HALL OF HACKS

cybermaterial.com

Powered by 911CYBER

Table of Contents

Introduction 3

Executive Summary 4

Inductees 5

Findings 6

The Good

Top Investments 7
Top M&As 8
Top Regulations 9
Top Judicial Actions 10

The Bad

Top Threat Actors 11
Top Threats 13
Top Exploited Vulnerabilities 14
Most Vulnerable Vendors 15

The Ugly

Top Victims 16
Most Affected Industries 17
Most Affected Regions 18
Top Legal Actions 19

Trend Landscape 20

The 'Hall of Hacks' report for July 2024 reveals important insights into the cybersecurity landscape, focusing on investments, emerging threats, and their effects on global digital defense strategies.

Introduction

This report analyzes cybersecurity incidents and trends from July 2024, organized into three categories: The Good, The Bad, and The Ugly, providing essential insights into the current landscape of digital security.

Key findings include:

The Good:

- **Top Investments:** Highlights the most significant investments in the cybersecurity field.
- **Top M&As:** Provides insights into noteworthy mergers and acquisitions within the cybersecurity sector.
- **Top Regulations:** Analyzes impactful cybersecurity policies and regulatory developments.
- **Top Judicial Actions:** Profiles key apprehensions and legal actions against cybercriminals.

The Bad:

- **Top Threat Actors:** Identifies prominent threat actors responsible for cybersecurity incidents.
- **Top Threats:** Details the most prevalent and disruptive cybersecurity threats observed.
- **Top Exploited Vulnerabilities:** Reviews the most important known exploited vulnerabilities reported during the month.
- **Most Vulnerable Vendors:** Highlights vendors that have the highest number of reported vulnerabilities in their products.

The Ugly:

- **Top Victims:** Profiles organizations and entities most severely affected by cyber incidents.
- **Most Affected Industries:** Analyzes industries disproportionately impacted by cyberattacks.
- **Most Affected Regions:** Provides insights into geographic areas experiencing heightened cyber activity.
- **Top Legal Actions:** Summarizes significant legal actions and regulatory responses related to cybersecurity breaches

Our Goal

This report aims to provide readers with actionable insights to enhance cybersecurity resilience and mitigate risks effectively in an increasingly complex digital landscape.

Executive Summary

July 2024 proved to be another eventful month in cybersecurity, featuring a mix of positive, negative, and alarming incidents. These occurrences led to some notable additions that solidified their positions in our **Hall of Hacks**.

On the good side, Atos secured the largest investment of $1.6B. Additionally, Arieli EL to acquires a 59.1% stake in Elron Ventures, a leading cybersecurity and B2B software holding company. US Senate passed landmark bill enhancing children's online safety and privacy. Meanwhile, the UK Police arrested a 17-Year-Old for his role in the MGM Resort ransomware attack, member of Scattered Spider Ransomware Gang.

On the bad side, there was a surge in ransomware attacks, with AlphV/BlackCat gang with the most attacks. DarkGate, AsyncRAT, Remcos RAT and NOOPDOOR were the most active malware with 2 occurrences each. ServiceNow had the most critical vulnerability CVE-2024-5217, while Microsoft was found to be the most vulnerable vendor, reporting 143 CVEs.

On the ugly side, 33M phone numbers from Twilio's' customers were compromised. The Healthcare industry was recorded to be the most impacted by cyber attacks with 53 reported incidents. Once again, the US was the most targeted country with 252 major incidents out of 331. And in one of the most notable legal cases, Meta reached a settlement agreement with the State of Texas totaling $1.4 billion over the unauthorized use of facial recognition technology.

July 2024 brought both progress and challenges to the cybersecurity landscape. While major investments and legal actions marked key advancements, persistent threats and widespread data breaches underscored the urgent need for stronger security measures.

INDUCTEES

Top Investment

ATOS

$1.6 Billion

Top M&A

Elron Ventures

$53.2M

Top Regulation

KOPSA

Kids Online Safety and Privacy Act - USA

Top Judicial Action

17-yeard old member of Scattered Spider

Arrested

Top Threat Actor

Alphv/BlackCat

Most Active

Top Threat

DarkGate

Most Active

Top Vulnerability

CVE-2024-5217

Highest CVSS score

Most Vulnerable Vendor

Microsoft

Most CVEs

Top Victim

Twilio

33 million

Most Affected Industry

Healthcare

Most Incidents

Most Affected Country

USA

Most Targeted

Top Legal Action

META

$1.4B Settlement

Findings

CyberMaterial has gathered, curated, and analyzed thousands of articles related to cybersecurity from media outlets, government agencies, companies, and other cybersecurity organizations worldwide in July 2024.

This is what we found:

CYBER INCIDENTS

331

THREAT ALERTS

235

VULNERABILITIES

1250

KNOWN EXPLOITED VULNERABILITIES

8

MALICIOUS CAMPAIGNS

26

ACTIVE MALWARE

57

NEW MALWARE

30

NEW THREAT ACTOR

7

ACTIVE THREAT ACTORS

27

APTs

11

RANSOMWARE GANGS

11

INVESTMENTS

17

LEGAL ACTIONS

31

REGULATIONS

22

Top Investments

In July 2024, the cybersecurity sector saw substantial investment activity, underscoring the urgent demand for advanced security solutions. Notable funding rounds included Series C investments for Odaseva and Vanta, aimed at enhancing data security and AI capabilities, respectively.

Atos secured €1.675 billion in financing amid a debt restructuring, emphasizing the company's commitment to strengthening its cybersecurity offerings. New startups like Command Zero and Sola Security gained traction with their innovative approaches to investigations and emerging security needs.

Insight

This wave of funding highlights a diverse range of initiatives targeting critical cybersecurity challenges, from crisis management to software supply chain vulnerabilities.

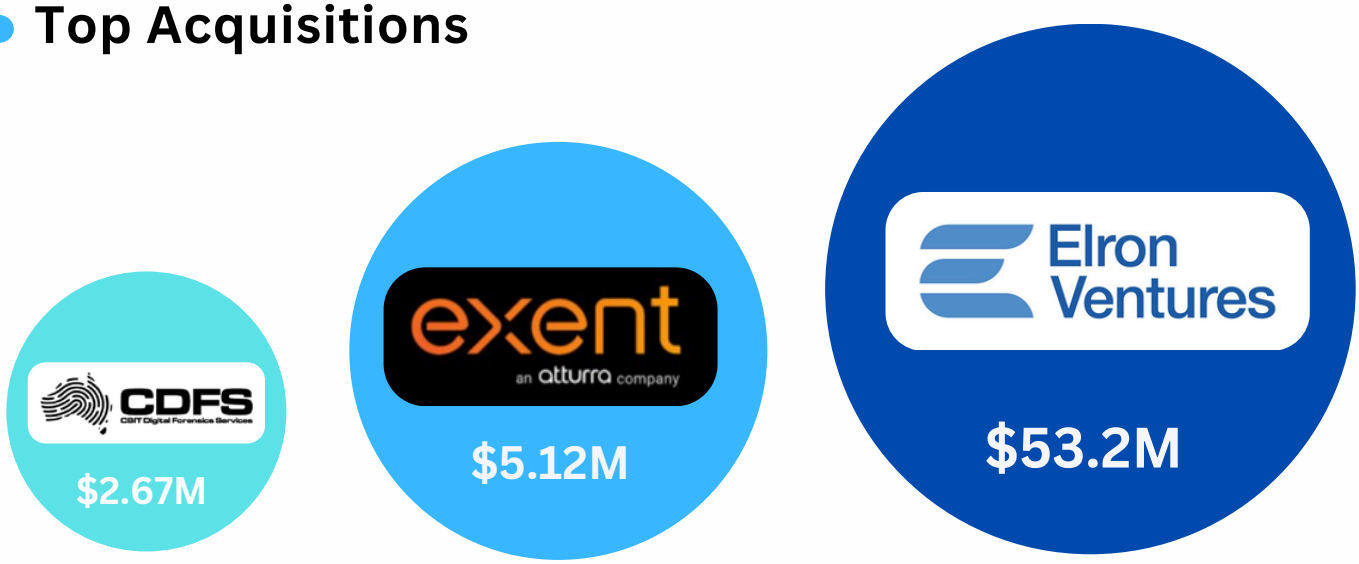
Top M&As

Notable acquisitions in the cybersecurity sector highlight a trend of companies enhancing their capabilities and services. Northamber, SIXGEN, and Marlink have expanded their cybersecurity reach through strategic acquisitions, while companies like Sony and Consensys are entering new markets with acquisitions focused on cryptocurrency and security solutions.

Other important moves include Accenture acquiring True North Solutions for energy safety and Bell enhancing its cybersecurity capabilities with the acquisitions of Stratejm and CloudKettle.

Additionally, firms like Arieli EL are investing significantly to boost cybersecurity innovation, underscoring the growing importance of security across various industries. Overall, these acquisitions reflect a proactive approach to addressing the evolving cybersecurity landscape and enhancing service offerings.

Top Acquisitions



Insight

The recent surge in cybersecurity acquisitions highlights a strategic focus on enhancing security capabilities and expanding into new markets. Organizations are proactively addressing growing cyber threats and diversifying their service offerings to meet client demands. This trend emphasizes the importance of innovation and adaptability in navigating the complexities of the modern cybersecurity landscape.

Top Regulations

Amendment

Act on the Protection of Personal Information (APPI)

Japan's Personal Information Protection Commission

Japan reviews personal information protection law with public input

Bill

S. 4630

United States Congress

New Act aims to unify cybersecurity regulations across the United States

Guideline

General Data Protection Act

Brazil's National Data Protection Authority (ANPD)

Brazil outlines new Data Protection Rules under resolution 18

Law

Kids Online Safety and Privacy Act (KOPSA)

United States Senate

US Senate passes landmark bill enhancing children's online safety and privacy

Executive Order

Executive Order 14110

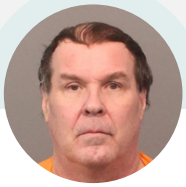
U.S. Department of the Treasury

This proposed rule sets forth regulations that would implement Executive Order 14105 of August 9, 2023, "Addressing United States Investments in Certain National Security Technologies and Products in Countries of Concern"

Top Judicial Actions

Global law enforcement agencies took significant action against cybercrime and fraud. Indonesian authorities arrested over 100 foreigners in Bali for cyber fraud, while international operations dismantled elderly fraud schemes and shut down 600 illicit Cobalt Strike servers.

High-profile convictions included Outcome Health executives sentenced for defrauding clients, and a Nevada man given 65 years for child exploitation. Additionally, arrests targeted the LockBit ransomware group, North Korean ransomware conspirators, and Russian hackers attacking critical infrastructure. These efforts underscore growing international cooperation in combating digital threats.



James Patrick Burns

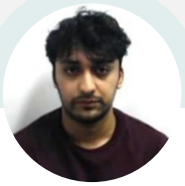
Distributing child sexual abuse material
65 Years

Sentenced

17-yeard old member of Scattered Spider

Suspected of being involved in the MGM Resorts attack

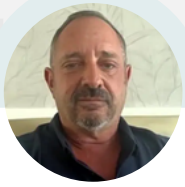
Arrested



Amar Tagore

Selling Malware Used in DDoS Attacks

Jailed



Andrew Left

$16M market manipulation scheme

Indicted

Ruslan Astamirov
Mikhail Vasiliev

Involvement in the **LockBit** ransomware group

Guilty

Amin Timovich Stigal

Targeted the Ukrainian cyber infrastructure

Wanted

Top Threat Actors

In July, the cybersecurity sector witnessed the emergence of numerous threat actors. Notable APTs included APT29, APT36, and APT44, alongside with ransomware groups like LockBit, BlackSuit, 8Base, and Alphv/BlackCat. Significant players such as ShinyHunters, DragonForce, Cyber Army, and the Medusa Gang also made headlines.

Additionally, new threat actors emerged, including Volcano Demon, ObamaCare, michupa, CloudSorcerer, CRYSTALRAY, CyberDragon, and emo, indicating a dynamic and evolving threat environment.

CYBERCRIMINALS

19 Entries

ShinyHunters - 888 - ObamaCare - michupa - OilAlpha - CRYSTALRAY - TAG-100 - GhostEmperor - MirrorFace - emo - Revolver Rabbit - PINEAPPLE - FLUXROOT - Vigorish Viper - Stargazer Goblin - Chinese Smishing Triad - Cyber Anarchy Squad - Bloody Wolf

STATE SPONSORED ACTORS

3 Entries

MuddyWater - Velvet Ant Group - UAC-0057

APTs

14 Entries

APT29 - APT36 - APT43 - APT44 - Void Banshee - APT41 - APT-C-09 - Evasive Panda - APT45 - T-APT-04 - Void Banshee - APT10 - CloudSorcerer

HACKTIVISTS

5 Entries

DragonForce - Team ARXU - CyberDragon - Cyber Army of Russia - Zeus Group

RANSOMWARE GROUPS

18 Entries

Lockbit - 8Base - Ransomhub - BlackSuit - Volcano Demon - 8Base - Medusa Gang - APT INC (SEXi) - Play - Alphv/BlackCat - Akira - RA World

Most Active Ransomware Group

Alphv/BlackCat

BlackCat/ALPHV emerged in late 2021 and quickly gained notoriety for its sophisticated Ransomware-as-a-Service (RaaS) platform. The group is particularly adept at evading security tools and has become one of the most active ransomware families.

Top Threat Actors

1 China
GhostEmperor
APT41
MirrorFace
Velvet Ant Group
Vigorish Viper
Evasive Panda
Chinese Smishing Triad
APT10

2 Russia
APT29
APT44
CyberDragon
Cyber Army of Russia

3 North Korea
APT43
APT45

4 Belarus
UAC-0057

5 Iran
MuddyWater

New Threat Actor

ObamaCare

The threat actor known as "ObamaCare" has gained notoriety within the cybercriminal community for orchestrating significant data breaches and password compilations. Operating on platforms like BreachForums, ObamaCare is credited with the release of RockYou2024, a massive collection of nearly 10 billion plaintext passwords.

This password compilation, which built upon the infamous RockYou2021 breach, highlights the threat actor's capability to gather, refine, and distribute vast amounts of sensitive data. The scale of this breach positions ObamaCare as a prominent figure in the dark web's thriving trade of stolen information.

Top Threats

Top Malware

*Entries

2* **DarkGate**

Darkgate is a multifunction malware active since December 2017 which combines ransomware, credential stealing, and RAT and cryptomining abilities.

2 **AsyncRAT**

AsyncRAT has emerged as a formidable player since its release in 2019. This remote access trojan (RAT) has gained notoriety for its dual capabilities

2 **Remcos RAT**

Remcos is a RAT that first appeared in the wild in 2016. Remcos distributes itself through malicious Microsoft Office documents

2 **NOOPDOOR**

NOOPDOOR, has recently gained notoriety for its sophisticated techniques and alarming effectiveness in infiltrating target networks.

New Malware

Xctdoor
DeerStealer
MadMxShell
PGoShell
BugSleep

Ongoing Malicious Campaigns

01 **GTA VI Beta Scam**

GTA VI Beta Version Download scam from sponsored Facebook ads includes malware

02 **Russian Disinformation Campaign**

A network of Russia-based websites acting as American newspapers with fake stories targeting the US election

03 **Apple Spyware Attack**

Apple Issues New Spyware Attack Warning To iPhone Users

04 **ERIAKOS**

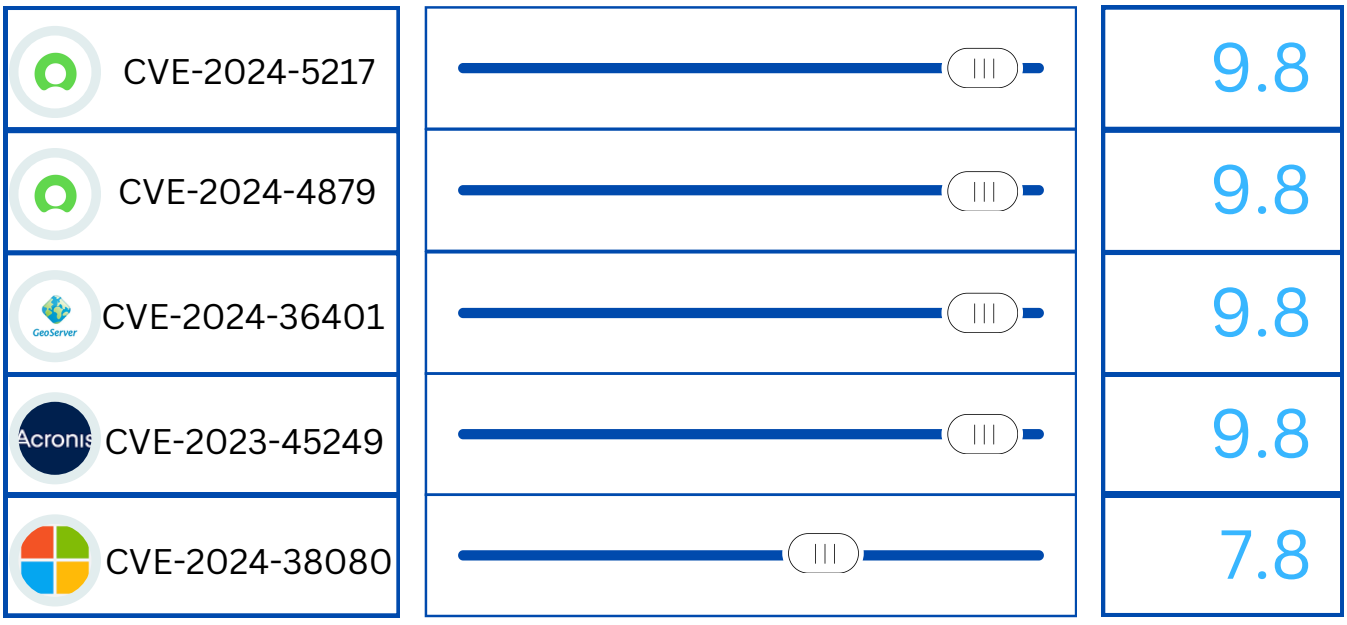
Scam e-commerce network, named the "ERIAKOS" campaign, targeting Facebook users. Involves 608 fraudulent websites .

Top Exploited Vulnerabilities

Critical vulnerabilities have been addressed across various platforms. **ServiceNow** has patched an input validation flaw in its Washington DC, Vancouver, and earlier Now Platform releases, which could allow unauthenticated users to execute code remotely. Customers are advised to apply the latest patches and hotfixes immediately to secure their instances.

GeoServer, prior to versions 2.23.6, 2.24.4, and 2.25.2, contained a Remote Code Execution (RCE) vulnerability, exposing all instances due to unsafe evaluation of XPath expressions. A patch is now available, along with a workaround that removes the vulnerable component, though this may disrupt functionality.

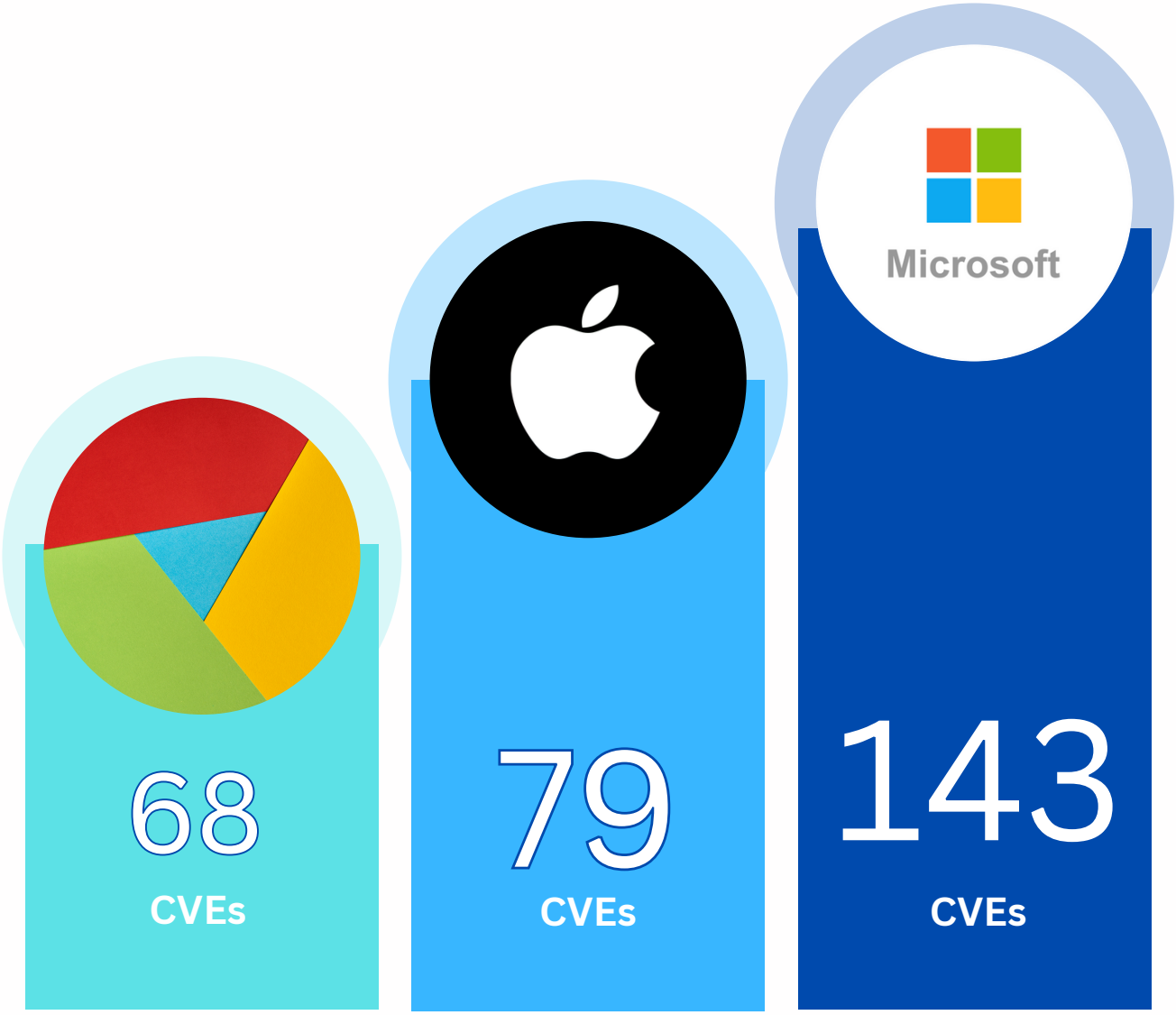
Additionally, **Acronis Cyber Infrastructure** and **Windows** platforms have resolved significant security risks, including vulnerabilities related to default passwords and privilege elevation, respectively. Applying the recommended updates is crucial to ensure system security



Most Vulnerable Vendors

In July, the top vendors with the highest number of Common Vulnerabilities and Exposures (CVEs) were Microsoft, Apple, and Google. Microsoft led the list with 143 reported vulnerabilities, followed by Apple with 79, and Google with 68.

These figures highlight the ongoing security challenges faced by major technology providers as they work to address vulnerabilities and protect users from potential threats.

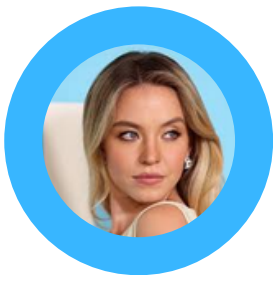


Top Victims

Truecaller, along with X (Twitter) and Twilio, have come under scrutiny due to significant data breaches affecting millions of users. These breaches exposed the personal information of 273 million Indian users, 200 million global user records and including 33 million phone numbers. Additionally, 39 million legal records were compromised, raising serious concerns about data security and privacy across these platforms.

Other notable incidents include Vivamax, which reported an impressive 6.8 million subscribers, and the Karafs Fitness App leak that compromised the sensitive data of over five million users. Additionally, actress Sydney Sweeney was targeted in a SIM-swap attack connected to a fraudulent cryptocurrency scheme. In another serious incident, Iseto Corporation experienced a ransomware attack that exposed 900,000 personal records, while SunExpress suffered a data breach that revealed nearly two million email addresses. These events highlight the urgent need for robust security measures across the industry.

Truecaller	**273 million** Indian users personal information
X (Twitter)	**200 millions** users records
Rapid Legal	**39 million** legal records
Twillio	**33 million** users phone numbers



SYDNEY SWEENEY

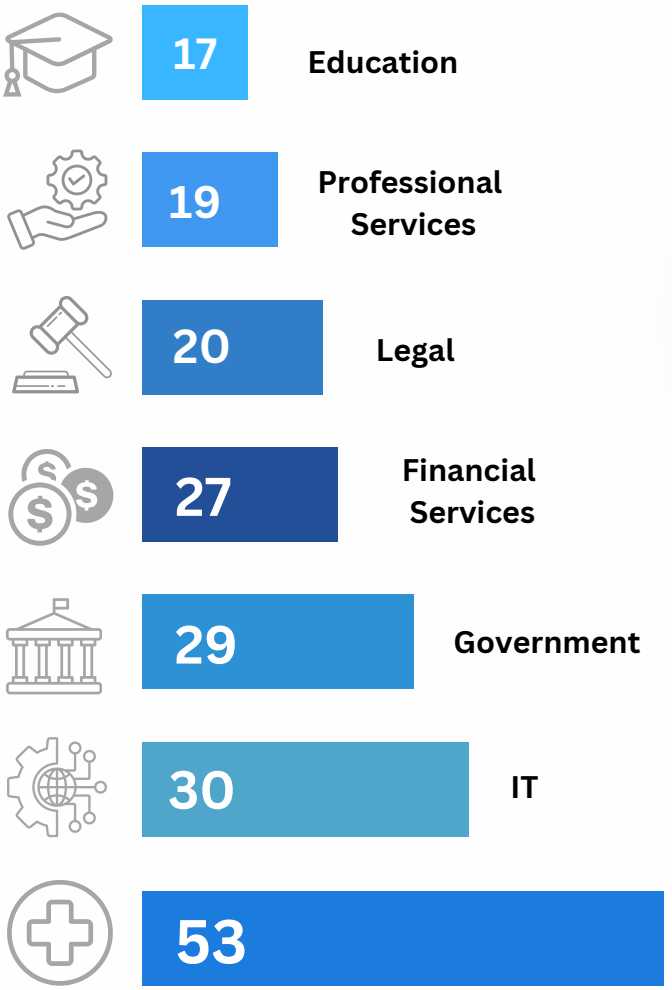
TARGETED IN A SIM-SWAP ATTACK

CONNECTED TO A FRAUDULENT CRYPTOCURRENCY SCHEME ON TWITTER

Most Affected Industries

This month cybersecurity incident analysis highlights considerable disparities across sectors, with healthcare at the forefront, reporting 53 incidents. IT follows with 30 incidents, underscoring the vulnerability of industries relying heavily on digital infrastructure. Government agencies reported 29 incidents, showcasing the ongoing challenge of protecting sensitive public sector data. Professional services (19) and financial services (27) also face notable exposure, reflecting the broader trend of cybercriminals targeting high-value data.

Healthcare remains a top target due to the wealth of sensitive patient information, with ransomware attacks being particularly prevalent. The IT, financial, and government sectors are also increasingly vulnerable, with a surge in phishing campaigns, cloud service attacks, and espionage attempts. Additionally, cryptocurrency and industrial sectors are seeing a rise in sophisticated attacks, reflecting the evolving strategies of threat actors looking for new avenues to exploit.



Insight

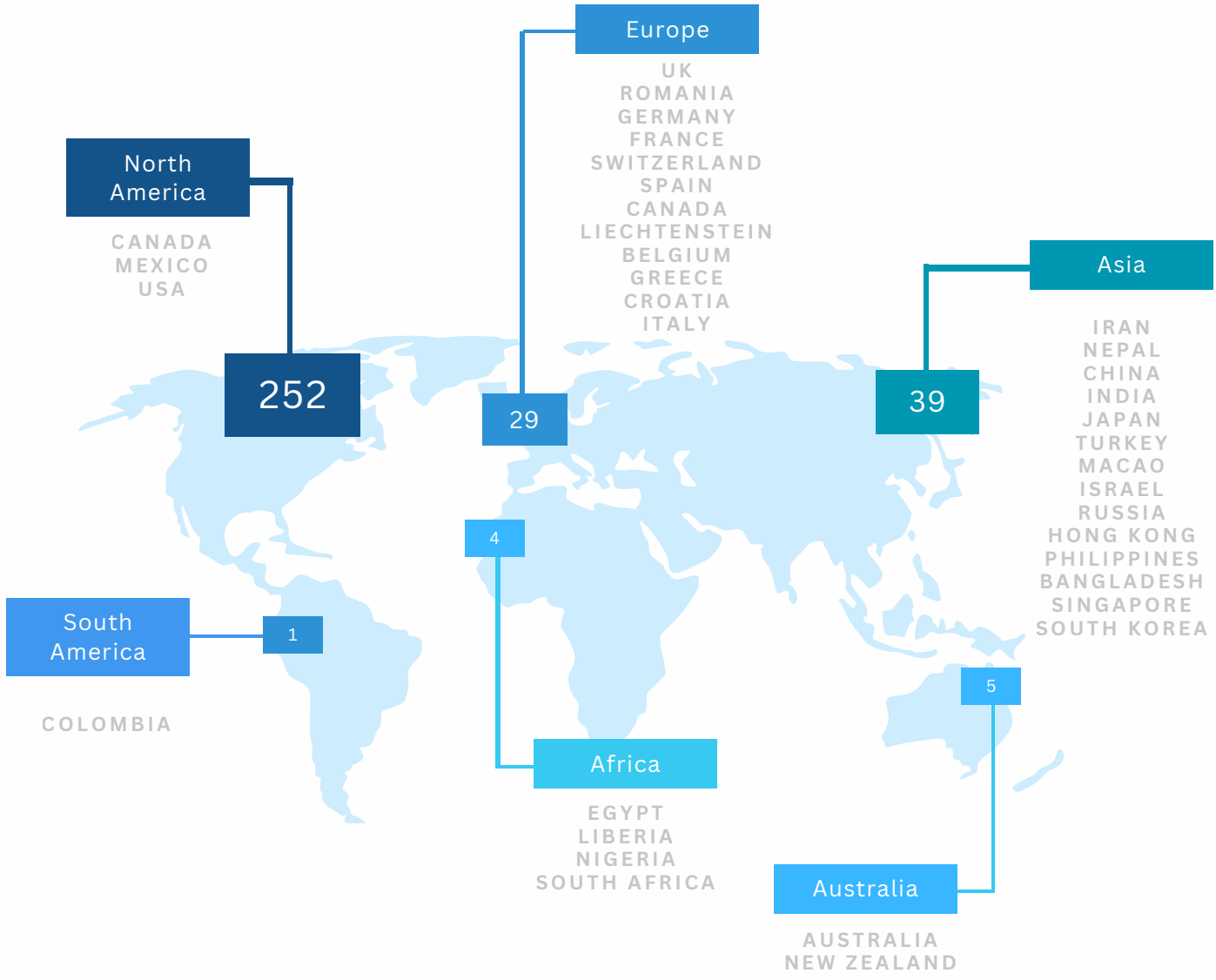
This month's cybersecurity incident analysis highlights a significant trend in cyber attacks across sectors, with healthcare remaining the most targeted industry.

These attacks stems from the sector's rich repository of sensitive patient data, making it a prime target for cybercriminals, especially for ransomware attacks.

Most Affected Regions

Map of 331 analyzed incidents

GLOBALLY



Insight

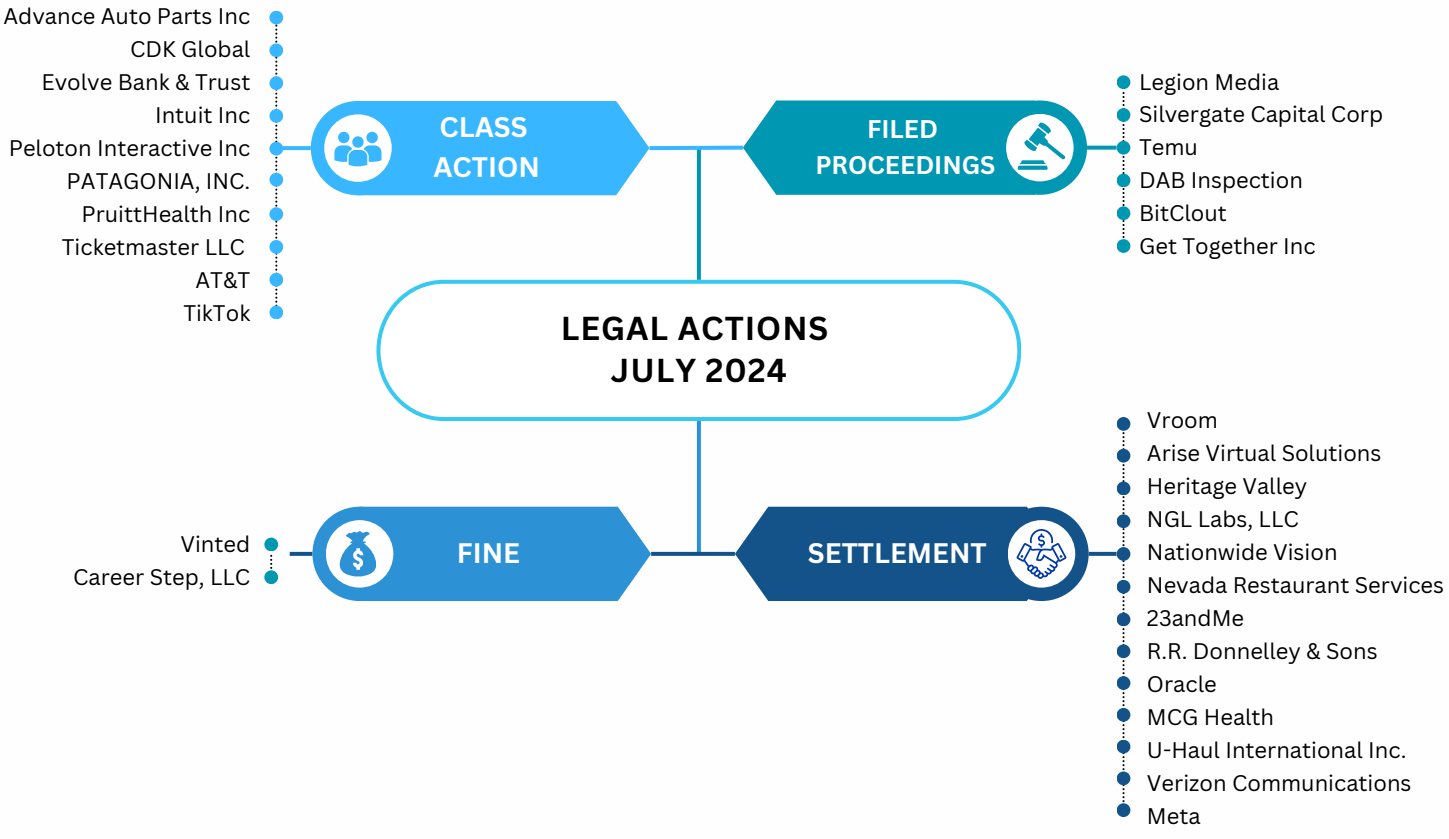
Out of the **331** incidents analyzed, **1** was deemed to have a global impact.

The North America region emerged as the most affected, with the United States being the primary target.

Top Legal Actions

Legal actions involving various companies highlight ongoing concerns related to data breaches, consumer fraud, and data privacy violations. In a significant class action lawsuit, **Advance Auto Parts** faced allegations of exposing employee information due to a data breach, while **Intuit** was also under scrutiny for a **TurboTax** data breach. Additionally, **Evolve Bank & Trust and CDK Global** were hit with lawsuits concerning inadequate data security measures. The Federal Trade Commission (FTC) took action against several companies for deceptive practices, including **Vroom**, which settled for $1 million over fraudulent activities, and **Arise Virtual Solutions**, which faced a $7 million settlement for misleading earnings claims.

The Securities and Exchange Commission (SEC) charged **Silvergate Capital Corporation** with misleading investors and secured settlements with companies like **R.R. Donnelley & Sons** for $2.1 million following a cyberattack. In another notable case, **Meta** agreed to a $1.4 billion settlement related to unauthorized facial recognition practices in Texas. These actions reflect a broader trend of increased scrutiny against companies that fail to adequately protect consumer data and uphold ethical practices. As organizations face legal challenges, the emphasis on data security and transparency remains critical in restoring public trust.



Trend Landscape

This trend landscape highlights the most relevant names in the cybersecurity sector for July 2024.

HALL OF HACKS

This report was prepared by:

Marc Raphael

Sofia Visciglia

Nicolas Peña

Ritu Choudhary

Varun Chandran

Arup Roy

Prapti Pal

Visit cybermaterial.com/hall-of-hacks

Powered by

911CYBER

https://911cyber.app