



ThreatMon
Under Cyber Wings



GLOBAL CYBER THREAT REPORT

MID-YEAR **2024**

threatmon.io



TABLE OF CONTENT

02 Executive Summary & Key Findings

04 Timeline of Incidents

09 Dark Web Insights

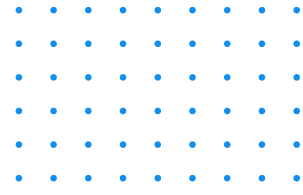
13 Ransomware Incidents

19 Data Breaches

21 Critical Vulnerabilities

24 ThreatMon End-to-End Intelligence

25 More Information About ThreatMon



EXECUTIVE SUMMARY & KEY FINDINGS

ThreatMon's 2024 Mid-Year Global Cyber Threat Report explores the global threat landscape to give you a comprehensive overview of the most significant cyber threats and trends observed in the first half of the year. The analysis highlights a marked increase in dark web activities, ransomware attacks, and data breaches across various sectors globally. In particular, the manufacturing, healthcare, and finance sectors were heavily targeted in H1 2024, experiencing significant disruptions due to these cyber threats. The manufacturing sector faced the highest number of ransomware attacks, while the healthcare and finance sectors saw a surprising and exceedingly high increase in data breaches, reflecting their valuable data and critical operations.

ThreatMon analyzes the threat landscape based on its extensive and detailed data covering most active dark web forums and ransomware groups' sites, the activities of most prominent threat actors, the vulnerability threat landscape, most used malware by threat actors, important breaches, and millions of stealer log data to present you insights into the the global threat landscape in the first half of 2024.

- *There was extensive dark web activity during the first half of 2024, with more than 750 critical incidents detected by ThreatMon.*
- *The most common types of dark web posts included data leaks, malware sales, and service access sales.*
- *The first half of 2024 saw a significant level of ransomware incidents, with over 2,500 attacks detected.*
- *Among numerous ransomware groups, LockBit, RansomHub, and Play group were the most active in H1 2024.*
- *February and May were particularly notable for their significant increases in ransomware activity, indicating periods of heightened threat levels.*
- *The manufacturing sector faced the highest number of ransomware attacks, accounting for 30% of the total incidents with 245 cases.*
- *In the first half of 2024, the healthcare sector saw a notable rise in ransomware activity, with 101 incidents accounting for 12% of the total. Meanwhile, the finance sector experienced an increase in targeted attacks, representing 4% of all incidents. These trends underscore threat actors' ongoing focus on these critical industries.*
- *The United States emerged as the most targeted country for ransomware attacks, experiencing 820 cases and accounting for 64.77% of the total incidents.*
- *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 26 billion records.*
- *One of the most critical incidents in 2024 occurred in May when Snowflake experienced a data breach affecting over 165 companies due to compromised customer credentials and the lack of multi-factor authentication. The threat actor UNC5537 exploited credentials obtained from stealer logs linked to third-party services, highlighting the necessity of a secure supply chain.*
- *In June 2024, a major supply chain attack on the Polyfill JS library, after its acquisition by a Chinese company, resulted in malware being injected into over 100,000 websites, targeting mobile devices and evading detection.*



TIMELINE OF INCIDENTS IN H1 2024

Significant Cyber Incidents

June

Polyfill JS Attack

May

Snowflake Data Breach Incident

April

El Salvador's Chivo Wallet Attack

March

United Nations Development Programme Ransomware Attack

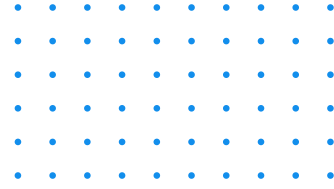
February

UnitedHealth Group Cyberattack

January

Mother of All Breaches (MOAB)

The first half of 2024 has been marked by a series of significant cyber incidents that have impacted various sectors globally. From DDoS and ransomware attacks to data breaches, these events highlight the increasing sophistication and frequency of cyber threats. Below is an overview of some of the most notable incidents that occurred during this period, providing insight into the evolving threat landscape.



June 2024

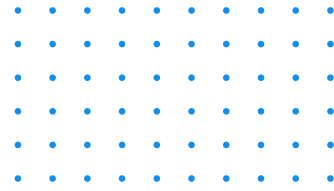
Polyfill JS Attack

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.

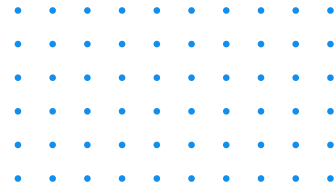
March 2024

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

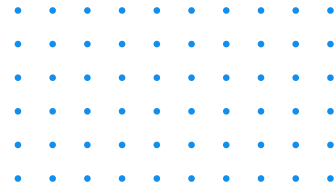
In February 2024, Bank of America announced a data breach that compromised the personal information of 57,000 customers. The breach occurred through a third-party vendor, Infosys McCamish Systems (IMS), which experienced a cyberattack in November 2023. The exposed data included names, addresses, Social 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.

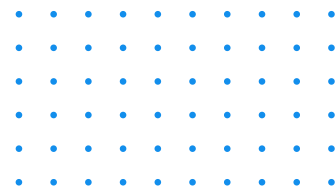
January 2024

Mother of All Breaches (MOAB)

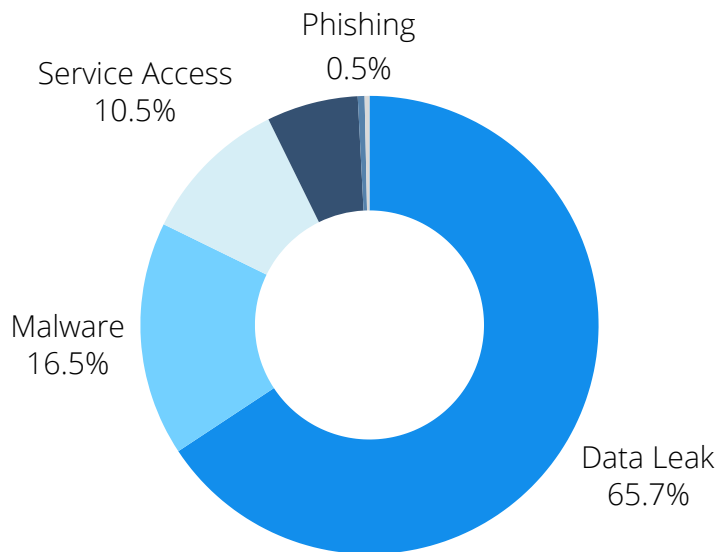
In January 2024, the "Mother of All Breaches" (MOAB) was discovered, exposing 26 billion records from a variety of sources, totalling 12 terabytes of data. The source of the breach remains unknown, with no one claiming responsibility. This breach included personal data from platforms like LinkedIn, Twitter, 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



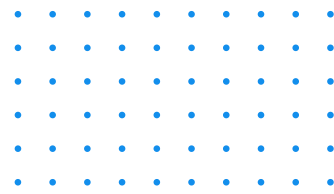
The first half of 2024 witnessed extensive dark web activities, underscoring its role as a thriving hub for cybercriminals. In total, ThreatMon has detected more than 750 incidents in the dark web, ranging from large-scale data breaches to the sale of newly developed malware strains.

Figure x. showcases the distribution of dark web posts by category. A majority, which is about 65%, of the dark web incidents recorded by ThreatMon were **data leak** posts, allegedly including sensitive information from various sectors, including **finance, healthcare, and government agencies.**

This alarming trend underscores the extensive risks associated with data leaks, driven by their frequent occurrence and the significant demand among threat actors.

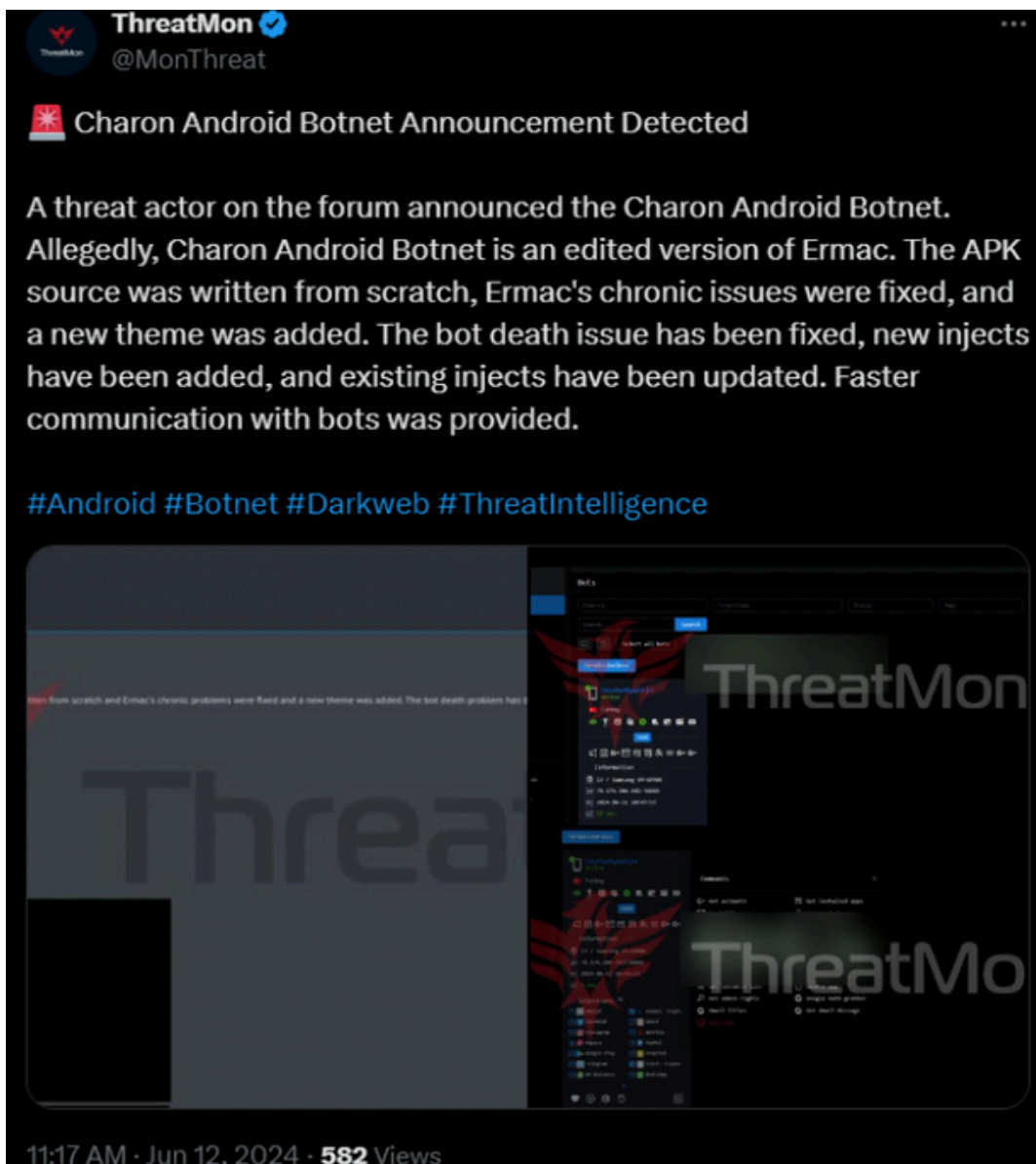
Following data leak posts, the second most common posts detected by ThreatMon on the dark web are sales, announcements, and sharing posts of malware. New and updated malware strains are frequently published on the dark web; some are sold at fixed prices or auctioned to the highest bidder, while others are freely shared as open-source tools for any threat actor to utilize.

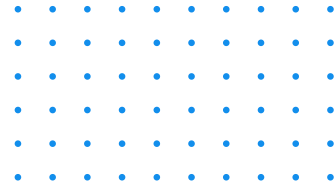
In particular, on June 12, an announcement post on a dark web forum, which was first detected by ThreatMon, revealed the update and the return of a notorious botnet called the Charon Android botnet. The botnet is an edited version of another infamous botnet called the Ermac botnet.



The announcement post reveals that the botnet was rewritten from scratch with the aim of resolving chronic issues in the Ermac botnet and adding additional features such as faster communication and new injects.

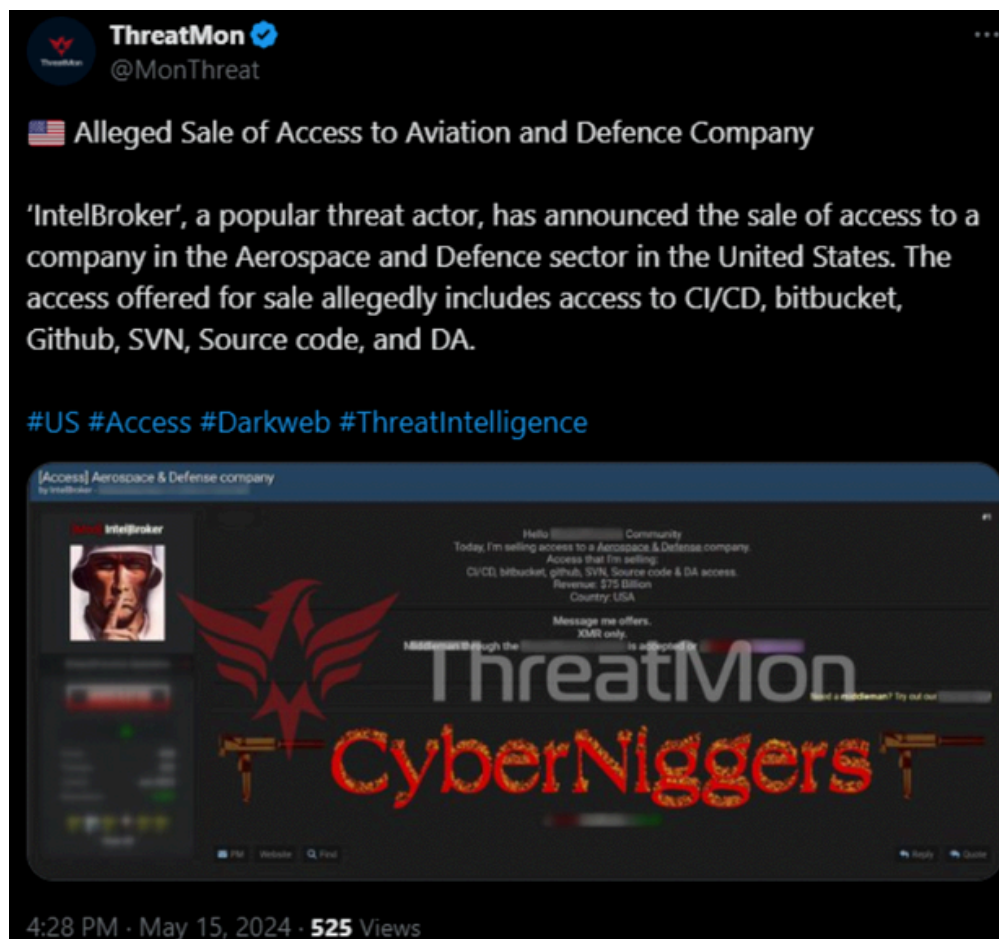
Figure x. displays the tweet announcing the detection of the botnet, published by ThreatMon on the social media platform X. ThreatMon's X account publishes critical cyber news and important cyber findings on a daily basis.

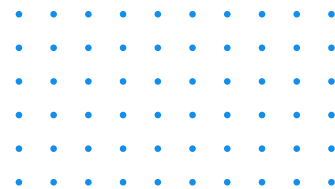




The third most common category of dark web posts detected by ThreatMon is service access posts, in which access to compromised systems, networks, or databases is either sold or directly shared for other threat actors to utilize. These posts are particularly concerning due to their potential to escalate cyber threats and further facilitate malicious activities

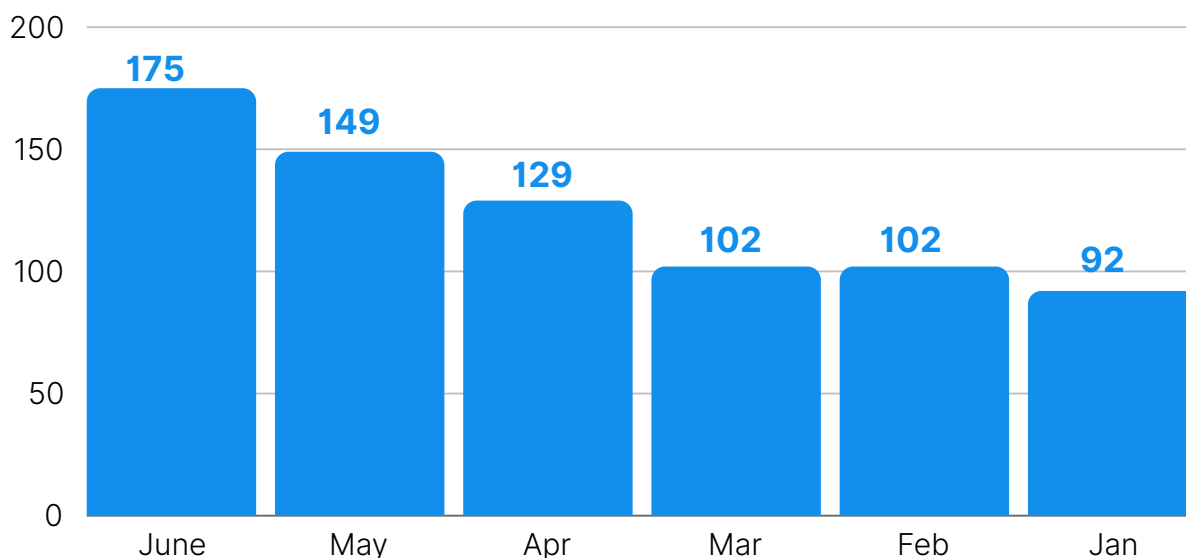
In particular, on May 15, ThreatMon's X account [@MonThreat](#) reported an alleged sale of access to an Aerospace & Defense company in the US with \$75 billion in revenue. The threat actor behind the sale, IntelBroker, is a very popular and active threat actor on the dark web, frequently selling access to various high-profile companies.





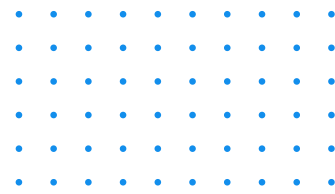
An unauthorized access acquired by a threat actor can lead to catastrophic consequences for organizations. For instance, although not a direct access sale, the critical Snowflake incident in May originated from the acquisition of stolen customer credentials found in numerous stealer log data. This critical incident underscores how stolen customer credentials, discovered in stealer log data, could escalate into a widespread cyber crisis, affecting more than 165 organizations globally.

Darkweb Activity Steadily Increased Throughout H1 2024



When we analyze the monthly dark web activity, a consistent increase in incidents over the first half of 2024 is observed. The number of monthly incidents nearly doubled from January to June, highlighting a concerning upward trend in cybercriminal activities on the dark web.

Analysts at ThreatMon expect the upward trend to continue for the rest of the year. As a result, we will observe a higher number of data leak posts, malware posts, service access posts, and much more. This sustained increase in dark web activity will result in a more volatile and dangerous threat landscape.

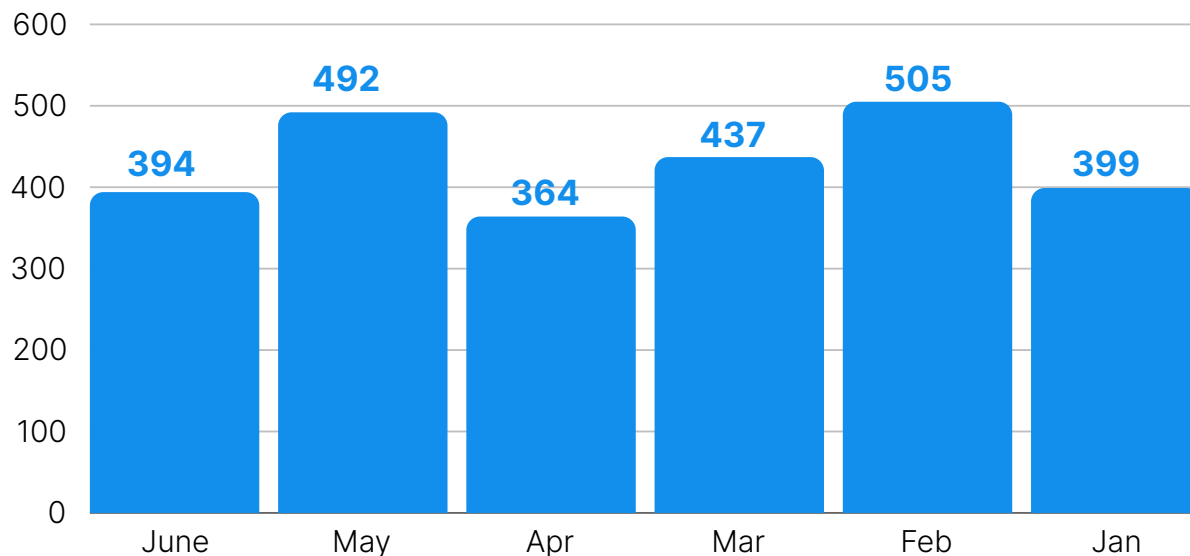


RANSOMWARE INCIDENTS

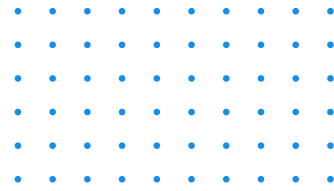
Ransomware attacks are one of the most valuable tools for threat actors, targeting government organizations, companies, and critical infrastructures. While the primary aim is financial gain through ransom payments, these incidents often result in other severe consequences, such as sensitive data loss, data leaks through double extortion tactics, and prolonged disruption of the victim's services.

Ransomware Peaks in February and May 2024

In H1 2024, ransomware groups remained highly active, with ThreatMon detecting over 2,500 ransomware incidents attributed to 67 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.



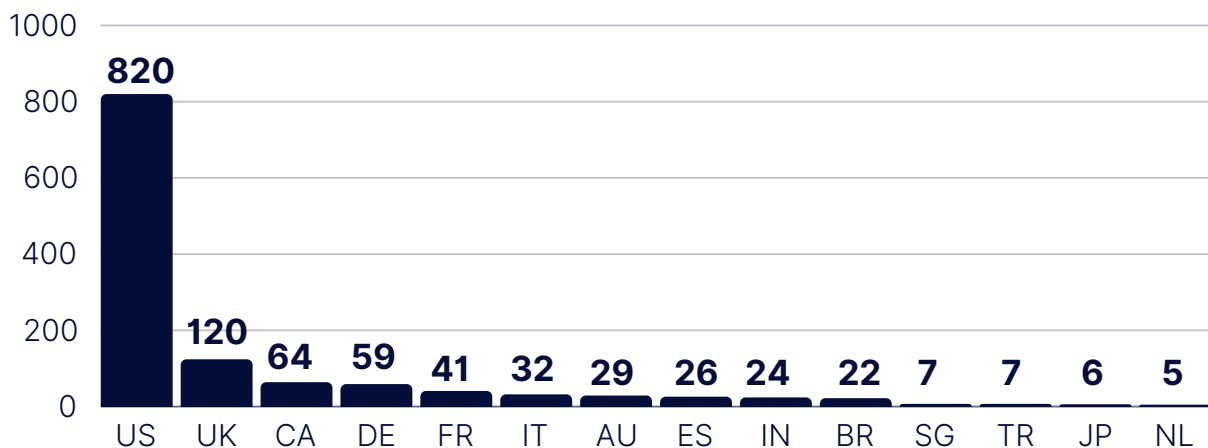
In H1 2024, February emerged as the month with the most ransomware activity, highlighting a peak in the number of attacks during this period, as presented in Figure x. The spike in February was followed by another high in May, indicating a worrying trend of increasing ransomware incidents. The overall activity remained alarmingly high throughout the first half of the year. Given the current alarming trend, we expect this troubling pattern to continue into the second half of the year

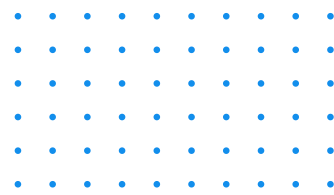


The United States Remains the Most Targeted Country in Ransomware Attacks



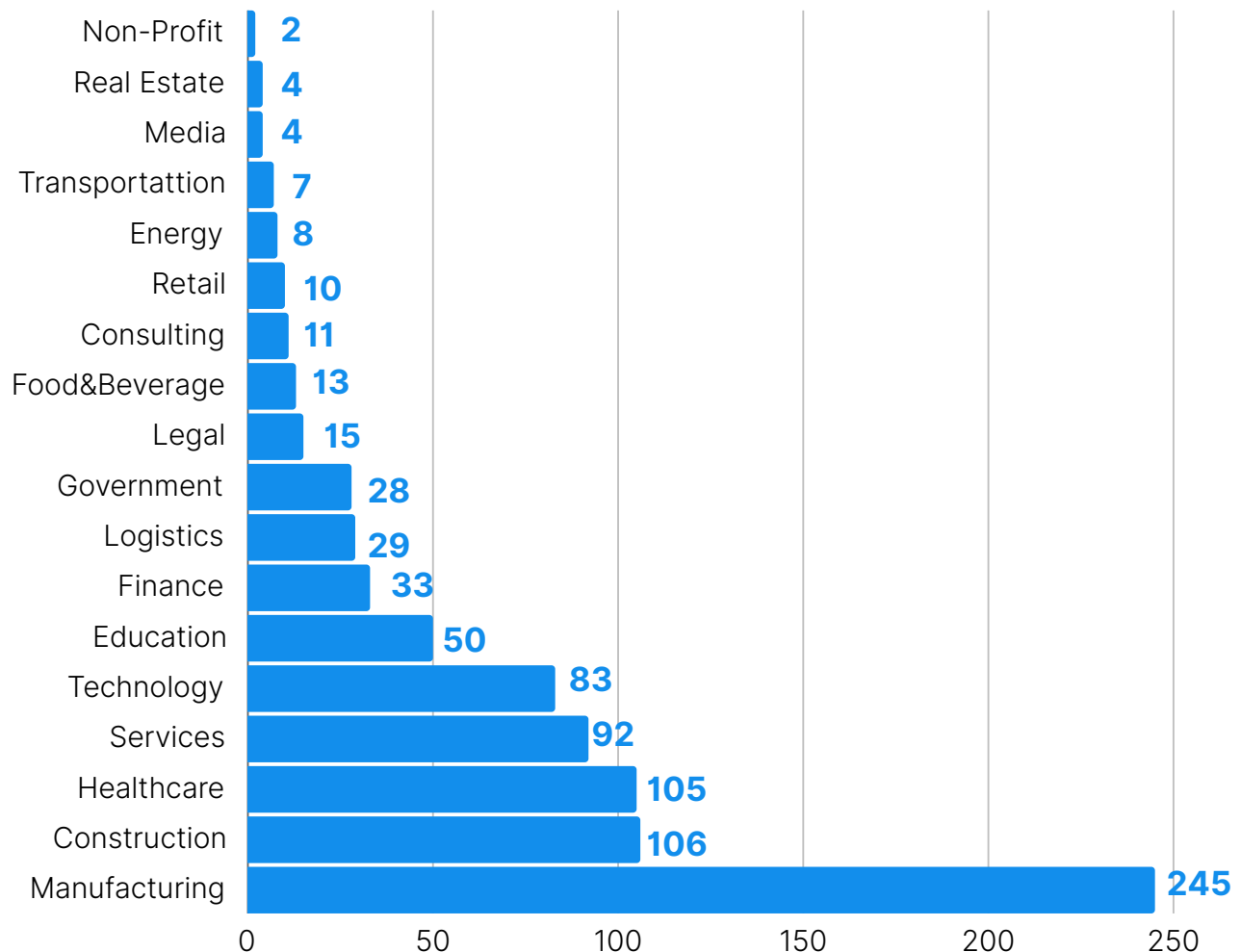
The global distribution of ransomware incidents, depicted in Figure X, shows that the United States has been the most affected, with 820 cases, making up 64.77% of the total incidents. This is followed by the United Kingdom, which saw 124 incidents, representing 9.79% of the total. Other affected countries include Canada, Germany, and France, highlighting the global reach of these cyber threats. Western countries are prime targets for ransomware groups, accounting for 80% of the incidents due to their wealth and valuable assets. In contrast, countries in the MENA region and Asia are less frequently targeted, indicating a lower likelihood of being hit by ransomware attacks.

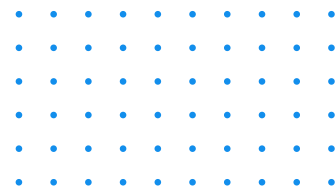




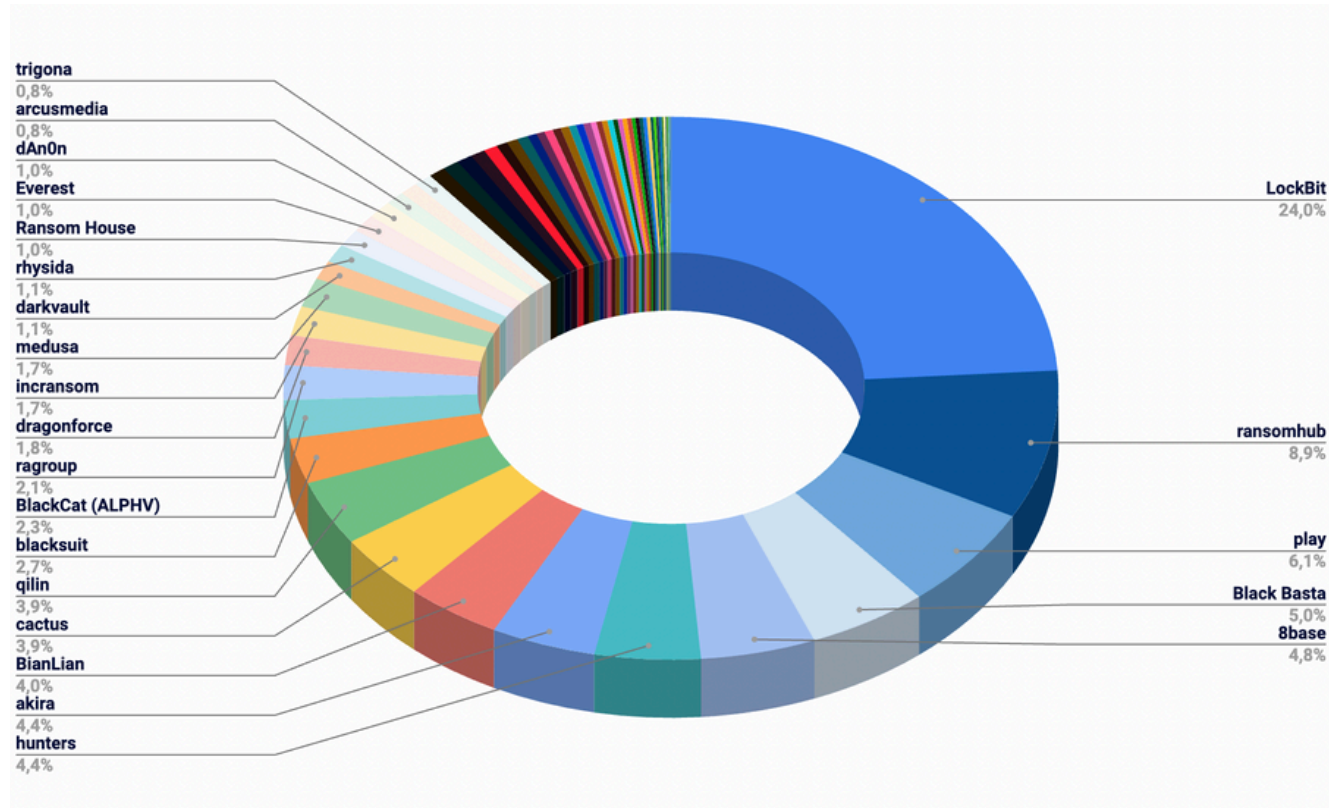
Unprecedented Increase of Attacks Targeting Finance and Healthcare Sectors

The distribution of ransomware incidents across various sectors shows that the manufacturing sector faced the majority of the attacks, accounting for 30% of the total incidents with 245 cases, as illustrated in Figure Y. Other sectors impacted include IT, construction, education, and logistics, highlighting the widespread reach of ransomware threats. Compared to previous years, the rise in attacks on the health and finance sectors underscores the shifting focus of cybercriminals towards these vital industries. The healthcare sector has seen a worrying rise in ransomware activity, with 101 incidents representing 12% of the total. Additionally, the finance sector, which saw an uptick in targeted attacks, comprised 4% of the total incidents.

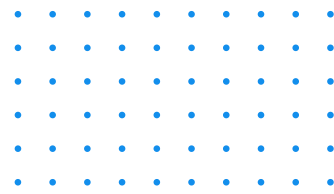




Top Ransomware Groups: LockBit, RansomHub, and Play Group Lead the Way



The analysis has highlighted an increase in ransomware incidents involving 67 distinct ransomware groups. Similar to previous years, LockBit remains the most active ransomware group, responsible for 619 incidents. With its constantly updated malware, LockBit is infamous for its widespread and relentless attacks on various sectors, including government organizations and large enterprises. Its ability to quickly adapt and target high-value entities has made it a significant threat in the cybersecurity landscape. LockBit has been closely followed by RansomHub, which has been particularly active in targeting the healthcare and education sectors, often exploiting vulnerabilities in outdated systems. Additionally, the Play group has been responsible for numerous high-profile attacks on financial institutions and large corporations. Together, these groups have demonstrated substantial activity, significantly contributing to the overall ransomware threat landscape.



Highlights

ThreatMon's Ransomware Monitoring account, [@TMRansomMonitor](#), actively provides updates on significant ransomware incidents, ensuring that followers stay informed about the latest threats and breaches. Throughout H1 2024, ThreatMon reported many critical incidents, highlighting the pervasive threat of ransomware across various sectors. Here are some of the most important incidents reported:

LoanDepot

On the X account, ThreatMon reported the LoanDepot ransomware attack in January 2024. The ALPHV/BlackCat group was responsible for this breach, demanding a \$6 million ransom. LoanDepot's refusal to pay led to the exposure of nearly 17 million records, causing significant financial and reputational damage. This incident underscored the severe impact ransomware could have on financial institutions. [Read more](#)



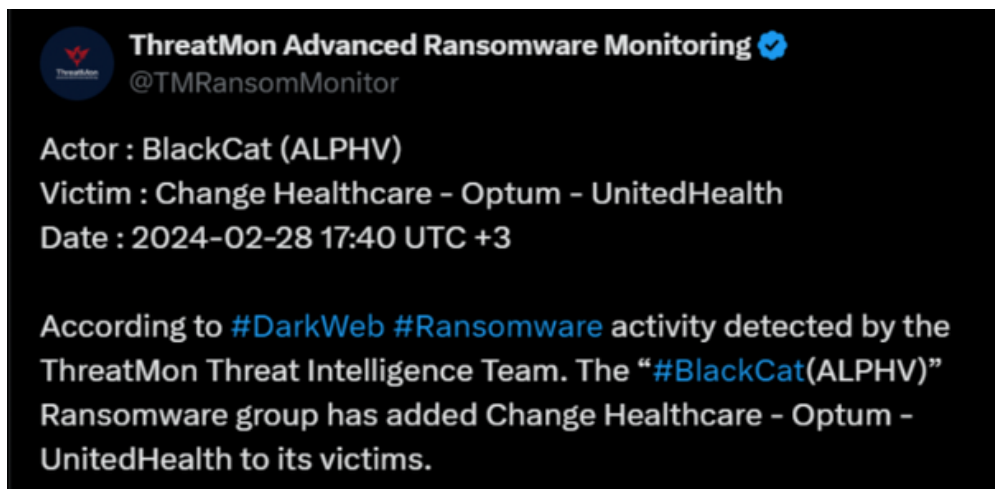
Foxsemicon Integrated Technology Inc.

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 cybersecurity concerns in Taiwan, adding to the complexity of the situation

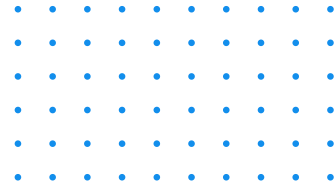


Change Healthcare - OPTUM Group - United HealthCare

In February 2024, ThreatMon reported on the ransomware attack against Change Healthcare, part of the OPTUM Group under United HealthCare. The ALPHV/BlackCat group was responsible for the attack. Following this breach, the group appeared to shut down its operations in what was described as an exit scam, after pocketing the ransom payment. This attack caused considerable disruption within Change Healthcare and highlighted the vulnerability of the healthcare sector to ransomware threats. [Read more](#)



For more details and updates on these incidents, you can follow ThreatMon Ransomware Monitoring on X at [@TMRansomMonitor](#). This account specializes in providing reliable real-time information exclusively on ransomware activities. By following ThreatMon, you can stay informed about the latest ransomware attacks, trends, and developments, helping you remain vigilant and prepared against potential threats.

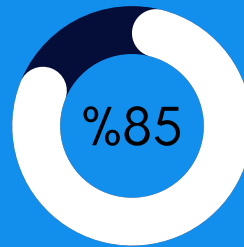


DATA BREACHES

Throughout the first half of 2024, data breaches persisted without rest, highlighting an enduring and significant threat to companies. Overall, In H1 2024, ThreatMon detected 33,216,107,668 compromised records from various significant data breaches. The graph illustrates the monthly distribution of breached records from January to May, with the highest spike in January due to the "Mother of All Breaches" (MOAB) incident, resulting in 28,403,500,419 compromised records. February and March saw a decrease, with another peak in April due to the Discord breach.

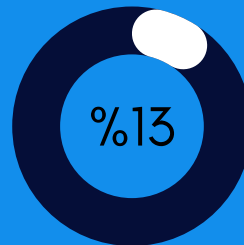
Compromised Records

33,216,17,668



January

28403500419



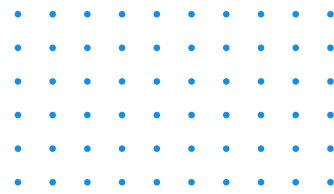
April

4197622652



February

409358410



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

Mother of All Breaches (MOAB)

The Mother of All Breaches (MOAB) was one of the most significant breaches due to its unprecedented scale, containing over 26 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.

Cyber Attack on the Russian Center for Space Hydrometeorology

The cyber attack on the Russian Center for Space Hydrometeorology (Planeta) severely disrupted satellite data services and meteorological forecasting. This attack compromised critical data and communication channels, highlighting the vulnerability of national space and weather monitoring infrastructure to cyber threats.

Trello Data Breach

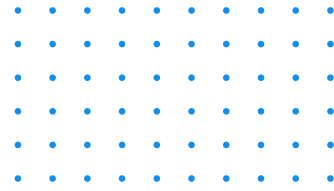
The Trello data breach exposed the sensitive information of approximately 12 million users due to a misconfiguration in their database. The breach included email addresses, user names, and project details.

Discord (via Spy.pet)

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.

Bank of America Data Breach

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.



CRITICAL VULNERABILITIES

The first half of 2024 has underscored the persistent and evolving threat of critical vulnerabilities in both software and hardware systems. These vulnerabilities, often exploited by threat actors, pose significant risks to organizations across various sectors. They can lead to critical data breaches, sensitive data loss, and disruption of essential services. To effectively prioritize and address these vulnerabilities, it's crucial to evaluate not just their technical severity but also their potential real-world impact.

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.

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

CVE-2024-38526

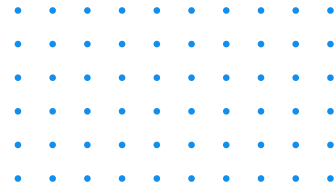
CVE-2024-38526 is a high-severity vulnerability in pdoc, an API documentation tool for Python projects, where the pdoc --math option is linked to JavaScript files from polyfill.io, which now serves malicious code after being sold. This issue has been fixed in pdoc version 14.5.1.

CVE-2024-38526 7.2 CWE-116: Improper Encoding or Escaping of Output

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-2024-3400 10.0 CWE-77: Command Injection



CVE-2024-27322

CVE-2024-27322 is a deserialization vulnerability in the R programming language that allows the execution of arbitrary code via malicious RDS files in versions 1.4.0 to 4.3.1.

CVE-2024-27322 8.8 CWE-502: Deserialization of Untrusted Data

CVE-2024-4985

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

CVE-2024-4985 10.0 CWE-287: Improper Authentication

CVE-2024-3094

CVE-2024-3094 is a critical supply chain vulnerability in XZ Utils versions 5.6.0 and 5.6.1 that allows remote code execution via a backdoor introduced through malicious code in the liblzma library.

CVE-2024-3094 10.0 CWE-912: Hidden Functionality (Backdoor)

CVE-2024-27198

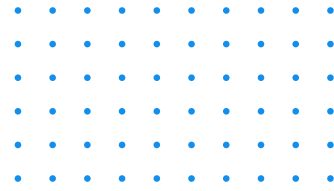
CVE-2024-27198 is an authentication bypass vulnerability in JetBrains TeamCity before version 2023.11.4, allowing remote unauthenticated attackers to take administrative control of the server.

CVE-2024-27198 9.8 CWE-288: Authentication Bypass

CVE-2024-20353

CVE-2024-20353 is a vulnerability in the management and VPN web servers for Cisco ASA and FTD software that allows unauthenticated remote attackers to cause a denial of service (DoS) condition by reloading the device.

CVE-2024-20353 8.6 CWE-400: Uncontrolled Resource Consumptio



CVE-2024-27130

CVE-2024-27130 is a buffer overflow vulnerability in several QNAP operating system versions that allows remote code execution via a specially crafted request.

CVE-2024-27130 7.2 CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

CVE-2024-24919

CVE-2024-24919 is an information disclosure vulnerability in Check Point Security Gateways that allows attackers to read sensitive information when connected to the internet with remote Access VPN or Mobile Access Software Blades enabled.

CVE-2024-24919 8.6 CWE-200: Exposure of Sensitive Information

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-2024-2389 10.0 CWE-78: Improper Neutralization of Special Elements used in an OS Command

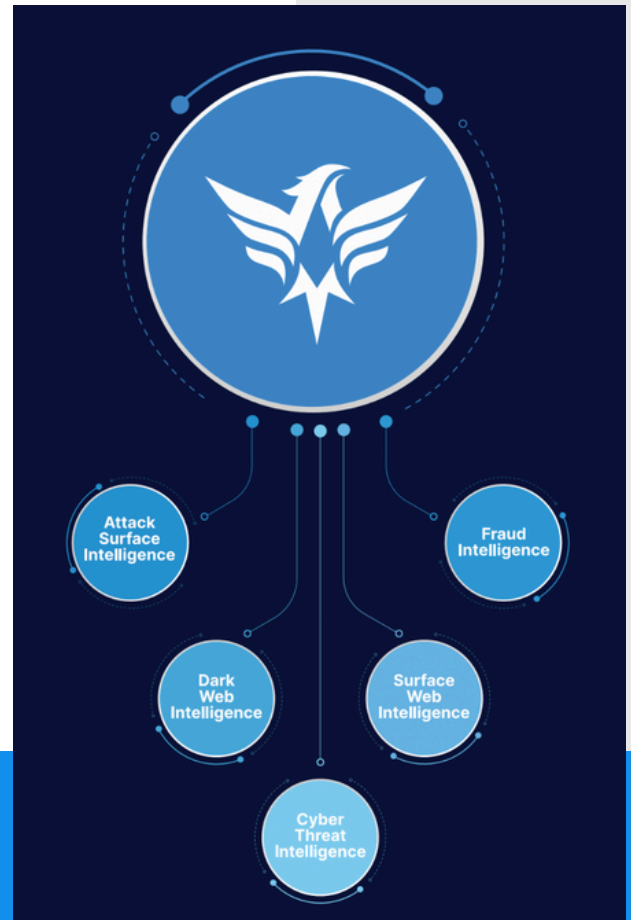


THREATMON END-TO-END INTELLIGENCE

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

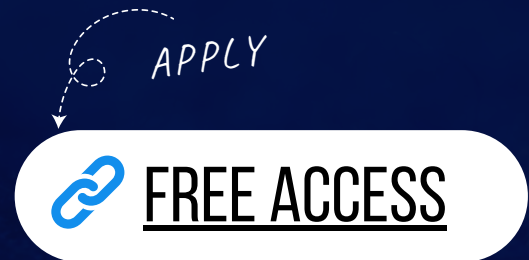


One Platform for all intelligence needs.

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



Contact Us :

Email Address
team@threatmonit.io

<https://x.com/MonThreat>

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