CYBLE®

Global Cyber Threat Intelligence Overview 2024

The Year So Far ...

CONTENTS

INTRODUCTION

The cybersecurity landscape in 2024 has gone from being a dystopian dream to a devastating reality, with significant technological advancements and evolving threats combining to inflict unprecedented damage on critical infrastructure and corporate networks alike. Although the number of government crackdowns on cybercriminal networks is near record, that has not deterred cybercriminals, as the intensity and ferocity of the attacks keep increasing exponentially.

The global cyber threat landscape saw substantial shifts in the first half of 2024, driven by rising cybercrime activity across critical sectors. This mid-year review from Cyble Research and Intelligence Labs highlights a surge in ransomware incidents, data breaches, and dark web operations, significantly impacting healthcare, construction, finance and manufacturing industries worldwide.

In particular, the construction, professional services, and manufacturing sector faced the brunt of ransomware assaults, accounting for the largest number of incidents. Meanwhile, the healthcare and financial sectors experienced a sharp uptick in data breaches, signaling the growing value of their sensitive data and essential services.

This report provides a comprehensive overview and analysis of the latest trends, key statistics, and notable incidents in the realm of cyberthreats globally.

KEY FINDINGS

- Recent research detected over 750 significant cyber incidents on the dark web during the first half of 2024. These ranged from data leaks and malware sales to access to services.
- Ransomware attacks continue to grow, with more than 2,600 cases recorded. LockBit, RansomHub, and Play Group were among the most active groups, with a significant spike in May 2024.
- The United States remained the most targeted nation for ransomware, making up more than 70% of all incidents, with 496 cases reported just in the last three months – August, July and June.
- The largest data breach, dubbed the "Mother of All Breaches" (MOAB), occurred in January, exposing a staggering 26 billion records.
- A major breach in May 2024 affected 165 companies using Snowflake, driven by compromised credentials and the lack of multi-factor authentication (MFA).
- **Increase in Cyberattacks:** The number of reported cyberattacks increased by **35%** compared to 2023.
- **Ransomware:** Ransomware attacks remain one of the most prevalent threats, accounting for **40%** of all cyber incidents reported in the first half of 2024.
- **Phishing Attacks:** There has been a **25%** increase in phishing attacks, with sophisticated techniques targeting both individuals and organizations.
- **Data Breaches:** Over **500 million** records were compromised in data breaches during the first eight months of 2024.
- **Average Cost of a Data Breach: $4.24 million** per incident.
- **Zero-Day Vulnerabilities:** The exploitation of zero-day vulnerabilities has surged by **20%**, posing significant challenges to organizations.

MAJOR THREATS AND TRENDS

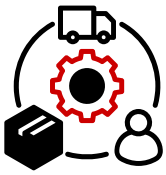
The numbers show a concerning trend, but what are the major threats and their trends? Here is our analysis.

RANSOMWARE

Ransomware continues to dominate the threat landscape in 2024. Attackers are employing more advanced encryption methods and targeting critical infrastructure, healthcare, and financial sectors. The average ransom demand has increased by **50%** compared to last year. What's more, some victims have been paying the ransom, thus increasing the incentive for these attacks to continue.

PHISHING AND SOCIAL ENGINEERING

Phishing remains a major threat and frequent entry point, with attackers using more personalized and convincing tactics. The use of AI to craft realistic phishing emails has led to a higher success rate. Organizations reported a **30%** increase in successful phishing attempts.



SUPPLY CHAIN ATTACKS

Supply chain attacks have become more frequent and damaging. Attackers are targeting third-party service providers to gain access to larger networks. Notable incidents in 2024 include breaches in major software and hardware supply chains. Even an event with just a few exposures can cause significant damage because of the number of downstream customers of a single victim.

INTERNET OF THINGS (IoT) VULNERABILITIES

With the proliferation of IoT devices, vulnerabilities in these devices have become a significant concern. IoT-related attacks have increased by **45%**, with many devices lacking proper security measures.

STATE-SPONSORED ATTACKS

State-sponsored cyberattacks have escalated, with nation-states targeting critical infrastructure, government agencies, and private corporations. These attacks are often sophisticated and well-funded, posing a serious threat to national security.

TIMELINE OF SIGNIFICANT INCIDENTS (H1 2024)

The first half of 2024 was marked by several high-profile cyber incidents, illustrating the increasingly complex and global nature of cyber threats. These events spanned multiple industries and included attacks such as ransomware, supply chain breaches, and significant data leaks.

AUGUST 2024

National Public Data (NPD) suffered a breach impacting 1.3 million people, with up to 2.9 billion records potentially exposed. NPD collects public data for background checks and criminal records.

JULY 2024

Evolve Bank & Trust and supply chain breach on HealthEquity cumulatively impacted nearly 12 million individuals in the U.S.

JUNE 2024

A supply chain attack on the popular JavaScript library, Polyfill JS, impacted over 100,000 websites. A major hosting site was acquired by a Chinese company, which injected malware that targeted mobile users.

MAY 2024

A breach at Snowflake exposed sensitive data from over 165 companies, including Ticketmaster and Santander. The attack was attributed to the exploitation of compromised customer credentials with no MFA enabled.

APRIL 2024

El Salvador's government-run Bitcoin wallet, Chivo Wallet, suffered a severe breach, exposing the personal information of nearly the entire adult population. The hacker group CiberInteligenciaSV claimed responsibility.

MARCH 2024

The UN Development Programme was hit by a ransomware attack from the 8Base gang, which led to the theft of 100,000 sensitive records. Simultaneously, France faced a massive DDoS attack linked to pro-Russian hackers.

FEBRUARY 2024

Bank of America and Cencora both announced data breaches. LockBit ransomware was behind the Bank of America incident, while Cencora's attack exposed personal and health data from pharmaceutical companies.

JANUARY 2024

The "Mother of All Breaches" (MOAB) surfaced, exposing 26 billion records from sources such as LinkedIn, Twitter, Adobe, and Tencent, marking one of the largest breaches in history.

DARK WEB INSIGHTS

Dark web activity surged in the first half of 2024, with over 700 notable incidents identified. The majority of posts on the underground forums involved data leaks, followed by malware sales and service access listings.

1. **DATA LEAKS (65% of incidents)**

Financial, healthcare, and government sectors were frequently mentioned and targeted in these posts.

2. **MALWARE SALES (16% of incidents)**

New and improved strains of malware were advertised, often auctioned to the highest bidder.

3. **SERVICE ACCESS (10% of incidents)**

These posts involved access to compromised systems or networks, potentially leading to more serious breaches.

In June 2024, the Charon Android botnet resurfaced on the dark web, reengineered from the older Ermac botnet. This new botnet features faster communication and additional inject capabilities, making it a potent threat.

RANSOMWARE INCIDENTS

Ransomware continued to wreak havoc globally in the first half of 2024, with over 2,600 attacks recorded. LockBit, RansomHub, and Play Group were the most active, driving a significant number of incidents, particularly in February and May.

TOP TARGETED SECTORS

- **Manufacturing (30% of incidents):** With 245 recorded cases, this sector remained the most targeted.
- **Healthcare (12%):** This sector saw a marked increase, with 101 attacks.
- **Finance (4%):** Financial institutions experienced a growing number of ransomware attempts, reflecting a heightened focus on high-value targets.

GEOGRAPHIC DISTRIBUTION

- **United States (More than 70% of incidents):** With 496 attacks, the U.S. saw the highest volume of ransomware incidents in the past three months.
- **United Kingdom (9%):** The UK was the second-most targeted nation with 51 incidents in the same time frame.

DATA BREACHES

Data breaches continued to be a major concern, with over 33 billion records compromised in H1 2024. Notable incidents included:

- **MOAB (JANUARY 2024):** The "Mother of All Breaches" exposed an unprecedented 26 billion records from platforms such as LinkedIn, Adobe, and Tencent.
- **TRELLO DATA BREACH (JANUARY 2024):** The breach impacted 15 million users, leaking sensitive data due to an API vulnerability.
- **BANK OF AMERICA (FEBRUARY 2024):** A third-party vendor breach exposed personal and financial information of 57,000 customers.
- **DISCORD DATA BREACH (APRIL 2024):** Over 4.1 billion public messages were scraped from Discord servers, exposing user data through the site Spy.pet.

These breaches highlight the growing threat to sensitive data, driven by third-party vulnerabilities and credential-based attacks. Ensuring robust multi-factor authentication and stricter access controls can mitigate many of these risks.

CRITICAL VULNERABILITIES

The first half of 2024 exposed several high-severity vulnerabilities across various software and hardware systems. These flaws, if exploited, pose substantial risks, including data breaches, unauthorized access, and significant service disruptions. Although technical severity is often assessed using the Common Vulnerability Scoring System (CVSS), real-world impact depends on factors such as deployment context and vulnerability reach. Here are the top vulnerabilities identified during the first half of 2024:

1. **CVE-2024-38526:** A critical vulnerability in the pdoc tool, commonly used for API documentation in Python projects, allowed malicious JavaScript injection via the compromised polyfill.io service. Though it had a relatively low CVSS score (7.2), the widespread use of polyfill.io amplified its impact. The issue has since been fixed in pdoc version 14.5.1.

2. **CVE-2024-3400:** This is a command injection vulnerability in Palo Alto Networks' PAN-OS, allowing unauthenticated attackers to execute arbitrary code with root privileges on affected firewalls. Rated at a maximum CVSS score of 10.0, this vulnerability is critical for network security.

3. **CVE-2024-27322:** Found in the R programming language, this deserialization flaw allows the execution of arbitrary code through malicious RDS files in versions 1.4.0 to 4.3.1. It received a CVSS score of 8.8 due to its significant exploitation potential.

4. **CVE-2024-4985:** This vulnerability in GitHub Enterprise Server enables attackers to bypass authentication by forging SAML responses, granting unauthorized access with site administrator privileges. With a CVSS score of 10.0, it poses severe risks for organizations using this platform.

5. **CVE-2024-3094:** A supply chain vulnerability in XZ Utils versions 5.6.0 and 5.6.1 allowed for remote code execution via a backdoor introduced through malicious code in the liblzma library. Rated at 10.0, it represents a significant risk to any system relying on these utilities.

6. **CVE-2024-27198:** A serious authentication bypass flaw in JetBrains TeamCity (versions prior to 2023.11.4) allows remote unauthenticated attackers to take full administrative control of the server. This vulnerability has a CVSS score of 9.8.

CRITICAL VULNERABILITIES

7 **CVE-2024-20353:** Affecting Cisco ASA and FTD software, this vulnerability causes a denial-of-service (DoS) condition by reloading the device. It can be triggered remotely by unauthenticated attackers, with a CVSS score of 8.6.

8 **CVE-2024-27130:** This buffer overflow vulnerability affects several versions of QNAP operating systems, allowing remote code execution via specially crafted requests. It received a CVSS score of 7.2.

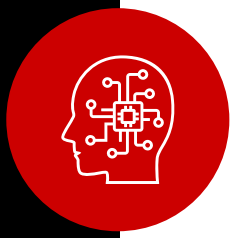
9 **CVE-2024-2389:** A command injection flaw in Flowmon (prior to versions 11.1.14 and 12.3.5) allows unauthenticated users to execute arbitrary system commands via the management interface. With a CVSS score of 10.0, it is considered highly critical.

10 **CVE-2024-24919:** This information disclosure vulnerability in Check Point Security Gateways allows attackers to access sensitive information when connected via remote VPN or Mobile Access Software Blades. The CVSS score for this vulnerability is 8.6.

11 **CVE-2024-4577:** It is a PHP vulnerability that affects installations running CGI mode. The vulnerability primarily affects Windows installations using Chinese and Japanese language locales, but it is possible that the vulnerability applies to a wider range of installations. Multiple malware campaigns: Gh0st RAT, RedTail cryptominers, and XMRig were seen exploiting this 9.8 rated bug.

These vulnerabilities highlight the importance of maintaining a rigorous patch management process and keeping all systems up to date. Organizations must not only rely on CVSS scores but also consider the broader context, including deployment environments and potential reach, when prioritizing vulnerability remediation.

EMERGING TRENDS IN CYBER THREAT INTELLIGENCE FOR 2024



1. ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

Artificial Intelligence (AI) and Machine Learning (ML) are being increasingly leveraged both by cyber defenders and attackers. AI-driven threat detection systems like Cyble's Vision X are becoming more sophisticated, capable of identifying anomalies and potential threats in real-time. Conversely, attackers are using AI to craft more convincing phishing attacks and automate the discovery of vulnerabilities.

2. CLOUD SECURITY

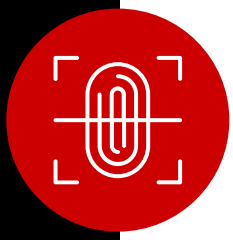
As organizations continue to migrate to the cloud, securing cloud environments has become a top priority. Threat intelligence is focusing on identifying vulnerabilities in cloud infrastructure and services. Cloud providers are enhancing their security offerings, and organizations are adopting multi-cloud strategies to mitigate risks.

3. EXTENDED DETECTION AND RESPONSE (XDR)

Extended Detection and Response (XDR) platforms are gaining traction as they provide a more comprehensive view of threats across an organization's entire IT environment. XDR integrates data from multiple sources, including endpoints, networks, and cloud environments, to provide a holistic approach to threat detection and response.

4. SUPPLY CHAIN SECURITY

Supply chain attacks have become a significant concern. Threat intelligence is increasingly focusing on identifying risks within third-party vendors and partners. Organizations are implementing more stringent security measures and conducting thorough assessments of their supply chains to mitigate potential threats.



5. ZERO-TRUST ARCHITECTURE

The adoption of Zero-Trust Architecture is on the rise. This approach assumes that no entity, whether inside or outside the network, should be trusted by default. Threat intelligence is playing a crucial role in identifying potential risks and ensuring that all access requests are continuously verified.

EMERGING TRENDS IN CYBER THREAT INTELLIGENCE FOR 2024

6. SOCIAL ENGINEERING ATTACKS

Social engineering attacks, particularly phishing, are becoming more sophisticated. Threat actors are using advanced techniques to manipulate trust and deceive individuals. The use of AI to craft personalized phishing emails has increased the success rate of these attacks.

7. INTERNET OF THINGS (IoT) SECURITY

With the proliferation of IoT devices, securing these devices has become critical. Threat intelligence is focusing on identifying vulnerabilities in IoT devices and developing strategies to mitigate risks. Ensuring that IoT devices are properly configured and regularly updated is essential for maintaining security.

8. THREAT INTELLIGENCE SHARING

Collaboration and information sharing among organizations and industries are becoming more prevalent. Threat intelligence sharing platforms and initiatives are helping organizations stay informed about the latest threats and vulnerabilities, enabling them to respond more effectively.

9. STATE-SPONSORED ATTACKS

State-sponsored cyberattacks are becoming more sophisticated and targeted. These attacks often focus on critical infrastructure, government agencies, and large corporations. Threat intelligence is vital in identifying the tactics, techniques, and procedures (TTPs) used by nation-state actors and developing strategies to defend against them.

10. PRIVACY AND DATA PROTECTION

With increasing regulations around data protection, such as GDPR and CCPA, organizations are prioritizing the security of personal data. Threat intelligence is focusing on identifying risks related to data breaches and ensuring compliance with regulatory requirements.

CONCLUSION

The cybersecurity landscape in 2024 presents both challenges and opportunities. The rapid pace at which cybercriminals collaborate and launch attacks calls for a comprehensive approach to cybersecurity.

While the threat landscape is evolving with more sophisticated attacks, advancements in threat intelligence and mitigation strategies offer hope for more resilient defenses.

Cyble's AI-driven intelligence offers businesses a proactive toolset for detecting and mitigating cyber risks before they escalate. With features like **attack surface management, brand intelligence, cyber threat intelligence, dark web monitoring, vulnerability management, takedown and disruption,** Cyble provides real-time, actionable insights to help organizations stay ahead of emerging threats.

By leveraging Cyble's platform, businesses can bolster their defenses and minimize the risks posed by an ever-evolving threat landscape.