ThreatMon
Under Cyber Wings

2024

GLOBAL CYBER THREAT REPORT

EXECUTIVE SUMMARY & KEY FINDINGS

ThreatMon's 2024 Global Cyber Threat Report analyzes the global threat landscape, offering a comprehensive overview of the most significant cyber threats and trends observed throughout the year. The analysis reveals a notable escalation in dark web activities, ransomware attacks, and data breaches across various sectors globally. Technology, healthcare, and finance sectors were among the most targeted, with technology facing the highest volume of ransomware attacks. Meanwhile, the healthcare and finance sectors experienced a dramatic surge in data breaches, highlighting the critical importance of their operations and the value of their sensitive data.

ThreatMon's analysis leverages detailed data from active dark web forums, ransomware group activities, prominent threat actor operations, critical vulnerabilities, widely used malware, significant breaches, and millions of stealer logs to deliver insights into the global cyber threat landscape for 2024.

Below are the key insights included in this report:

- *The CrowdStrike IT meltdown in July disrupted 8.5 million devices globally, causing over $5 billion in damages across industries such as airlines and healthcare.*
- *The Salt Typhoon hack in December targeted U.S. telecom networks, compromising metadata to geolocate millions of Americans, including government and politically affiliated individuals.*
- *The "Mother of All Breaches" (MOAB) in January 2024 stands out as one of the largest data breaches in history, with an unprecedented exposure of more than 28 billion records.*
- *In May, a Snowflake data breach affected 165 companies as the threat actor UNC5537 exploited stolen credentials, emphasizing the need for secure supply chains and multi-factor authentication.*
- *Over 6,100 ransomware incidents were attributed to 95 distinct ransomware groups, with peaks in April and November.*
- *Active ransomware groups, including LockBit, RansomHub, and BlackCat, were responsible for the majority of ransomware incidents, with RansomHub leading with over 610 ransomware attacks.*
- *The United States was the most targeted country, accounting for 63% of global ransomware incidents.*
- *Healthcare and finance sectors experienced a significant increase in attacks, contributing to 20% of ransomware incidents.*
- *Data breaches in 2024 exposed more than 37 billion records, with the MOAB incident alone accounting for more than 28 billion records.*
- *The Change Healthcare breach in October exposed the personal and healthcare data of over 100 million individuals, marking it as one of the largest healthcare data breaches in recent years.*
- *ThreatMon detected more than 1,600 critical dark web incidents, with data leaks (37%) and data sales (34%) dominating activity.*
- *Threat actors increasingly targeted healthcare and finance sectors, exploiting outdated systems and third-party service vulnerabilities.*
- *Supply chain attacks, such as the Polyfill JS and Blue Yonder incidents, showed the need for securing third-party dependencies.*

TIMELINE OF INCIDENTS

Significant Cyber Incidents

January
Mother of All Breaches (MOAB)
Trello Data Breach

February
Bank of America Data Breach
Cencora Attack
Tangerine Telecom Attack
UnitedHealth Group Cyberattack

March
United Nations Development Programme Ransomware Attack
DDoS attack on French state websites

April
El Salvador's Chivo Wallet Attack

May
Snowflake Data Breach Incident

This year has been marked by a series of significant cyber incidents that have impacted various sectors globally. These events, ranging from large-scale data breaches to supply-chain attacks impacting more than hundreds of companies, show the increasing sophistication and impact of cyber threats. The following provides a summary of the most significant incidents during this time, offering insights into the shifting dynamics of the threat landscape.

Significant Cyber Incidents

June

Polyfill JS Attack

July

City of Columbus Ransomware Attack
CrowdStrike IT Meltdown
Disney Slack Data Breach

August

National Public Data Breach
Microchip Technology Ransomware Attack

September

BingX Cryptocurrency Platform Hack

October

Change Healthcare Data Breach

November

Change Healthcare Data Breach

December

Salt Typhoon Hack on U.S. Telecom Networks
Kawasaki Europe Cyberattack

December 2024

Salt Typhoon Hack on U.S. Telecom Networks: Salt Typhoon is a Chinese-backed hacking group that has infiltrated multiple U.S. telecommunications networks including AT&T, Verizon, and T-Mobile. Federal investigators first detected Salt Typhoon infiltrations in early December 2024 and identified unauthorized data-access events across nine major U.S. telecommunications networks. The hackers exploited vulnerabilities to access metadata, allowing them to geolocate millions of Americans through their cellphones and focus on government and politically affiliated individuals, particularly in Washington, D.C. In one notable incident, the group obtained credentials for an administrator account with access to over 100,000 routers and erased most activity logs, leaving insufficient data to assess the full extent of the breach.

Kawasaki Europe Cyberattack: In December 2024, the RansomHub ransomware group claimed responsibility for a cyberattack on Kawasaki Motors, alleging they had stolen nearly 500 GB of sensitive data. The stolen files reportedly include employee records, financial documents, customer data, and proprietary manufacturing information. RansomHub threatened to leak the data publicly if their ransom demands were not met and have already released portions on their dark web portal. Despite the breach, Kawasaki reported that it had successfully restored over 90% of its server functionality and resumed normal operations for dealers, business administration, and third- party suppliers such as logistics companies.

November 2024

Starbucks Third-Party Ransomware Incident:

In November 2024, Starbucks experienced significant operational disruptions following a ransomware attack on its third-party technology provider, Blue Yonder which is a supply chain management software company.

The Termite ransomware group claimed responsibility for the breach. The attack disrupted supply chain processes and forced Starbucks and other affected clients to revert to manual operations temporarily. While Starbucks confirmed that its systems were not directly breached, the incident caused delays in deliveries to stores, affecting inventory levels and daily operations. Investigations are ongoing as Starbucks works to manage the disruption, restore normal operations, and ensure minimal impact on its customers and business continuity.

October 2024

Change Healthcare Data Breach:

In October 2024, UnitedHealth Group confirmed that the February ransomware attack on Change Healthcare had exposed the personal and healthcare data of over 100 million individuals, marking it as the largest healthcare data breach in recent years. The stolen data included Social Security numbers, medical records, and billing information, affecting a substantial proportion of the U.S. population. The U.S. Department of Health and Human Services Office for Civil Rights officially recorded the breach, and UnitedHealth disclosed that the incident has incurred costs totalling $2.5 billion.

September 2024

BingX Cryptocurrency Platform Hack:

In September 2024, Singapore-based cryptocurrency exchange BingX suffered a significant security breach that resulted in the theft of approximately $44.7 million in digital assets. The attack targeted the platform's hot wallets and led to unauthorized transfers of funds. In response, BingX promptly implemented emergency measures, including transferring assets to cold wallets and temporarily suspending withdrawals to safeguard user funds. The company assured users that the losses were minimal and would be covered by BingX's capital reserves. Additionally, BingX has offered a substantial bounty for information leading to the recovery of the stolen assets or the identification of the attackers.

August 2024

Microchip Technology Ransomware Attack:

In August 2024, Microchip Technology Inc. fell victim to a ransomware attack organized by the Play hacking group, which resulted in a significant data breach and operational disruptions. The attackers reportedly exfiltrated sensitive data, later confirming its theft and demanding a ransom to prevent its release. Play has admitted to leaking the stolen data after Microchip Technology failed to meet their ransom demands within the set deadline. The leaked 4 GB archive reportedly contains personal information, client documents, and files related to budgets, payroll, accounting, contracts, taxes, and finances. The company disclosed in an SEC filing that the attack incurred a financial impact of $21.4 million to cover ransom payment and recovery costs.

National Public Data Breach:

In August 2024, National Public Data (NPD), a consumer data broker, suffered a significant data breach that exposed approximately 2.9 billion records containing sensitive personal information. The compromised data included the names, Social Security numbers, addresses, and phone numbers of individuals across the United States, the United Kingdom, and Canada.

The breach was performed by a hacker identified as "USDoD," who began selling the stolen data on the dark web for $3.5 million. NPD acknowledged the breach in August 2024, revealing that unauthorized access had been ongoing since December 2023.

July 2024

CrowdStrike IT Meltdown:

In July 2024, a flawed update from cybersecurity firm CrowdStrike triggered one of the largest IT outages in history, affecting approximately 8.5 million Microsoft Windows devices worldwide. The update corrupted critical Windows registry settings and led to widespread disruptions across sectors such as airlines, hospitals, and financial institutions. System failures, loss of functionality, and extended downtime for businesses relying on Windows environments compounded the impact. The financial toll was substantial, with U.S. Fortune 500 companies incurring more than $5 billion in losses, including $500 million reported by Delta Air Lines alone.

City of Columbus Ransomware Attack:

In July 2024, the City of Columbus, Ohio, became the target of a ransomware attack by the Rhysida ransomware gang which compromised the personal data of approximately 500,000 individuals. The attackers claimed to have stolen 6.5 TB of sensitive data, including employee credentials, city video camera feeds, server dumps, and other critical information. Following the city's refusal to pay the ransom, the gang began leaking portions of the stolen data on their dark web portal. The leaked information included thousands of documents and files containing highly sensitive material. The city confirmed that investigations and recovery efforts would require several months and could cost more than millions of dollars, making it one of the most impactful ransomware attacks on a U.S. municipality in recent years. Disney Slack Data Breach: In July 2024, Disney suffered a major data breach when a threat actor known as "NullBulge" infiltrated the company’s Slack platform, stealing 1.1 TB of sensitive data. The attacker claimed to have accessed all messages and files from nearly 10,000 Slack channels which expose details of upcoming projects, internal communications, and proprietary documents. Among the stolen files were more than 12,000 confidential spreadsheets containing critical corporate strategies and intellectual property. Following the breach, The Walt Disney Company announced it would no longer use Slack for internal communication.

June 2024

Polyfill JS Attack:

In June 2024, a significant supply chain attack occurred involving the popular Polyfill JS library. After the domain (cdn.polyfill.io) and the GitHub account of the library were acquired by a Chinese company, malware was injected into over 100,000 websites. This malware, exploiting the vulnerability CVE-2024-38526, targeted mobile devices, redirecting users to malicious sites and bypassing detection by delaying execution in the presence of web analytics services. Major actions taken include Cloudflare's real-time rewrites and Namecheap putting the domain on hold to prevent further exploitation of the vulnerability.

May 2024

Snowflake Data Breach Incident:

In May 2024, Snowflake experienced a significant data breach that affected more than hundreds of high-profile clients, including Ticketmaster and Santander. The threat actor behind the attack, UNC5537, exploited stolen customer credentials. The threat actors were able to log in to accounts that did not enable multi-factor authentication (MFA) to carry out the breach, which impacted over 165 companies. The breach resulted in the theft of data from potentially 30 million Santander customers and up to 560 million Ticketmaster users. The threat actor behind the hack used a tool named "RapeFlake" to exfiltrate data from Snowflake's databases and demanded ransom for the stolen data. Snowflake and Mandiant, who conducted the investigation, emphasized that the breaches resulted from compromised customer credentials rather than a vulnerability or misconfiguration in Snowflake’s platform. The investigation revealed that many affected accounts lacked MFA and had outdated credentials. In response, Snowflake issued guidance on enhancing security measures, including implementing MFA and network allow lists to restrict access to trusted locations.

April 2024

El Salvador's Chivo Wallet Attack:

In April 2024, El Salvador's Chivo Wallet, the government-operated Bitcoin wallet, suffered a major data breach by the hacker group CiberInteligenciaSV. The hackers released the wallet's source code and VPN credentials on the black hat forum BreachForums. Earlier in the same month, the same hacker group exposed the personal information of approximately 5.1 million Salvadorans, nearly the entire adult population. This earlier leak included full names, unique identity numbers, dates of birth, addresses, phone numbers, email addresses, and high- definition photos, totaling 144 GB of sensitive information. Both incidents have raised significant privacy concerns and highlighted the vulnerabilities in the Chivo Wallet's security.

March 2024

United Nations Development Programme Ransomware Attack:

In March 2024, the United Nations Development Programme (UNDP) suffered a ransomware attack by the 8Base ransomware gang, leading to the theft of sensitive data from its IT infrastructure in Copenhagen. The attack compromised approximately 100,000 records, including personal information of past and present personnel, procurement data, invoices, receipts, and confidential agreements. Despite the hackers' demands, UNDP confirmed no ransom was paid and has been notifying affected individuals and entities.

DDoS attack on French state websites:

In March 2024, the French government faced a severe distributed denial of service (DDoS) attack of unparalleled intensity, impacting over 17,000 IP addresses and devices. The pro- Russian hacktivist group Anonymous Sudan claimed responsibility for the attack. The DDoS attack disrupted several government websites and services for hours, prompting the French National Cybersecurity Agency (ANSSI) to activate a crisis cell to mitigate the damage. The attack is believed to be linked to France's political stance on Ukraine and the upcoming Paris Olympics.

February 2024

Bank of America Data Breach:

In February 2024, Bank of America announced a data breach that compromised the personal information of 57,000 customers. The breach occurred through a third-party vendor, Infosys McCamish Systems (IMS), which experienced a cyberattack in November 2023. The exposed data included names, addresses, Social Security numbers, dates of birth, and financial account details of customers with deferred compensation plans. The LockBit ransomware gang claimed responsibility for the attack.

Cencora Attack:

In February 2024, Cencora, a major pharmaceutical services provider formerly known as AmerisourceBergen, disclosed a cyberattack that resulted in the theft of sensitive personal information. The breach, which impacted at least 24 pharmaceutical and biotechnology companies, included sensitive data such as names, addresses, dates of birth, health diagnoses, and medication details of potentially hundreds of thousands of individuals. Over 540,000 individuals have been notified across several states, and the company is offering two years of free identity protection and credit monitoring services. No ransomware group has claimed responsibility for the hack.

Tangerine Telecom:

In February 2024, Tangerine Telecom was targeted by the BlackCat/ALPHV ransomware gang, leading to a breach that impacted 232,000 customers. The attackers accessed a legacy customer database using compromised login credentials from a contractor. Stolen data included full names, dates of birth, mobile and email addresses, postal addresses, and Tangerine account numbers. No financial or identity documents were leaked. The breach prompted Tangerine Telecom to pay a ransom to prevent public disclosure of the stolen data .

UnitedHealth Group Cyberattack:

In February 2024, UnitedHealth Group was hit by a ransomware attack from the BlackCat/ALPHV gang, leading to a $872 million loss. The attackers stole 6TB of sensitive data, including medical records, insurance records, and personally identifiable information of millions, including U.S. military personnel. UnitedHealth paid a ransom to prevent this data from being disclosed publicly. The attack disrupted services for over 70,000 pharmacies, revealing major security weaknesses in the healthcare sector.

January 2024

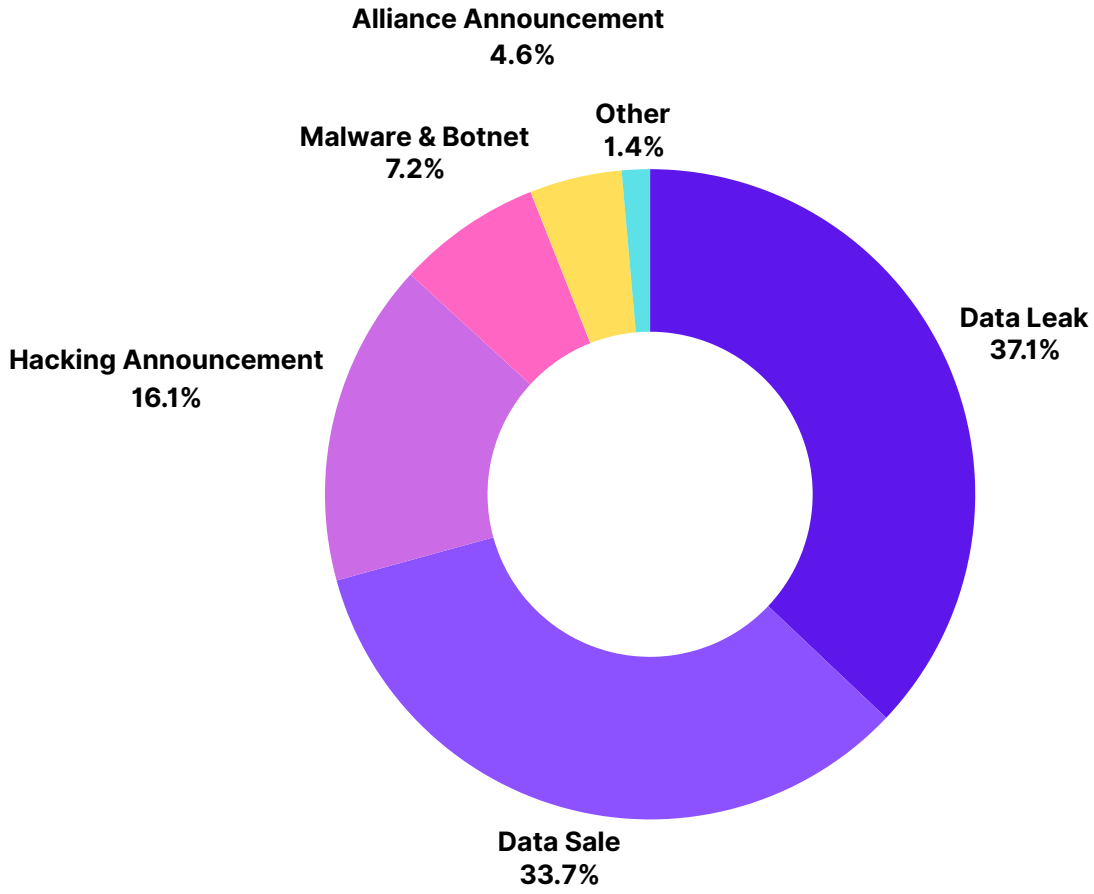
Mother of All Breaches (MOAB):

In January 2024, the "Mother of All Breaches" (MOAB) was discovered, exposing more than 28 billion records from a variety of sources, totalling 12 terabytes of data. The source of the breach remains unknown, with no one claiming responsibility. This breach included personal data from platforms like LinkedIn, Twitter, Adobe, and Tencent, with the latter contributing 1.4 billion records alone. The leaked data comprised a mix of past breach information and new, previously unseen data. This unprecedented exposure poses severe risks for identity theft, phishing, and other cybercrimes, affecting billions of accounts worldwide.

Trello Data Breach:

In January 2024, Trello suffered a data breach when a threat actor named "emo" exploited an exposed API, leading to the leak of personal information for over 15 million users. The compromised data, including emails, usernames, full names, and other account details, was listed for sale on a dark web forum. Trello's investigation revealed that the breach was due to web scraping, using email addresses from previous breaches to gather publicly accessible profile information, rather than a direct hack. Although no passwords were exposed, the leaked data poses risks for phishing and credential-stuffing attacks. Trello has since implemented measures to limit querying user-profiles and increased monitoring to prevent similar incidents

DARK WEB INSIGHTS



Threat actors extensively continued to use the dark web as a major hub for their malicious activities throughout 2024. In total, ThreatMon detected more than 1600 critical incidents on the dark web, including the sale of data from large-scale breaches, announcements of companies who were the victims of a ransomware incident, the distribution of newly developed malware and botnet variants, and other numerous malicious activities.

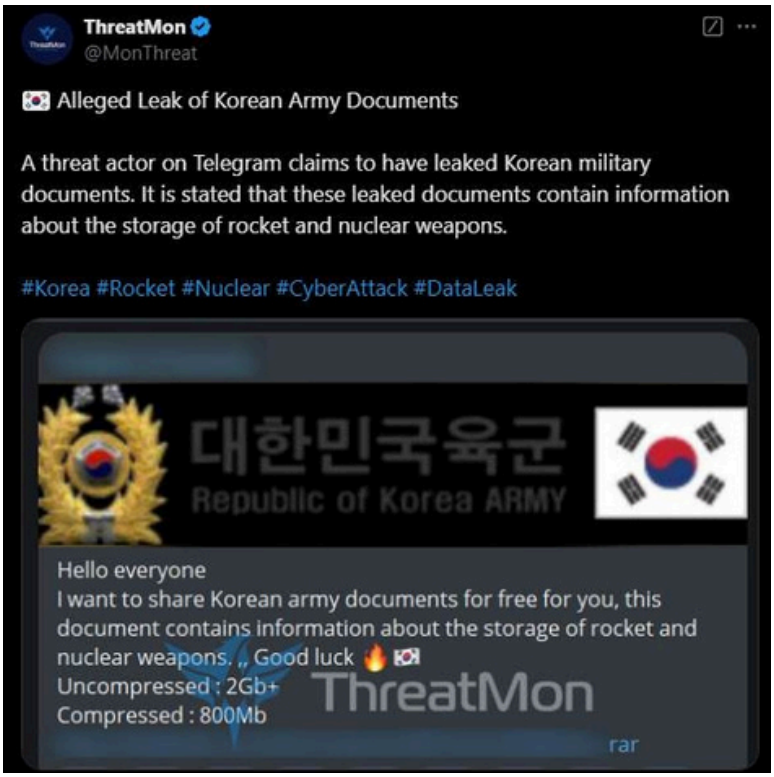
An analysis of the distribution of dark web posts by category reveals that data leaks were the most frequent post type, accounting for approximately 37.1% of all posts. These posts often claim to include highly sensitive information from various sectors such as finance, healthcare, nd government agencies, posing a high risk to companies in such sectors.

The high frequency of data leak posts highlights the necessity and importance of implementing robust cyber measures to protect sensitive data and mitigate the substantial risks posed by data breaches and their exploitation on the dark web.

Closely following, data sales emerge as the second most common category, comprising 33.7% of the total posts. These posts often involve the sale of stolen databases, personal identifiable information (PII), or corporate intelligence, and are frequently marketed to criminal enterprises or individual threat actors. The demand for these datasets is driven by the threat actors' utility in fraudulent activities, such as phishing campaigns and highly targeted cyberattacks. Combined, data leak and data sale posts highlight the dark web's central role in facilitating malicious activities and the urgent need for proactive cyber measures.

In particular, on November 13, ThreatMon detected and reported an alleged data leak involving confidential documents from the Korean military. A threat actor on Telegram claimed to have leaked sensitive documents containing details about the storage of rocket and nuclear weapons. In the Telegram message, the threat actor leaked the classified documents, free for anyone to access.

ThreatMon's X account @MonThreat posted a tweet on the social media platform X providing details about the alleged leak, including the Telegram message and the alleged contents of the documents. ThreatMon's X account consistently provides timely updates on critical cyber incidents and emerging threats within the cyber landscape.

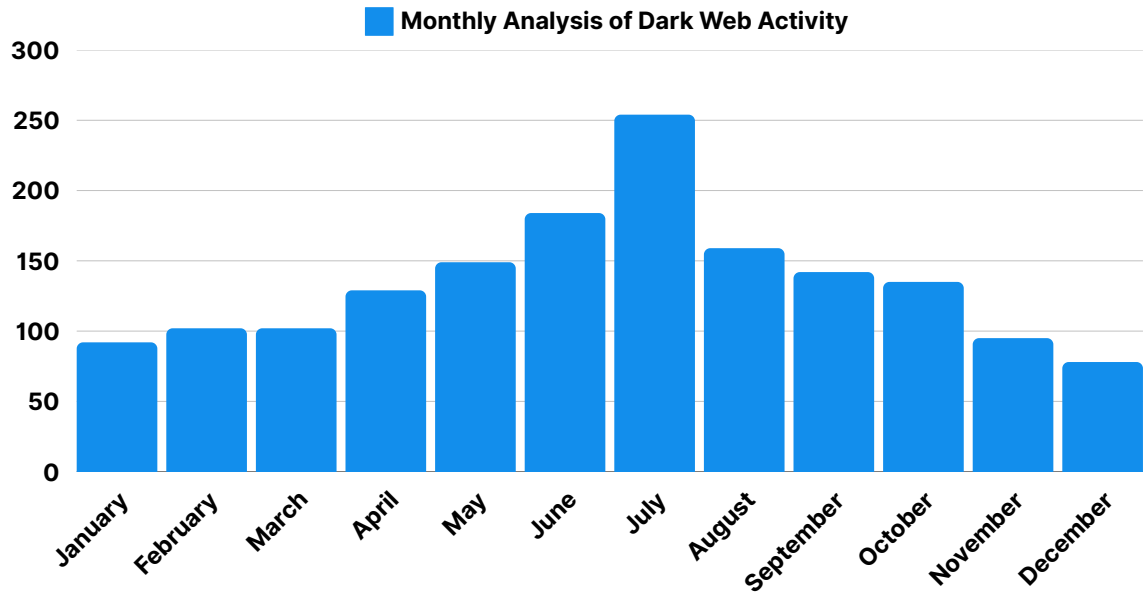


Following data leak and data sale posts, hacking announcements and malware & botnet sales were among the most notable dark web activities. Malware & botnet announcements and sale posts are especially significant because they often introduce new tools and techniques that enable threat actors to carry out their malicious cyber activities. These posts not only facilitate the dissemination of malicious software but also act as a marketplace for the development and exchange of cyber tools, further amplifying the scale and sophistication of cyber incidents.

In particular, on June 12, ThreatMon detected a significant dark web forum post announcing the update and return of the notorious Charon Android botnet. The botnet is an edited version of another infamous botnet called the Ermac botnet. The announcement post reveals that the botnet was rewritten from scratch to resolve chronic issues in the Ermac botnet and add additional features such as faster communication and new injects.

ThreatMon was the first to identify the botnet's announcement on a dark web forum. The discovery was shared on ThreatMon's X account @MonThreat, where a tweet was posted to inform the public about the detection of this botnet.

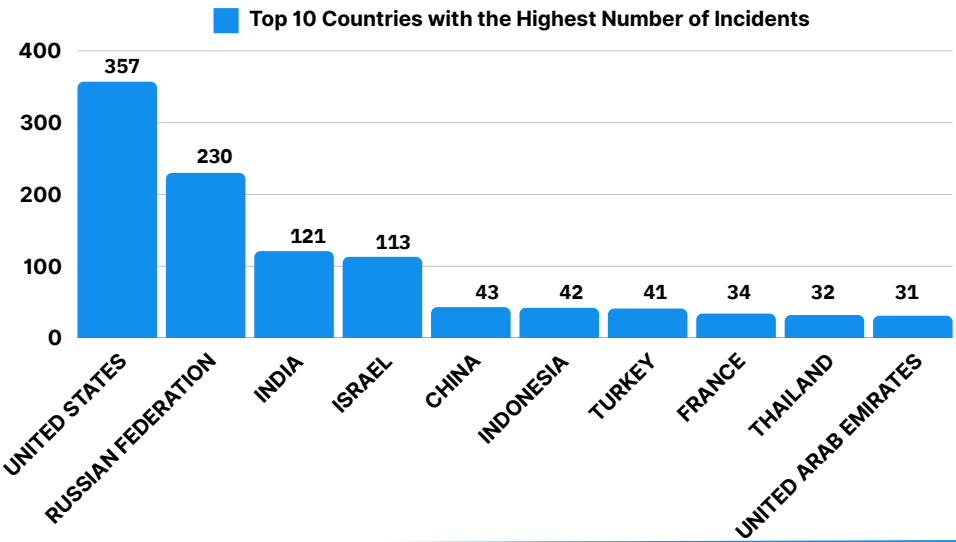
July Marks the Peak of Dark Web Activity in 2024



When analyzing the monthly activity on the dark web throughout 2024, a notable surge in incidents is observed, with July marking the peak of recorded activity. The number of incidents steadily increased from January to June, reaching more than 250 dark web posts in July, the highest monthly total for the year. This significant spike highlights an unprecedented level of cyber threat engagement during the mid-year period.

Following the July peak, dark web activity began to decline gradually, yet it remained consistently high in subsequent months, with August and September maintaining significant levels of incidents. High amounts of data leak and data sale posts throughout the year highlight the sustained demand for stolen information and sensitive data among threat actors. Such patterns emphasize the need for continuous monitoring and enhanced security measures to
address the evolving threats originating from the dark web.
Analysts at ThreatMon predict that this trend of heightened activity on the dark web will continue to pose significant challenges for organizations and individuals. As threat actors evolve their tactics and expand their operations, the dark web will remain a critical hub for the distribution of stolen data,malicious tools, and collaboration among cybercriminals.

The United States Leads in Dark Web Activity

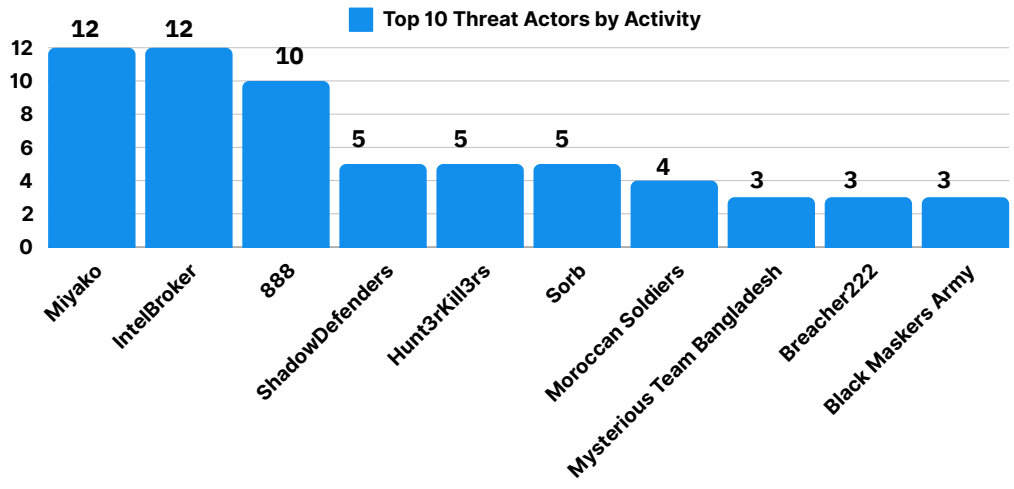


An analysis of the top 10 countries with the highest number of incidents on the Dark Web shows that the United States has the highest number of records with more than 350 incidents, indicating a significant concentration of the targeted activity. The Russian Federation comes next with 230 incidents, while India and Israel are in third and fourth place. Meanwhile, countries such as China, Indonesia, and Turkey have reported fewer incidents.

This uneven distribution suggests that a small group of nations bears the majority of Dark Web activity, highlighting the need for focused security efforts in those regions. However, areas with fewer reported incidents are not exempt from risk and should remain alert to prevent emerging threats from escalating.

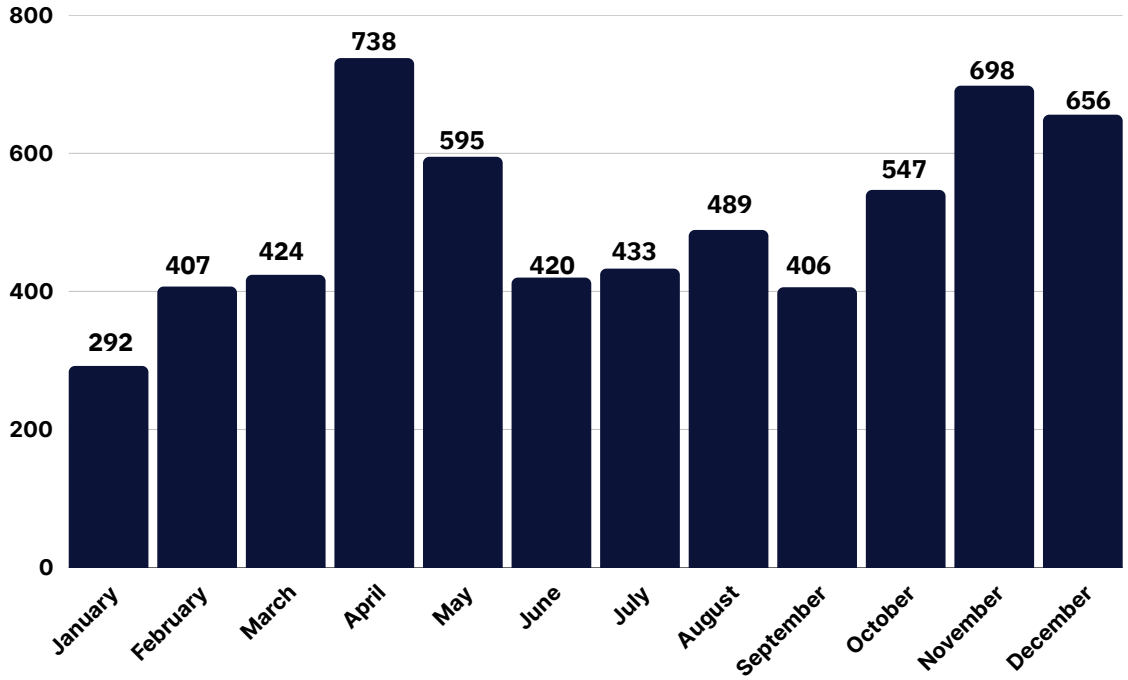
Top Threat Actors in 2024:

Miyako, IntelBroker, and 888 Lead the Rankings A closer look at the top 10 Dark Web threat actors reveals that miyako, whose activity has experienced a significant increase in recent months, and IntelBroker lead the rankings, while 888 follows closely. miyako is a highly advanced threat actor targeting critical infrastructure with cutting-edge cyber tools, driven by both financial and geopolitical motives. IntelBroker, on the other hand, has built a reputation for trading stolen data, frequently posting compromised credentials and sensitive information for sale. Although the remaining actors have fewer posts, their activities still demonstrate the broad range of threats that arise from the Dark Web.



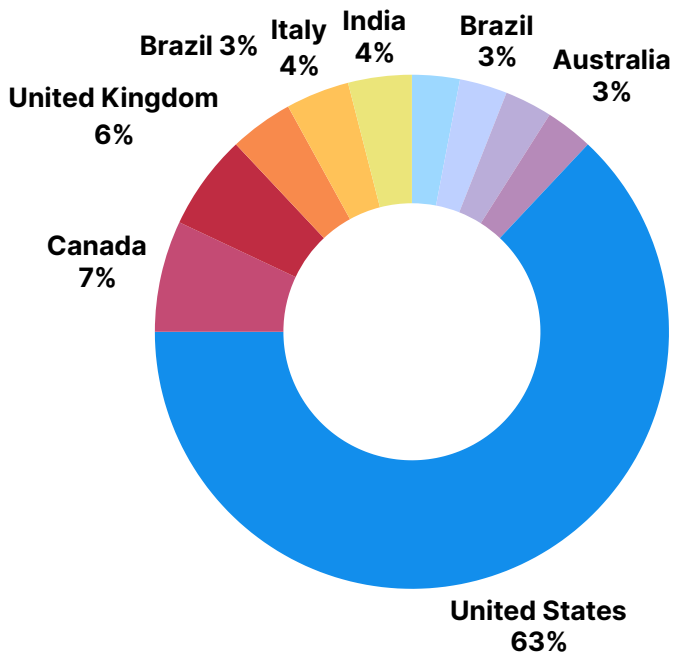
RANSOMWARE INCIDENTS

Ransomware attacks are a powerful tool for cybercriminals to extort substantial sums of money, disrupt critical operations, and further solidify their foothold in a rapidly evolving threat landscape. Throughout 2024, ransomware attacks continued to escalate in both frequency and sophistication, targeting organizations across all sectors and regions. Threat actors deployed numerous advanced tactics, such as double extortion and supply chain compromise, to maximize disruption and profit. In response, organizations found themselves racing to adopt more resilient cyber measures, yet many still fell victim to the evolving threat landscape. This section delves into the emerging ransomware trends of 2024, focusing on monthly incident patterns, country-level and sector-specific analyses, and providing an overview of the most active ransomware groups worldwide. Ransomware Peaks in April and November 2024 In 2024, ransomware groups remained highly active, with ThreatMon detecting over 6,100 ransomware incidents attributed to 95 distinct ransomware groups. These attacks significantly impacted both small and medium-sized businesses (SMBs) and large corporations, resulting in critical breaches, data leaks, and huge financial losses.



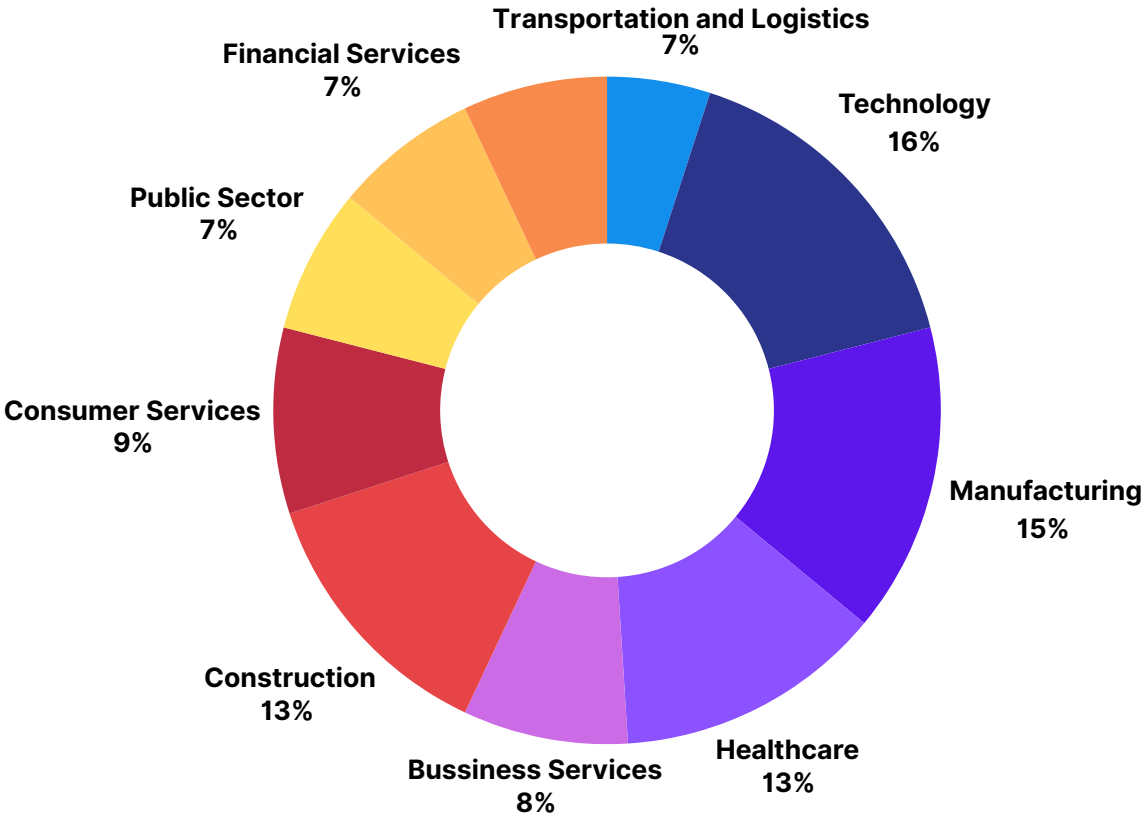
Throughout 2024, ransomware activity remained alarmingly high. More than 6,000 companies suffered the consequences of a ransomware attack, with some succumbing to significant financial losses, operational disruptions, and even permanent data loss. April recorded the highest volume of ransomware incidents, representing a peak in the number of critical incidents in this period. While April recorded the highest volume of ransomware incidents in 2024, the final two months of the year also experienced a marked increase in ransomware activity. Analysts at ThreatMon expect this increase in ransomware activity will persist into the first few months of 2025.

The United States Remains the Most Targeted Country in Ransomware Attacks An analysis of global ransomware incidents reveals that the United States tops the list with more than 2,600 reported cases, accounting for approximately 63% of all attacks. Canada follows with more than 270 cases (approximately 7%), while other impacted nations—such as the United Kingdom, Germany, and Italy—illustrate the worldwide reach of these cyber threats. Western countries collectively comprise 80% of the reported incidents, largely due to their
economic wealth and high-value digital assets. By contrast, nations in the MENA region and parts of Asia experience fewer such attacks, indicating a comparatively lower likelihood of being targeted.

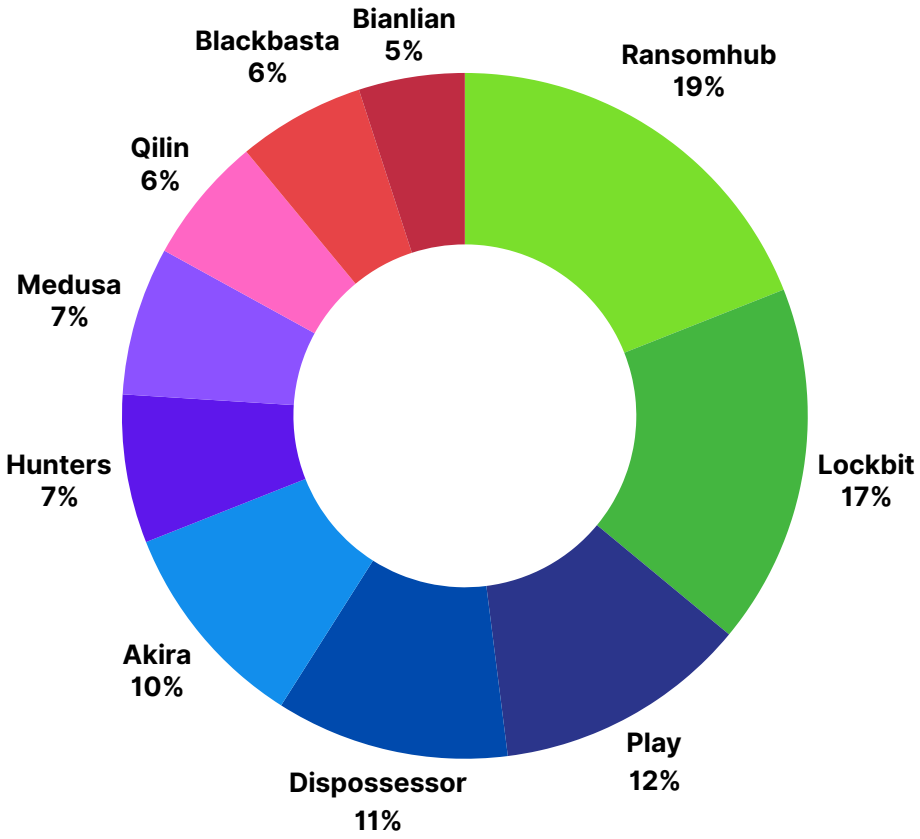


Unprecedented Increase of Attacks Targeting Finance and Healthcare Sectors

The distribution of ransomware incidents across multiple sectors reveals that the technology industry experienced the highest number of attacks, at 16%. Other affected sectors—such as manufacturing, construction, consumer services, and business services—further illustrate the broad scope of ransomware threats.
Compared to previous years, the rise in attacks on the healthcare and finance sectors demonstrates cybercriminals' growing focus on these critical industries. The healthcare sector, in particular, reported a concerning increase with more than 600 incidents (13% of the total), while the finance sector saw an alarming increase as well, accounting for 7% of all ransomware incidents.



Top Ransomware Groups:
LockBit, RansomHub, and Play Group Lead the Way



Analysis of threat actor activity shows a rise in ransomware incidents attributed to 95 distinct groups. Continuing its dominance, RansomHub remains the most active group, responsible for more than 600 reported attacks. RansomHub has primarily targeted the healthcare and education sectors, exploiting outdated systems. Close behind is LockBit, known for pervasive attacks spanning government entities and large enterprises. Its ability to adapt quickly and focus on high-value targets has established LockBit as a major threat in the cybersecurity landscape. Meanwhile, the Play group has carried out numerous high-profile attacks on financial institutions and major corporations. Collectively, these groups have significantly shaped the overall ransomware threat landscape.

Highlights

ThreatMon's Ransomware Monitoring account, @TMRansomMon, actively provides updates on significant ransomware incidents, ensuring that followers stay informed about the latest threats and breaches. Through 2024, ThreatMon reported many critical ransomware incidents, highlighting the widespread threat of ransomware across various sectors. Here are some of the most important incidents reported: Blue Yonder Group, Inc In November 2024, the Termite ransomware gang breached Blue Yonder, stealing 680 GB of data, including databases, emails, and documents. The attack disrupted operations for Starbucks and affected scheduling and payroll across over 10,000 stores. Additionally, the UK grocery chains Morrisons and Sainsbury's fresh food warehouse systems are disturbed. Termite has reportedly leaked samples of the stolen data to pressure Blue Yonder in December 2024.

Microchip Technology

In August 2024, Microchip Technology Inc. was targeted by the Play ransomware group, leading to a significant data breach and operational disruptions. The attackers exfiltrated 4 GB of sensitive data, including personal information, client documents, and financial records. Play leaked the data after Microchip failed to meet their ransom demands. The incident incurred $21.4 million in costs, covering ransom payments and recovery efforts, as disclosed in an SEC filing.

City of Columbus, Ohio

In July 2024, the Rhysida ransomware gang targeted Columbus, Ohio, stealing 6.5 TB of data affecting 500,000 individuals. Stolen data included employee credentials, video feeds, and sensitive files, with leaks starting after the city refused to pay. Recovery efforts are expected to take months and cost millions, marking it as one of the most impactful U.S. municipal ransomware attacks.

Foxsemicon Integrated Technology Inc.

ThreatMon also highlighted the ransomware attack on Foxsemicon Integrated Technology Inc., a subsidiary of Foxconn, in January 2024. The LockBit group claimed responsibility for this attack, during which they allegedly stole 5 terabytes of sensitive data.

Despite Foxsemicon's assurance that the breach would not significantly disrupt operations, the attackers threatened total destruction of the company if their demands were not met. This attack occurred during a period of heightened cyber concerns in Taiwan, adding to the complexity of the situation.

Change Healthcare - OPTUM Group - United HealthCare

In February 2024, ThreatMon reported a significant ransomware attack targeting Change Healthcare, part of the OPTUM Group under United HealthCare. The ALPHV/BlackCat group was identified as the threat actor behind the breach. After allegedly collecting the ransom payment, the group appeared to shut down its operations in what many have described as an exit scam. This incident caused substantial disruption at Change Healthcare and demonstrated the healthcare sector's continued vulnerability to ransomware threats.

For additional information and ongoing updates, follow ThreatMon Ransomware Monitoring on X at @TMRansomMon, which focuses on providing accurate, real-time insights into ransomware activity. By staying connected with ThreatMon, you can remain informed about the latest attacks, trends, and developments, helping you stay vigilant and prepared against potential threats.

DATA BREACHES

Over the course of 2024, data breaches remained a significant concern for organizations worldwide. ThreatMon recorded more than 37 billion compromised records stemming from multiple high-profile incidents during the year. A month-by-month review reveals that January experienced the largest spike, driven by the "Mother of All Breaches" (MOAB), which alone compromised over 28.4 billion records. Although the numbers dipped in February and March, they climbed again in April with the Discord breach. Another notable surge took place in August, caused by the National Public Data (NPD) Breach.

Compromised Records

33,216,17,668

January

28403500419

April

4197622652

February

409358410

The healthcare sector reported the highest number of breaches, closely followed by the finance industry. Many incidents stemmed from compromises in third-party services—a vulnerability highlighted by the Snowflake breach, which impacted organizations like Ticketmaster, Santander, and QuoteWizard. These examples emphasize the urgent need for robust cyber measures when integrating external providers.

Some of the most critical breaches, involving companies such as the Bank of America, Change Healthcare Group, and NPD, resulted in the sensitive data loss of more than millions of people. Now, let's take a look at the most significant breaches in this period.

Mother of All Breaches (MOAB): January 2024

The Mother of All Breaches (MOAB) was one of the most significant breaches due to its unprecedented scale, containing over 28 billion records. This breach included highly sensitive personal information such as names, addresses, phone numbers, and social security numbers, making it one of the largest data breaches in history.

Bank of America Data Breach: February 2024

The Bank of America data breach compromised the financial data of approximately 57,000 customers. This breach included unauthorized access to account numbers, transaction histories, and personal identification details, posing severe risks of financial fraud and identity theft.

Discord (via Spy.pet): April 2024

In April 2024, a significant data breach involving Discord, facilitated by the data scraping site Spy.pet, exposed over 4.1 billion public messages from approximately 620 million users across 14,000 servers. The harvested data included user aliases, connected accounts, and public messages, which were sold online in exchange for cryptocurrency.

Snowflake: May 2024

Snowflake was breached by UNC5537, impacting 165 companies, including Ticketmaster and Santander. Using stolen credentials and bypassing accounts without MFA, the attackers stole data affecting 560 million Ticketmaster users and 30 million Santander customers.

Snowflake confirmed the breach resulted from compromised credentials, not platform vulnerabilities.

Financial Business and Consumer Solutions (FBCS): July 2024

In July 2024, FBCS confirmed that the February ransomware attack exposed the data of 4.2 million individuals, including 237,703 Comcast customers. Stolen information included names, Social Security numbers, dates of birth, and account details. Initially estimated at 1.9 million affected, the impact grew significantly as investigations progressed.

National Public Data (NPD): August 2024

National Public Data (NPD) confirmed a breach exposing 2.9 billion records with sensitive information like Social Security numbers, addresses, and phone numbers. The hacker, "USDoD," had been accessing data since December 2023 and began selling it on the dark web for $3.5 million. The breach impacted individuals in the U.S., U.K., and Canada.

Cisco Systems: October 2024

Cisco confirmed a security incident in its public-facing DevHub environment, where the hacker "IntelBroker" claimed to have exfiltrated 4.5 TB of data. Leaks included source code, hardcoded credentials, and confidential documents, with 2.9 GB initially leaked on BreachForums, later exceeding 4 GB. Cisco attributed the breach to DevHub misconfigurations and has taken the site offline while investigating further.

CRITICAL VULNERABILITIES

Throughout 2024, critical vulnerabilities in both software and hardware systems have remained a persistent and evolving concern. These vulnerabilities, frequently exploited by malicious actors, expose organizations across multiple sectors to substantial risks, including data breaches, loss of sensitive information, and disruption of essential services. Addressing these vulnerabilities effectively calls for an assessment of not only their technical severity but also the potential real-world consequences they may carry.

The CVSS score is a valuable tool for assessing the severity of vulnerabilities, but it does not always capture their real-world impact. For instance, the JavaScript polyfill incident had a relatively low CVSS score but affected many users due to the widespread use of the compromised library. This example highlights the importance of considering contextual factors, such as the deployment environment and the potential reach of the vulnerability, alongside CVSS scores to accurately evaluate and prioritize security risks.

It is also important to look at two critical vulnerabilities that emerged in November 2024, CVE-2024-0012 and CVE-2024-9474, because their combined exploitation enables attackers to bypass authentication, elevate privileges, and execute arbitrary code on PAN-OS devices.
Following the release of a proof-of-concept (PoC) on November 19, 2024, there has been an increasing number of attacks that leverage these vulnerabilities. This example showcases how two vulnerabilities can be used together to increase the impact of a cyber incident, which in this case, enables threat actors to bypass authentication and deploy a variety of malicious payloads.

Here are the top 10 most important vulnerabilities discovered in 2024.

CVE-2024-38526

CVE-2024-38526 is a high-severity vulnerability in pdoc, an API documentation tool for Python projects, where the pdoc --math option is linked to JavaScript files from polyfill.io, which now serves malicious code after being sold. This issue has been fixed in pdoc version 14.5.1.

CVE-2024-3400

CVE-2024-3400 is a critical command injection vulnerability in Palo Alto Networks PAN-OS, allowing unauthenticated attackers to execute arbitrary code with root privileges on certain firewalls.

CVE-2024-4985

CVE-2024-4985 is a critical authentication bypass vulnerability in the GitHub Enterprise Server that allows attackers to forge SAML responses and gain unauthorized access with site administrator privileges.

CVE-2024-21762

CVE-2024-21762 is a critical out-of-bounds write vulnerability in Fortinet FortiOS and FortiProxy across multiple versions. It allows attackers to execute unauthorized code or commands via crafted requests. Patching to the latest secure versions is strongly recommended.

CVE-2024-47575

CVE-2024-47575 is a critical vulnerability in Fortinet's FortiManager and FortiManager Cloud platforms, affecting versions 6.2 through 7.6. This flaw allows attackers to execute arbitrary code or commands via specially crafted requests

CVE-2024-9474

CVE-2024-9474 is a privilege escalation vulnerability in Palo Alto Networks PAN-OS that allows administrators with management web interface access to execute actions with root privileges. Cloud NGFW and Prisma Access are not affected.

CVE-2024-0012

CVE-2024-0012 is an authentication bypass vulnerability in Palo Alto Networks PAN-OS (versions 10.2, 11.0, 11.1, and 11.2). It allows unauthenticated attackers with network access to the management web interface to gain administrator privileges, tamper with configurations, or exploit other vulnerabilities like CVE-2024-9474.

CVE-2024-42448

CVE-2024-42448 is a Remote Code Execution (RCE) vulnerability in VSPC. If the management agent is authorized on the server, attackers can exploit this flaw to execute code on the VSPC server from the management agent machine.

CVE-2024-2389

CVE-2024-2389 is an operating system command injection vulnerability in Flowmon versions prior to 11.1.14 and 12.3.5, allowing unauthenticated users to execute arbitrary system commands via the management interface.

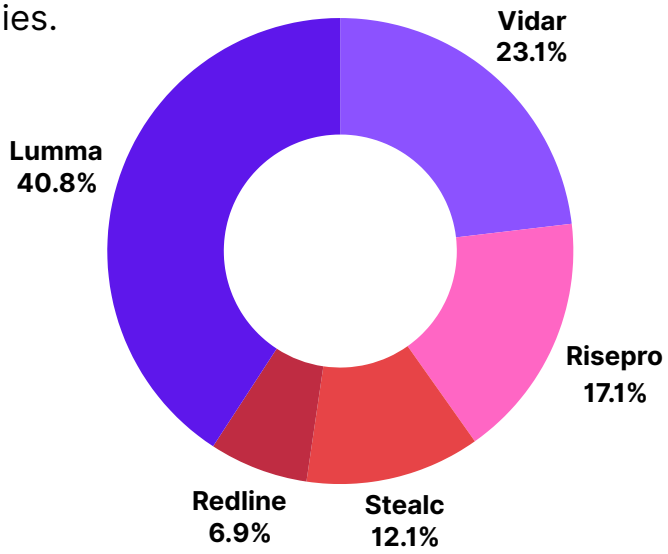
CVE-2024-9680

CVE-2024-9680 is a use-after-free vulnerability in Animation timelines, allowing attackers to execute code in the content process. It has been exploited in the wild and affects Firefox versions before 131.0.2, Firefox ESR before 128.3.1 and 115.16.1, and Thunderbird versions before 131.0.1, 128.3.1, and 115.16.0.

CVE ID	CVSS Score	CWE ID and Name	Publish Date
CVE-2024-38526	7.2	CWE-116: Improper Encoding or Escaping of Output	06/25/2024
CVE-2024-3400	10.0	CWE-77: Command Injection	04/12/2024
CVE-2024-4985	10.0	CWE-287: Improper Authentication	05/20/2024
CVE-2024-21762	9.8	CWE-787: Out-of-bounds Write	02/09/2024
CVE-2024-47575	9.8	CWE-306: Missing Authentication for Critical Function	10/23/2024
CVE-2024-9474	6.9	CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11/18/2024
CVE-2024-0012	9.3	CWE-306: Missing Authentication for Critical Function	11/18/2024
CVE-2024-42448	9.9	CWE-94: Improper Control of Generation of Code ('Code Injection')	12/11/2024
CVE-2024-2389	10.0	CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	04/02/2024
CVE-2024-9680	9.8	CWE-416: Use After Free	10/09/2024

Infostealer Analysis

Stealer malware remained a dominant cyber threat in 2024, with threat actors increasingly targeting credentials, financial data, and sensitive information. These malware leveraged advanced techniques to evade detection and demonstrated their adaptability in a constantly evolving cyber threat landscape. Understanding the activity patterns and prevalence of stealer malware provides critical insights for developing effective mitigation strategies.



The graph highlights the top five most popular stealer malware in 2024, with Lumma, Vidar, and Risepro emerging as the most prominent threats. Lumma, first observed in 2022, leads as the most popular malware in 2024 with a significant portion of the activity due to its widespread deployment and effectiveness. A long-established threat, Vidar, follows closely, demonstrating its sustained relevance in credential and financial data theft. Moreover, RisePro, which showed a notable increase in activity since late 2023, has rapidly gained traction.

The activity patterns show how newer threats like Lumma, and Risepro are learning from more established players like Vidar and Redline to utilize more effective tactics. These trends emphasize the importance of focusing on the most popular malware strains while closely following the evolving threat landscape for newer malware, as they continue to challenge existing mitigation techniques.

THREATMON
END-TO-END INTELLIGENCE

The ever-changing threat landscape evolves into a more fast-paced environment where threat actors collaborate the most, causing threats to emerge and harm much faster.

Today, it is proven that Businesses of all sizes may suffer from the agility of threat actors.

ThreatMon End-to-End Intelligence consists of multiple modules that enable businesses to obtain collectively exhaustive threat intelligence.

Key Features & Benefits

Holistic Intelligence

Comprehensive approach to threat intelligence covers all your security needs

Proactive Security

Real-time alerts and actionable intelligence

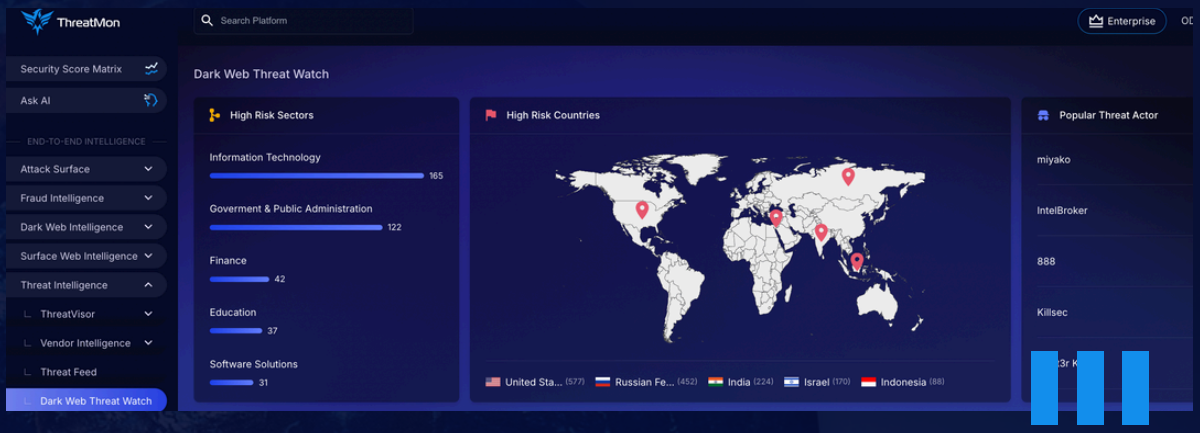
Scalable & Democratized

Flexible pricing options and a user-friendly interface

Enhanced Efficiency

Automated tools and intelligent insights

More Information About ThreatMon



One Platform for all intelligence needs.

ThreatMon End-to-end intelligence is a cutting-edge, cloud-based SaaS platform that continuously monitors the dark and surface web, providing early warnings and actionable insights into emerging threats.

We are a SaaS platform designed to help businesses proactively detect and address threats before a cyber attack occurs. Unlike traditional cyber threat intelligence, we provide comprehensive and holistic cyber intelligence.

- *Attack Surface Intelligence*
- *Fraud Intelligence*
- *Dark and Surface Web Intelligence*
- *Threat Intelligence*
- *Security Score matrix*
- *ThreatMon AI Agent*

APPLY

FREE ACCESS

Contact Us :

Email Address
info@threatmonit.io

https://x.com/MonThreat

https://www.linkedin.com/company/threatmon