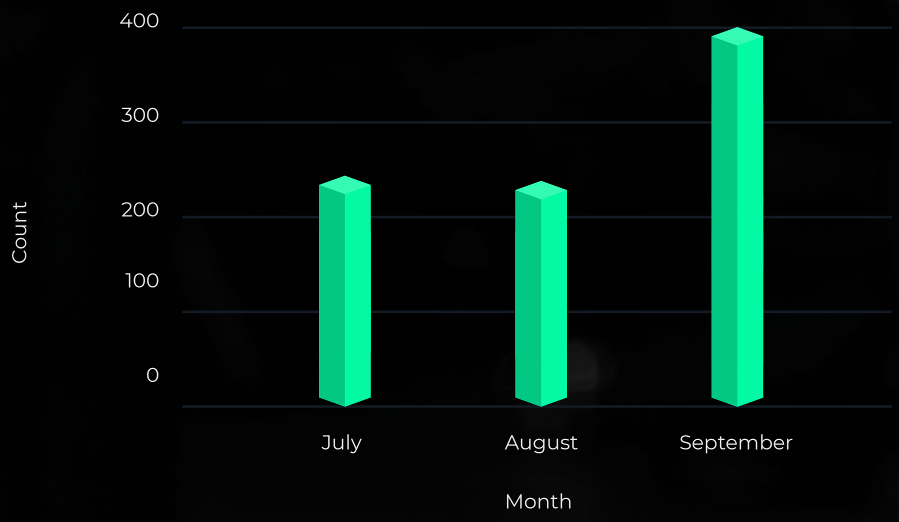
Countries analyzed : Bahrain, Egypt, Iran, Iraq, Israel, Jordan, Kuwait, Lebanon, Oman, Qatar, Saudi Arabia, Syria, Turkey, UAE, and Yemen.

ASEAN

Total Incidents (Q3): 891

Key Observations: **Indonesia**, **Thailand**, **Vietnam** and **Malaysia** were the hardest hit, with Data Breach and DDoS Attacks, often targeting Government, Education, Media and **Technology infrastructure.** Ransomware has recorded 32 incidents in this region while recording an upward trend in July and September. RansomHub (7 incidents) and Kill Security (4 incidents) were the most active ransomware groups in this region.



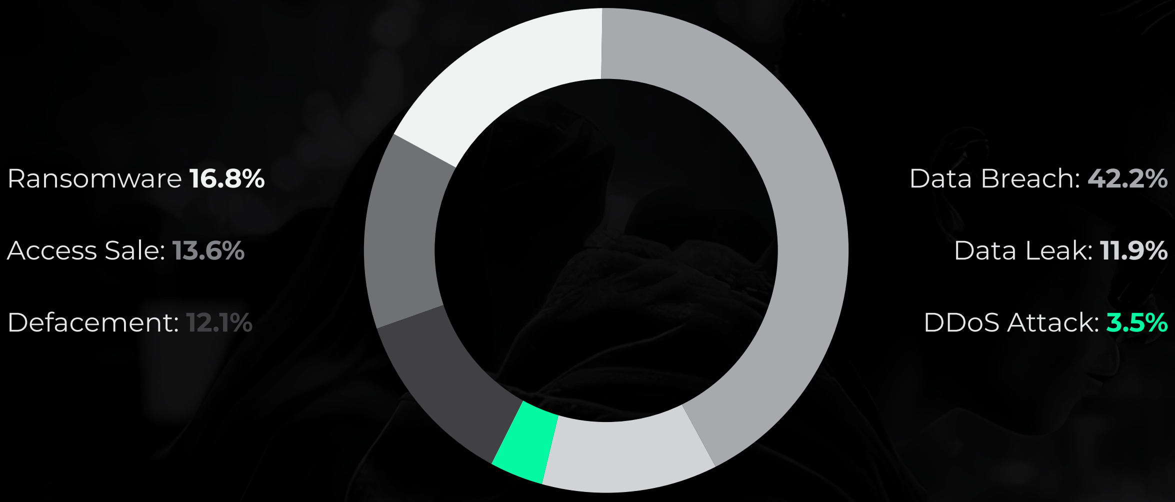


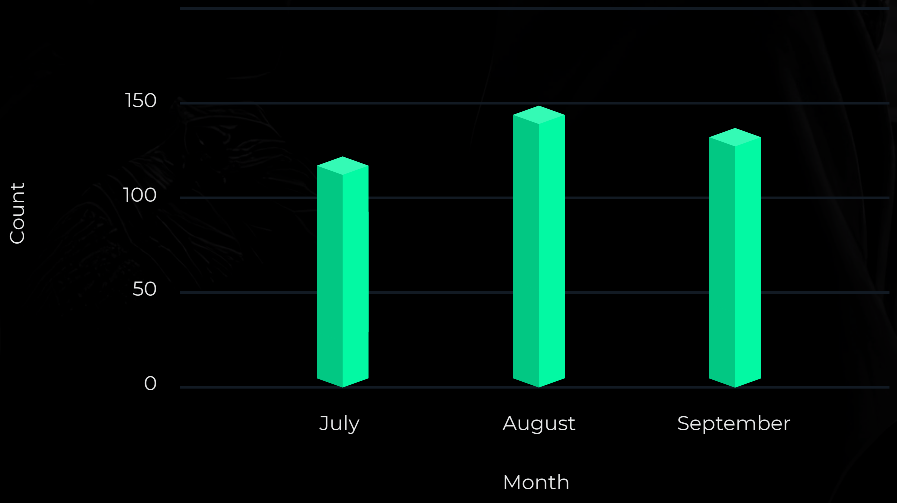
Countries analyzed : Cambodia, Indonesia, Laos, Malaysia, Myanmar, Philippines, Singapore, Thailand, Vietnam.

LATIN AMERICA

Total Incidents (Q3): 405

Key Observations: **Brazil** and **Argentina** were the primary targets along with Mexico Colombia and Peru, mainly facing **data breaches** and **Ransomware attacks**, particularly in the **Government**, **Technology**, **Manufacturing** and **Financial sectors**. Ransomware has recorded 68 incidents with increasing activity throughout the period. RansomHub (14 incidents) and LOCKBIT 3.0 (8 incidents) were the most active ransomware groups in this region.



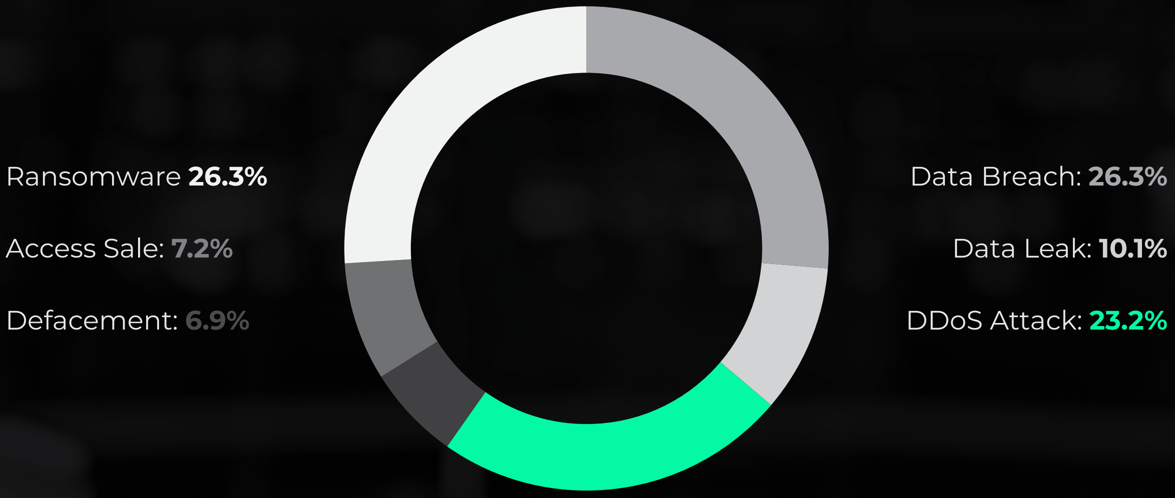


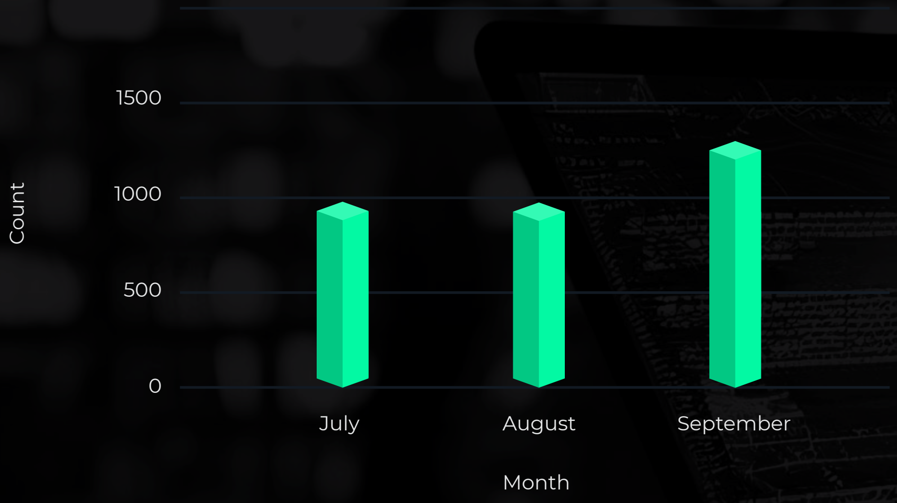
Countries analyzed : Argentina, Bolivia, Brazil, Chile, Colombia, Costa Rica, Cuba, Dominican Republic, Ecuador, El Salvador, Guatemala, Mexico, Panama, Paraguay, Peru, Uruguay, Venezuela.

APEC

Total Incidents (Q3): 3,145

Key Observations: **USA** and **Indonesia** saw a high volume of incidents of **Data Breach** and **ransomware attacks**, targeting **Government** and **Technology sectors**. Ransomware has recorded 815 incidents with consistent activity throughout the period. RansomHub (112 incidents) and PLAY (82 incidents) were the most active ransomware groups in this region.



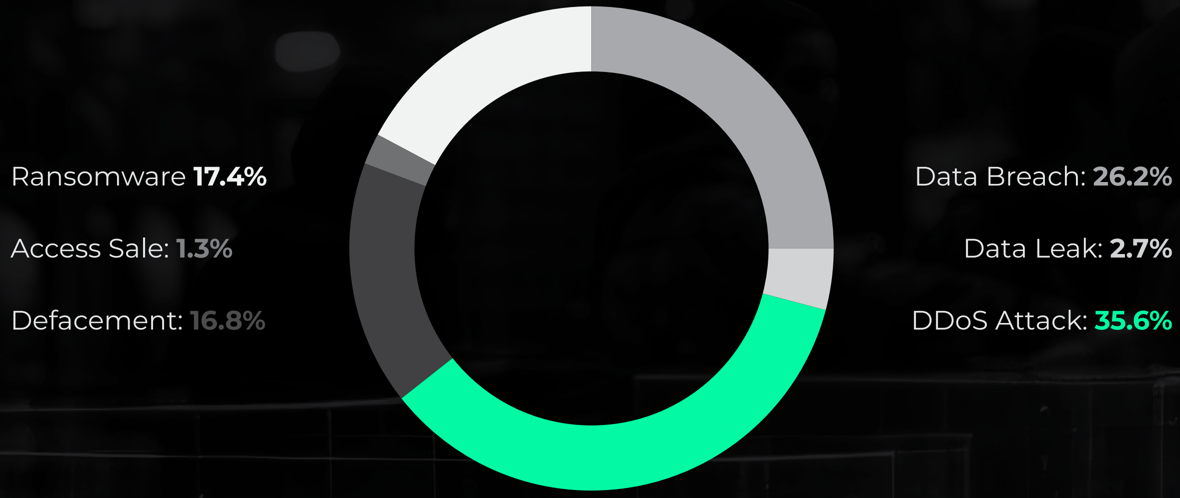


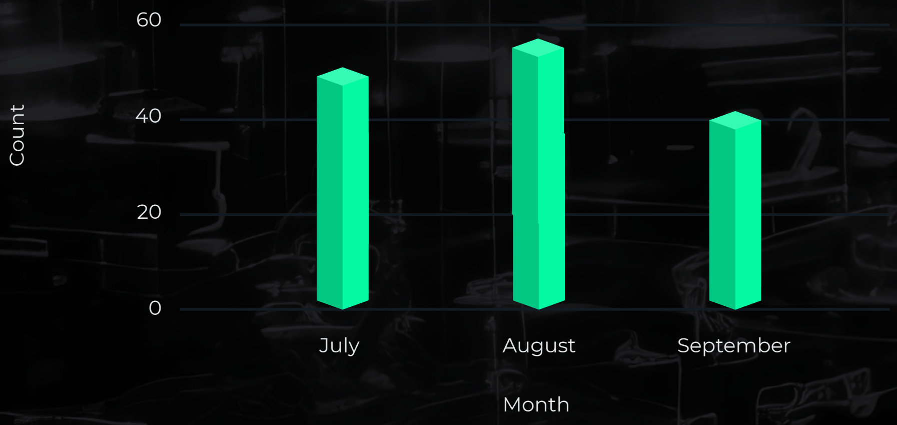
Countries analyzed : Australia, Canada, Chile, China, Indonesia, Japan, Malaysia, Mexico, New Zealand, Peru, Philippines, Russia, Singapore, South Korea, Taiwan, Thailand, USA and Vietnam.

AFRICA

Total Incidents (Q3): 149

Key Observations: Morocco, **Algeria** and **South Africa** were the most affected, with incidents largely driven by **data breaches** and **DDoS Attack.** The **Government**, **Financial** and **Technology** sector was primarily targeted during this period. Ransomware has recorded 26 incidents with heightened activity during august. DARKVAULT (3 incidents), HUNTERS INTERNATIONAL (3 incidents) and Kill Security (3 incidents) were the most active ransomware groups in this region.





Countries analyzed : Algeria, Angola, Burkina Faso, Cameroon, Chad, Djibouti, Ethiopia, Ghana, Ivory Coast, Kenya, Libya, Mauritius, Morocco, Mozambique, Namibia, Nigeria, Republic of the Congo, Rwanda, Senegal, Seychelles, Somalia, South Africa, Tanzania, Tunisia, Uganda, Zambia and Zimbabwe

KEY INSIGHTS AND TRENDS

Key Insights and Trends

DDoS Attacks

DDoS attacks surged by **771 incidents** from Q2 to Q3, indicating a growing reliance on disruption-based tactics. Sectors such as **Government and Transportation** sectors were particularly affected.

Ransomware

Ransomware activity remained consistent, particularly in **Manufacturing, Construction, Business & Professional Services and Healthcare** Sector, which remain prime targets for ransomware groups.

Data Breaches

Data breaches saw a steady increase from **1,596** in Q2 to **1,892** in Q3, driven largely by the targeting of **Information Technology** and **Government & Public** Sector entities.

MOST ACTIVE RANSOMWARE GROUPS IN Q3

RansomHub

Incidents: 194

Overview: RansomHub, emerging in February 2024 as a Ransomware-as-a-Service (RaaS) group, quickly gained traction. It primarily targeted the USA, UK, and Australia, with a focus on the Manufacturing, Construction, and Consumer Services sectors.

LockBit 3.0

Incidents: 96

Overview: Despite a brief disruption in February 2024 due to Operation Cronos, LockBit 3.0 swiftly resumed operations. The group mainly targeted organizations in the USA, France, and UK, focusing on the Manufacturing, Business & Professional Services, Healthcare, and Technology & IT Services sectors.

PLAY

Incidents: 91

Overview: PLAY ransomware, active since 2022, operates as a RaaS group. It primarily targeted the USA and Canada, focusing on the Manufacturing and Construction sectors.

CONCLUSION AND RECOMMENDATIONS

The **FalconFeeds.io** platform played a crucial role in gathering and analyzing the intelligence that underpins this report. Its real-time threat intelligence allows for the timely detection of trends, emerging threats, and actionable insights, which are critical for any organization looking to protect its assets.

Recommendations

01. Leverage FalconFeeds.io for Proactive Threat Monitoring:

Organizations should utilize **FalconFeeds.io** to gain insights into emerging threats, allowing for proactive monitoring of potential attacks. With real-time alerts and access to underground forum intelligence, companies can stay ahead of cybercriminals

02.. Strengthen DDoS Defenses:

The rise in DDoS attacks necessitates advanced DDoS mitigation strategies. Continuous monitoring and rapid response plans are essential to minimize downtime and service disruption.

03.Enhance Data Security:

With **data breaches** continuing to rise, organizations
must implement stringent security measures, including encryption and access control, while leveraging platforms like **FalconFeeds.io** to monitor dark web activity for any compromised data.

04.Enhance Data Security:

Given the consistent threat of **ransomware**, especially in critical sectors like **government, Information Technology, manufacturing, healthcare** and **education,** businesses must invest in backup solutions, employee training, and incident response strategies to mitigate the impact of attacks.

For more information, contact

FALCONFEEDS.IO

Email: support@falconfeeds.io
Website: falconfeeds.io