CybelAngel | 2025

External Threat Intelligence Report

CybelAngel

Foreword

2024 certainly made its mark.

We saw AI's continued gallop, escalating geopolitical tensions and economic uncertainties shake up global markets, hard. All the while, new and existing criminal gangs unleashed cyber quakes shaking some of the biggest brands to their core.

While it is a given that cybercriminals thrive in any environment, new malicious actors rose at speed to fill the shoes of fallen players. Take the example of the prolific fall of LockBit in April (they have racked up $91 million of ransomware payments in the U.S. alone). While a dominant player in 2023, our data found that RansomHub has since seized its crown.

With the stakes higher than ever, our 2025 External Threat Intelligence Report delves deep into threat data existing beyond your managed IT perimeter. We uncovered a staggering **60% increase in exposed assets** from the previous year. Internal data also found that **exposed hosts and applications with vulnerabilities rose by 16% in 2024**. What is consistent throughout this report is that cybercriminals are innovating at speed and the attack vector is larger than ever. And you need to catch up.

Moreover, we observed a **20% surge in open and unsecured databases** compared to the previous year. This underscores the accelerating trend towards the inability of the supply chain, vendors, and employees to properly secure critical data. Consequently, your external attack surface is expanding at an unprecedented rate. This was evident in our findings, with **a 51% increase in all alerts sent to our clients in 2024**.

While we chose to focus on certain items specific to each threat, more information from each section can be found on our blog.

Armed with this knowledge, this report will enable you to fortify your business and foster a culture of safety, security, and resilience.

This year, take time to survey your external threats, guided by our 2025 External Threat Intelligence Report.

Erwan Keraudy
Co-Founder and CEO

Table of contents

Section 1

Your Attack Surface

Executive Summary

An Overview of the State of External Attack Surface Management

Can you think of every internet-facing asset that your organization owns?

While the average organization has 4,000 visible digital assets, invisible assets are a much bigger total figure. Cloud-based applications, Shadow IT, Supply chain and third-party exposures, Internet of Things devices, and so on are all contributing to an ever-widening external attack surface.

Two significant use cases in 2024 should serve as a wake-up call for your teams about the consequences that stem from poor cyber hygiene, both internally and externally.

1: US telecom giants Verizon, AT&T, and Lumen Technologies fell victim to a massive cyber assault dubbed Salt Typhoon, linked to China.

The Wall Street Journal first reported on this infiltration in late 2024, sparking probes by US intelligence officials and private sector cybersecurity researchers. The Salt Typhoon group is believed to be connected to China's Ministry of State Security. Hackers targeted backdoors established for legitimate US government surveillance, potentially gaining access to approximately **68% of American wireless traffic**.

This attack stemmed overall from poor cyber hygiene. It came from weak password management, insufficient access controls, inadequate MFA, and unpatched systems—to name a few. Hard lessons came up in its aftermath.

2: RansomHub emerged as a major player in the ransomware-as-a-service (RaaS) market in 2024, quickly becoming one of the most prominent ransomware operations worldwide.

After its appearance on the dark web in February 2024, our data found RansomHub attacked at least **488** victims in 64 countries across various industries, including critical infrastructure sectors such as water and wastewater, government infrastructure, and healthcare. The group's activity showed a significant upward trajectory throughout 2024, with its share of ransomware attacks increasing from **2% in Q1** to **14.2% in Q3**.

RansomHub's meteoric rise exposes critical gaps in organizational cybersecurity. It pinpoints how essential it is to have proper incident response plans in place, not to mention maintaining offline encrypted backups, implementing strong password policies and so forth. This reduces a huge portion of exposure risk.

So, why are we not taking more action?

The overall ransomware landscape in 2024 saw median ransom payments increase from under

$200,000 in early 2023 to **$1.5 million by mid-2024**. The group's **90% commission rate** for affiliates means you will be hearing a lot more about them in 2025.

Overall, CybelAngel's objective with our 2025 External Threat Intelligence Report is twofold. We aim to share intelligence on the evolving threats that our clients, partners, and all cyber stakeholders face, as well as share notable data trends.

CybelAngel Methodology

CybelAngel protects top-tier organizations across diverse global industries from external cyber threats that emerge beyond their managed IT perimeter.

Leveraging a combination of proprietary technology and third-party feeds, CybelAngel collects billions of data points, which are then refined by machine learning models and analyzed by a highly skilled team of human analysts.

By identifying business-critical exposures in advance, CybelAngel helps prevent disruptions to business operations by providing proactive threat intelligence. The company delivers comprehensive reports to clients, providing actionable insights, contextual information, and investigation results. Working closely with exposed organizations, analysts determine areas of risk, ensuring prioritization and an unmatched zero false positive rate. The findings in this report are based on the monitoring and alerting technologies used to protect our customers, combined with expert opinions and recommendations from our industry specialists.

When we review threat patterns, we rely on data and results from our client base to demonstrate real alerts, assess the impact, and provide actionable strategies against today's threats. We also highlight the speed and sophistication of attacks, as well as the vulnerabilities exploited by attackers. Understanding the location and methods of these attacks is critical to our analysis.

Privacy and ethics are fundamental values for CybelAngel. Although we may illustrate examples of exposures, attacks, vulnerabilities, and vectors, we do not disclose or expose private information. This report showcases both the breadth and depth of the external attack surface as viewed from an attacker's perspective, covering data pre and post-filtering. Our expertise in AI and machine filtering, acquired over a decade, is evident in the content. Every alert comes from billions of digital exposures. Our scanners and crawlers work around the clock to find potential or confirmed risks to business operations.

After filtering, CybelAngel analysts thoroughly investigate each event to verify its criticality, ensuring it is genuinely relevant and sensitive to our client's business. The incident report provided to cybersecurity teams, along with Security Operation Centers, threat hunters, red teams, pen testers, and vulnerability management teams, includes the necessary context and additional investigative findings.

External Cyber Threat Intelligence at a Glance

An overview of your external attack surface from an attacker's perspective.

External Cyber Threat Intelligence is a crucial element of a proactive cybersecurity strategy. It encompasses all signals gathered, analyzed, and correlated to identify, assess, and mitigate cyber threats originating outside of an organization's perimeter. This includes coverage and awareness of the extended supply chain of vendors, trusted partners and remote workers who are part of an enterprise's cyber ecosystem.

A good External Threat Intelligence program focuses on adversary behaviors, attack infrastructure, and external risk factors which could impact an enterprise. The goal is to enhance situational awareness, predict emerging threats, and proactively reduce the attack surface before exploitation occurs.

An effective External Threat Intelligence program transforms a company's cybersecurity posture from reactive to predictive. By enabling a proactive defense through increased awareness, it helps reduce overall risk to the organization.

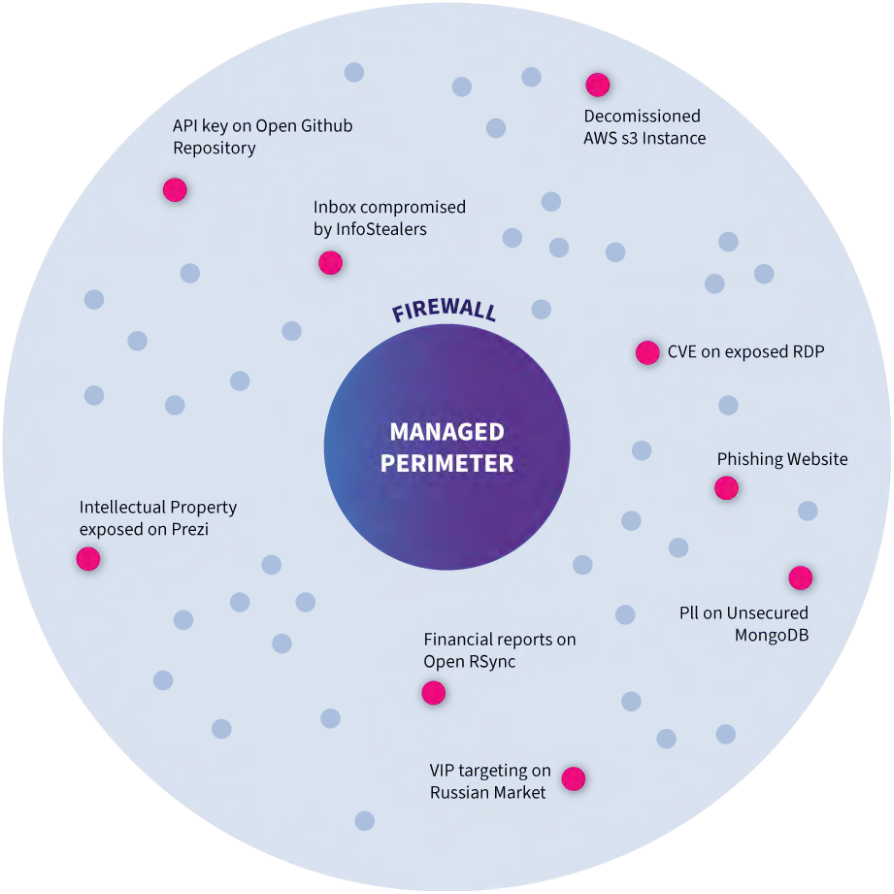

Figure: *A visual representation of your External Attack Surface.*

Section 2

Ransomware

Why Ransomware Attacks Increased in 2024

The year 2024 ushered in a historic wave of ransomware attacks. CybelAngel detected a **42% increase in reported attacks**, as well as an **increase of 125%** in the number of active groups from the previous year.

These attacks came from a rapidly growing group of new threat actors leveraging increasingly sophisticated techniques, which we will detail in full.

What will drive this surge in cyber attacks in 2025?

The increase in attacks, frequency and groups involved can be attributed to multiple factors.

Cybercriminals are employing more advanced techniques, exploiting zero-day vulnerabilities and utilizing AI-driven tools, making attacks more effective and harder to detect. IBM noted that the average time to prepare and start a ransomware attack dropped to **3.84 days in 2024**, down from **60+** days in 2019.

This, combined with the proliferation of Ransomware as a Service, RaaS, platforms, has lowered the barrier to entry for cybercriminals, enabling individuals with limited technical expertise to launch sophisticated attacks.

From **2023 to 2024** CybelAngel's analysis found that ransomware groups more than doubled from 62 to 140. The increase is due to the lower barrier, the ease of use of RaaS platforms and spin-offs from different traditional ransomware criminal groups.

Ransomware actors are increasingly focusing on essential services, including manufacturing, healthcare, and transportation sectors, leading to significant operational disruptions.

Impacted Industry due to Ransomware

	2023	2024
1	Building and Construction	Manufacturing
2	Information Technology Services	Building and Construction
3	Hospital and Health Care	Information Technology Services
4	Manufacturing	Hospital and Health Care
5	Education	Education
6	Financial Services	Transportation and Logistics
7	Transportation and Logistics	Financial Services

8	Law Firms	Law Firms
9	Government Services	Food and Beverage Industry
10	Real Estate/Insurance (tie)	Retail Industry

Figure: *Ransomware Impact Across Industries: 2023 vs 2024 Comparative Analysis*

Threat actors are leveraging increasingly sophisticated techniques to enhance the stealth of their attacks.

We analyzed stealthier methods in 2024

Beyond traditional encryption-based ransomware, adversaries are increasingly resorting to "**double extortion**" tactics, exfiltrating sensitive data and threatening public exposure to coerce victims into compliance. This approach has been notably employed by an increasing number of actors looking to enhance revenue on attacks.

Additionally, the proliferation of malicious open-source software packages has introduced a critical vector for supply chain attacks, as attackers compromise widely adopted libraries and tools to disseminate malware. This trend significantly amplifies risks for organizations dependent on open-source ecosystems, necessitating more robust software supply chain security measures.

Best practices for preventing ransomware-related attacks

1. Recognize indicators of compromise (IOCs): CISA lists file names, URLs, and IP addresses that could indicate that RaaS malware has been installed on a device. Read it here.

2. Read up on tactics, techniques and procedures (TTPs): Common techniques used by RaaS player affiliates include mass phishing and abusing Microsoft Windows Management Instrumentation to launch malicious payloads.

3. Create an incident response plan: Quarantining or removing affected accounts, reviewing compromised networks, setting up new account credentials, reviewing unusual activity, and reporting the breach, are integral.

4. Have a recovery plan (plus keep encrypted backup offline): This will ensure that even if your organization is subjected to a ransomware attack, you can mitigate the damage and restore systems quickly.

5. Follow NIST's password policies: When it comes to access controls, ensure everyone has passwords at least eight characters long, stored in industry-recognized managers, and implement lockout measures for multiple failed login attempts.

6. Have MFA enabled across all networks: This can prevent criminals from gaining remote access to your system through phishing, in particular via emails and virtual private networks.

7. Disable command-line and scripting activities: Threat actors often rely on these tools for their lateral movement workflows, so disabling them can block the ransomware from working.

Section 3

APIs

Exploring API Vulnerabilities, Trends, and Themes

Application Programming Interfaces (APIs) are the backbone of modern software communication. Through them, applications, systems, and devices interact and exchange data seamlessly. But as commonplace as API adoption is, so too is the surge in malicious actors who want to disrupt the flow of sensitive data and execute unauthorized commands on servers.

What is behind a *625%* rise in API exposure losses since 2021?

Rising API data breaches caused by bots, lack of API visibility, new vulnerabilities created by AI, and a lack of API security focus. These are just some of the reasons why excessive API data exposure is a growing headache for SOC teams everywhere.

A 2024 Imperva report estimated that insecure APIs accounted for up to $87 billion in losses annually, up an enormous 625% since 2021.

In 2024, APIs became more of a focal point for cybercriminals, and at the same time, threat actors became more sophisticated. The challenges experienced by the businesses below should serve as a reminder of why robust API security practices are essential. Other more digestible lessons below can act as another more straightforward reminder.

Four API exposure lessons to learn from 2024

These use cases illuminate the technical precision behind notable attacks.

1. The Sensitive Messages Breach
A flawed API exposed approximately 650,000 sensitive messages, including confidential information and passwords. Rigorous API testing and validation would have prevented this breach.

2. The Trello Data Exposure
Misconfigured APIs in Trello, a project management tool, led to the exposure of personal data from over 15 million users, and the full data set was released for free in July. A threat actor known as 'emo' exploited an unsecured REST API endpoint that allowed unauthenticated access to user profiles. Improper API configurations were at fault here.

3. The Internet Archive Breach
The Internet Archive, including its Wayback Machine, suffered a breach due to API vulnerabilities. Attackers accessed the data of 31 million users, exposing email addresses, usernames, and bcrypt-hashed passwords. Inadequate API security measures were linked to the origin of this issue.

4. The Snowflake Platform Compromise
Using stolen passwords, hackers accessed Snowflake's platform to extract sensitive data from global companies including Ticketmaster, Santander Bank, AT&T and 161 others. The scale of

the associated costs is huge with one victim, Advance Auto Parts, disclosing a $3 million loss in direct breach-related expenses. Weak authentication mechanisms and insufficient API access controls were found to be at fault.

Let's review what form these techniques took.

What common techniques were used to exploit APIs in 2024?

Cybercriminals are exploiting APIs through various techniques to access sensitive data, compromise systems, or disrupt services. Attacks observed in 2024 that are expected to continue in 2025 include:

1. Injection attacks

Attackers used SQL injection, XML injection, or another command injection by sending malicious payloads to API endpoints. Exploiting poorly sanitized inputs led to unauthorized database access or command execution.

2. Broken authentication and authorization

Weak or improperly implemented authentication mechanisms allow attackers to impersonate users, escalate privileges, or access restricted resources.

3. Excessive data exposure

Attackers have scraped sensitive data directly from poorly designed queries that lack data minimization principles and respond with more data than authorized.

4. Rate limiting and resource exhaustion (DDoS attacks)

Cybercriminals flood an API with requests, overwhelming the backend systems with APIs that don't have rate limiting protections.

5. Replay attacks and credential stuffing

Insecure APIs allow attackers to replay captured API requests or use stolen credentials to access resources.

6. Server-side request forgery (SSRF)

Attackers manipulate APIs to send unauthorized requests to internal systems, accessing sensitive internal resources or bypassing network restrictions.

Best practices for preventing API exposure

The increasing number of APIs and their use within the cyber ecosystem of companies will result in the exploitation of the supply chain as an attack vector to steal data in 2025.

For example, FireTail's 2024 API Security Report found that API data breaches increased by 80% year-over-year.

Here are several things to keep in mind for better API cyber hygiene.

1. Prioritize load balancing and rate limiting:

When developers spread traffic across several different servers, and limit how many actions people can run, they can ensure that the API service continues to run effectively.

These two measures will reduce latency and runtime, and make it harder for attackers to overwhelm a system through excessive API requests.

2. Review your authentication measures:

Deploying effective validation and authentication measures will mean that only authorized people can interact with the API. This reduces the chances of sensitive data being exposed to the wrong person.

Also, your authorization protocols should be regularly audited and reviewed for any loopholes or bugs that could turn into vulnerabilities in the future.

3. Justify the PII you process:

Before collecting any information for your system, ask yourself, "Do we really need to process this data?"

Focusing only on the essential data will reduce your attack surface as there is less sensitive information for hackers to exploit.

4. Optimize your API schemas:

Review all of your API responses to make sure they aren't delivering more information than necessary. You should also review all your error messages to ensure that they aren't delivering additional data.

By optimizing all of your API schemas, you can avoid letting sensitive information slip through unnecessarily.

As these themes and trends demonstrate, the consequences of API-related vulnerabilities can be severe, affecting millions of users and compromising critical systems. Strengthening API security must remain a top priority for organizations to protect their data and maintain trust in their digital ecosystems.

Section 4

APTs

The Striking Evolution of APTS

When we discuss Advanced Persistent Threats (APTs), we first need to be clear on the definition used. The term APT has changed in meaning and source over the years. It started as a term in the 2000s coined by Mandiant when identifying and cataloging Chinese attack groups.

Over the years, the focus has developed, broadening targets from defense and critical infrastructure to the private sector and supply chain. The attackers, once only nation-state actors, have bled into criminal elements. In Q3 2024 alone, organizations faced an average of 1,876 cyberattacks each—marking a 75% increase from the same period in 2023.

What has stayed the same but evolved, is the purpose. Let's explore the data that supports this evolving attack framework.

APTs then versus now

APTs use sophisticated attacks, and some tried-and-true methods, to infiltrate and maintain unauthorized access to a target network for an extended period. These are not the 'one-and-done' attacks used to monetize data or access for profit, but the long-term exploitation of networks, companies and infrastructure for disruption, large breaches and hybrid warfare.

APT groups in the early 2000s consisted of those powers who had the capabilities and wherewithal to conduct and sustain these programs. This included the Russians, Iranians, Chinese, North Koreans, and other Western powers. But due to AI, intelligence sharing and the growth of cyber expertise, smaller nations and independent groups are now in the mix.

Cybersecurity is about the management of risk. Depending on what you are trying to protect, the risk levels are not the same for all companies. What is consistent is the race between attackers and defenders. The CISO decides what to protect, based on risk, where to spend the budget and how to prioritize. The attackers use technologies like AI to increase the attack success, exploit vulnerabilities, and infiltrate.

But APTs are different. All adversaries are dangerous, but those with limitless time, money, and focus are on a different playing field.

What techniques were deployed by APTs in 2024?

In 2024, we saw the use of APTs in regional conflicts and the convergence with social media targeting (mainly via Telegram). In directing attacks they overwhelmed cybersecurity resources and postings were used to distort and influence the media.

Advanced techniques, supported by sophisticated nation-states, are the backbone of these attacks. They have focused on targeting the supply chain to distribute malware, including the use of AI chatbots.

APT groups have exploited zero-day vulnerabilities to infiltrate systems. For example, **Russian-linked APT29 (Cozy Bear)** conducted watering hole attacks by compromising government websites and exploiting unpatched iOS and Android vulnerabilities to target visitors.

Some APT groups have utilized legitimate software to avoid detection. The **BlackJack threat actor** used open-source tools and malware, including the LockBit ransomware and Shamoon wiper, to target government and industrial organizations. They also employed tunneling utilities like ngrok for persistent access. With the advancement of generative AI, APT groups have enhanced social engineering tactics to create convincing email threads and deepfake content.

These evolving tactics underscore the need for organizations to implement robust cybersecurity measures, including regular software updates, employee training on phishing awareness, and continuous monitoring of network activities to detect and respond to threats promptly.

These have been seen around elections, conflicts, major markets, and large social events in 2024. The continued use of social media, in conjunction with coordinated attacks on infrastructure, has increased and will increase in 2025 and the years to come.

Three key cyber APT campaigns in 2024

What can we learn from the most prevalent attacks last year?

1: Earth Baku (APT41) global campaign

Earth Baku (also known as APT41) launched data exfiltration attacks against global shipping, logistics, media, technology, and automotive sectors across multiple countries. The group used variants of known malware and public tools to infiltrate organizations and maintain persistence since 2023. This campaign highlights the need for robust defense against sophisticated, multi-tool attacks.

2: Andariel (APT45) escalation

Andariel, a North Korean hacking group with military ties, significantly expanded its operations in 2024, targeting sensitive military information and intellectual property in the defense, aerospace, and engineering sectors. The group combined ransomware attacks with cyber espionage, particularly focusing on US medical institutions. This incident underscores the growing trend of APTs diversifying their attack methods and targets.

3: Ivanti connect secure exploitation

Attackers, initially linked to the **UNC5221 group**, actively exploited critical vulnerabilities (CVE-2023-46805 and CVE-2024-21887) in Ivanti Connect Secure and Policy Secure products. This campaign allowed attackers to bypass authentication and execute arbitrary commands, leading to a sharp increase in threat actor activity from January 11, 2024. The incident highlights the importance of prompt patching and vulnerability management.

Best practices for preventing APT threats:

1. Conduct regular vulnerability assessments:
Regularly test your systems to identify and patch vulnerabilities before attackers can exploit them.

2. Educate your team:
Train employees to recognize phishing attempts and other social engineering tactics used by APT groups, and to follow data protection protocols.

3. Monitor your supply chain:
Vet third-party vendors and implement security protocols to reduce the risk of supply chain attacks.

4. Invest in threat intelligence:
Use services that provide real-time data on potential threats targeting your industry, such as CybelAngel, which offers comprehensive digital risk management with actionable threat intelligence across surface, deep, and dark web sources.

Section 5

Exposed Assets and IoTs

What do the Rising Numbers of Exposed Assets and IOT Devices Mean?

Why are cybersecurity watchdogs so concerned about the exploitation of exposed assets and IoT devices?

When we examine the data, things become a lot clearer.

The numbers from 2024 are a pointed reminder of how an ever-increasing attack surface, combined with the proliferation of interconnected devices, and weak security measures, make it a hacker's playground. And the total number of connected IoT devices will double to approximately **40 billion by 2030**.

There's also the associated surge in DDoS attacks. Last year Cloudflare blocked **21.3 million DDoS** attacks, marking a **53% increase from 2023**.

These vulnerabilities pose substantial risks across industries, with adversaries targeting IoT devices for lateral movement, data exfiltration, ransomware deployment, and botnet creation.

What patterns are these hyper-volumetric attacks following?

Many factors have contributed to the increased discovery and targeting of exposed assets. The rise in internet-facing systems, cloud misconfigurations, and shadow IT has led to a surge in exposed assets. Tools like **Shodan, Censys,** and **Nmap** enable attackers to locate exposed devices with little effort. Attackers have and will continue to target misconfigured databases (e.g., **Elasticsearch**, **MongoDB**), exposed APIs, and unpatched legacy systems.

In 2024, CybelAngel tracked a 20% year-over-year increase in the number of exposed databases (open and unsecured, mainly due to user negligence).

Within the exposed databases the top six table names exposed were:

Table name	Risk	Threat
system.version	Contains metadata on system's version, software, or database.	**Fingerprinting:** Attackers identify the exact version of the system or database, which may be vulnerable to known exploits. **Targeted Attacks:** Enables attackers to craft specific exploits or use pre-existing attack tools tailored for that version.
system.sessions	Store active session data for logged-in users or applications.	**Session Hijacking:** Tokens or cookies stored in plaintext, attackers hijack active sessions to impersonate legitimate users. **Privilege Escalation:** Compromising admin or privileged user sessions **User Enumeration:** Insights into active sessions reveal usernames or patterns, aiding brute-force or credential-stuffing attacks.
README	Contains documentation or instructions about the system.	**System Insights:** README files often include details about system setup, configuration, or usage. **Credential Exposure:** Some poorly managed README files might contain hardcoded credentials or sensitive information. **Attack Guidance:** Descriptions of system components or functionality could guide attackers in crafting tailored exploits.
transactions	Contains records of system transactions, such as financial data, user actions, or logs.	**Sensitive Data Exposure:** Financial or personal data exposed. **Regulatory Violations:** Breach of transaction records resulting in violations of GDPR, CCPA, or PCI-DSS. **Reconnaissance:** Patterns in transaction data can reveal system behavior or vulnerabilities.
startup_log	Logs related to the system or application startup process, including configuration details and initialization sequences.	**Configuration Exposure:** Could reveal system paths, services, or applications initialized at startup. **Credential Leakage:** Exposure of plaintext credentials or API keys used during initialization. **Exploit Guidance:** Identification of weak points, such as improperly secured services or misconfigurations.
accounts	Likely contains user account information, such as usernames, email addresses, or hashed passwords.	**Credential Theft:** Unsecured passwords lead to access of accounts and ATO. **Privilege Escalation:** Admin or privileged accounts targeted. **Phishing & Social Engineering:** Used for intelligence to create convincing phishing campaigns.

Figure: Exposed Database Trends 2024

Why did vulnerable assets grow 68.28% YOY?

CybelAngel processed data that identified a significant increase in assets and associated vulnerabilities detected in 2024 — a **68.28% increase to be precise**. Our data highlights how the attack vector is widened due to decentralized and fragmented IoT ecosystems.

IoT devices often have poor security hygiene: weak or default credentials, outdated firmware, and lack of encryption. Devices like surveillance cameras, routers, smart thermostats, and medical devices are frequent targets.

In 2024, more and more compromised IoT devices were used to infiltrate supply chains.

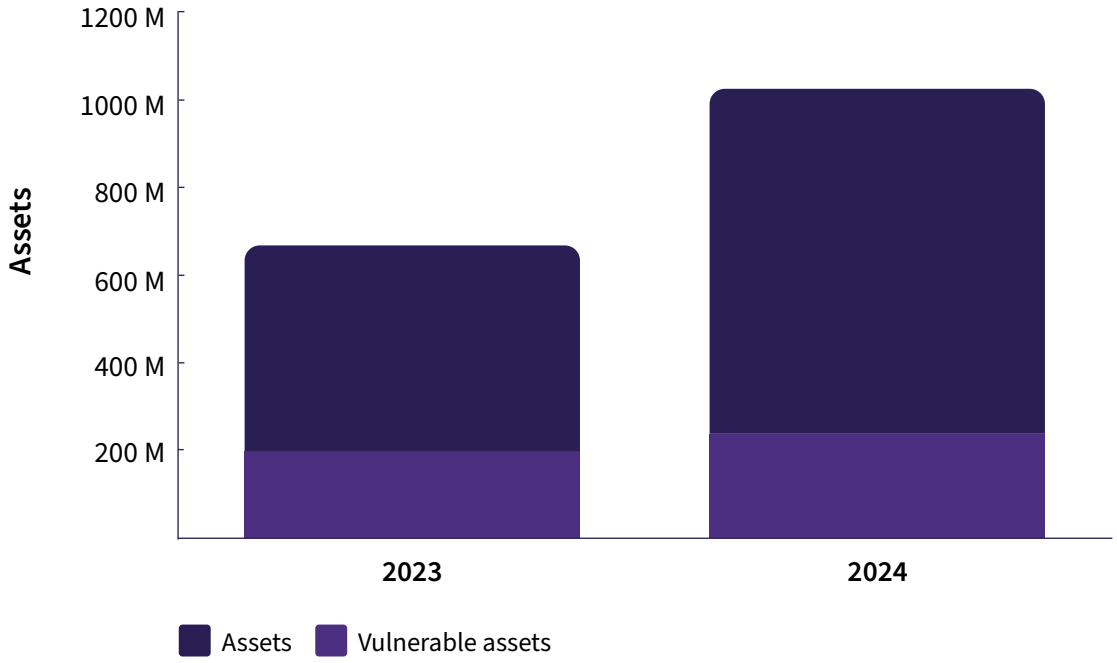

Figure: *The growth of vulnerable assets YOY date 2023 v 2024.*

Continuing ignorance of the threat to these devices is increasing the risk to companies' abilities to conduct business including physical safety, especially in the healthcare fields. Downtime, reputational damage, regulatory issues and financial losses, are several of the concerns along with the security and integrity of data. This entry point has been and will continue to be targeted by attackers for deeper network breaches.

By addressing these trends and leveraging robust security practices, organizations can better defend against the growing risks associated with exposed assets and IoT devices.

Four IoT exposure lessons we need to learn from 2024

The Smart Home Invasion

Attackers gained unauthorized access to thousands of smart home devices, including locks,

security cameras, and thermostats, by exploiting weak passwords and default settings. This breach compromised consumer privacy and posed potential physical security risks. Implementing strong authentication and encouraging users to change default credentials could have prevented this incident.

The Hospital Ransomware Crisis

A ransomware attack on connected medical IoT devices in several U.S. hospitals forced a reversion to manual procedures, disrupting patient care. Compromised patient monitoring systems, infusion pumps, and MRI machines highlighted the dangers of outdated security patches and insufficient pumps, and MRI machines highlighted the dangers of outdated security patches and insufficient network segmentation in healthcare facilities. Regular security updates and proper network isolation could have mitigated this threat.

The Hospital Ransomware Crisis

A ransomware attack on connected medical IoT devices in several U.S. hospitals forced a reversion to manual procedures, disrupting patient care. Compromised patient monitoring systems, infusion pumps, and MRI machines highlighted the dangers of outdated security patches and insufficient.

The Manufacturing Mayhem

European manufacturing plants fell victim to IoT-based attacks, resulting in disrupted production, manipulated machinery, and halted production lines. Attackers exploited vulnerabilities in Industrial IoT systems, including weak communication protocols and outdated security measures. Implementing robust security protocols and keeping systems up-to-date could have prevented significant financial losses.

The Botnet Surge

A malicious actor known as “Matrix” turned IoT devices into a global botnet for large-scale DDoS attacks. The threat actor targeted connected devices with known vulnerabilities, deploying Mirai botnet malware on infected machines. Regular vulnerability assessments and prompt patching of IoT devices could have thwarted this massive botnet formation.

What critical attack vector factors will drive this surge in cyber attacks in 2025?

As long as IoT devices are ignored, they will continue to be used to attack, disrupt and impact companies. These attacks have increased in size and significance in 2024 and will continue as the number of unpatched, unsecured, and vulnerable devices continues at an alarming rate.

Verizon’s 2024 Data Breach Investigations Report, found that **14% of breaches** began with vulnerability exploitation as the initial access method—nearly three times higher than the previous year.

Without identification of these devices through detection and management of exposed assets and IoT devices along with mitigation measures (patching, segmentation, zero trust principles), attackers will exploit at a greater rate influencing the efficiencies and security of those devices.

Best practices for protecting exposed assets and IoT devices

1. Comprehensive asset discovery:

Implement continuous asset discovery tools to maintain an up-to-date inventory of all web-connected devices on your network. Use both active scanning and passive monitoring techniques to identify shadow IT and rogue devices. CybelAngel's Asset Discovery and Monitoring solution offers a unique combination of pivoting and keyword matching technologies to provide an exhaustive, real-time map of your entire external digital landscape, uncovering hidden assets and vulnerabilities before they can be exploited.

2. Rigorous patch management:

Establish an automated patch management system for all IoT devices, especially easily patchable ones like printers. Prioritize critical vulnerabilities and set up a regular patching schedule to minimize exposure windows.

3. Advanced network segmentation:

Go beyond basic VLAN segmentation. Implement microsegmentation using EVPN-VX-LAN architecture to isolate IoT devices at a granular level. This approach provides enhanced security, visibility, and control while maintaining network flexibility.

4. Implement zero trust principles:

Apply zero trust architecture to your IoT environment. Verify every device, user, and application before granting access, regardless of their location within the network.

5. Enhance monitoring with AI/ ML:

Leverage artificial intelligence and machine learning for real-time threat detection and anomaly identification. These technologies can help identify patterns and potential security breaches that might be missed by traditional monitoring tools.

6.Deploy Data Security Platforms (DSP):

Utilize AI-enhanced DSPs to provide comprehensive data protection, including threat detection, access management, and regulatory compliance for your IoT ecosystem.

7. Conduct regular security assessments:

Perform frequent vulnerability scans and penetration tests specifically targeting your IoT infrastructure to identify and address potential weaknesses.

Section 6

Phishing

Essential Phishing Trends that Shaped 2024

One trend which continues to frustrate CISOs is phishing attacks, today, yesterday, and always.

Yet as much as CISOs attempt to combine training and technology to mitigate the risk evolving from phishing, the statistics on the number of attacks and their impact continue to grow year over year. Between 2022 and the end of 2024, attacks have increased as much as 1,000% with the majority of the attacks targeting credentials.

CybelAngel's requests for takedowns of fake domains surged by 116% in 2024 compared to 2023.

The increased use of AI and the ability of the attackers to produce a cleaner and more convincing attack has resulted in greater numbers of successful attempts. The FBI reports that email compromise scams with businesses have resulted in over $50 billion in losses since 2013.

The typical techniques used by attackers usually kick off with the creation of a fake deceptive domain. These techniques have been around for years but are the building blocks to a good and successful attack:

- Domains which closely resemble legitimate domains of the target by omitting or adding characters.
- Using characters from other alphabets which resemble ASCII characters to create deceptive domains.
- Registering domains with common typographical errors to misdirect traffic.

Not only are these sites used to harvest credentials, but they are also the basis for other attacks including the distribution of malware, loggers, and other malicious software.

AI-fueled attacks are enhancing classic phishing attacks

The emergence of AI for the average user is a double-edged sword. While it can be and is often used for good, attackers are using it to enhance their capabilities. **As a friendly reminder, since ChatGPT was released in November 2022, the volume of phishing emails has increased by 1,265%.**

Here are some ways AI has increased phishing efficacy:

- **Leveraging publicly available data** scraped from social media and corporate leadership biographies are being used to elevate the quality and efficacy of messages. The ability to mimic styles of communication, reference details, and use highly relevant content is realistic.

- **AI has increased the effectiveness** of phishing emails. While training can help employees find grammatical mistakes, non-vernacular language, and poor formatting amongst other things, it does not account for more subtle tweaks from AI. Now the attack vector has increased the ability to write fluidly for the most part, in multiple languages to scale orchestrated attacks.

- **The use of AI means** that the pressure of attacks has evolved hugely (67.4% of all phishing attacks utilized some form of AI last year). The use of AI is up to the user, as well as the controls placed on the depth of request. Attackers are using models to develop the next generation of threat vectors—like automated responses based on the click timing and response and the use of AI to mimic human responses in conversations. CybelAngel's Brand Protection solution combats these threats by detecting phishing campaigns, identifying fake websites, and monitoring for brand abuse across the surface, deep, and dark web, providing early warnings to mitigate potential breaches.

- **Other uses of AI** in phishing include lowering the bar for attacks with available phishing kits, creating believable websites, mimicking social media sentiment to target victims, and the use of deepfake voice and video in vishing to increase deception.

What patterns are we seeing within AI phishing attacks?

To evolve our defenses we should also focus on data from AI detection tools integrated into email systems. These can distinguish between machine-generated and human-created content. Additionally, data from domain monitoring services around companies and brands is crucial.

Statistics on the effectiveness of increased ICANN regulations and registrar accountability measures in blocking fake websites would provide valuable insights. These data points can help us quantify the impact of AI-driven threats, track the proliferation of malicious domains, and measure the success of regulatory efforts in curbing online fraud. This could make all the difference to your defensive strategies.

Understanding the key biases that social engineering attack scams exploit

Hackers are often armed with solid intel about their targets. You'll need to be just as familiar with how they leverage these cognitive biases in their attacks.

Here is a checklist of classic biases to be wary of:

1. **Authority bias:** Attackers impersonate figures of authority, such as executives or IT managers, to manipulate victims into divulging sensitive information or performing actions that compromise security.

2. **Reciprocity bias:** Social engineers offer help or rewards in exchange for information, exploiting the human tendency to return a favor.

3. **Scarcity bias:** Creating a false sense of limited availability or time pressure to spur victims into hasty actions, such as clicking on malicious links or providing sensitive data.

4. **Social proof:** Hackers exploit the tendency to follow others' actions by making it seem like peers or colleagues have already complied with their requests.

5. **Urgency bias:** Attackers create a sense of time pressure, forcing victims to act impulsively and bypass rational decision-making processes.

6. **Optimism bias:** Cybercriminals take advantage of people's tendency to overestimate positive outcomes and underestimate risks, often through fake job opportunities or insider information scams.

Overall, educating your wider team about these subtle manipulation tactics is crucial. Social engineering attacks work for a reason, but understanding these biases will help you and your team safeguard critical sensitive information from unauthorized access.

Section 7

Criminal Forums

Changing Dynamics Within Criminal Forums

Year over year, some things remain remarkably consistent.

When we examine trends in monetizing data, IP hacking upticks, and the old favorite "open door" unauthorized access, cybercriminals in the trenches have consistently focused on their end goal.

Whether they are deploying ransomware to make money or exploiting data, seemingly their motivation remains high. This trend is unwavering.

There are always groups and individuals who believe in the disruption of the digital world for a cause. These players prefer partnering up, as their ability to make a major impact is diminished unless they collaborate with financially motivated groups.

But what about their means and methods of communicating? This is one critical piece that has changed massively.

Let's look at the data we found tied to this.

Dark web channels shift: Telegram rises, Tor fades

CybelAngel pivots to monitor the areas where the criminal actors are talking, selling and discussing our clients. We look for mentions, discussions, access and data for sale, and other indicators of attack and/or targeting. Over the years, we have seen the movement of these groups from Tor access-only locations to more mainstream platforms available on the open web.

Board	2022	2023	2024	Total
openweb	2,846,889	4,716,598	4,849,936	**12,413,423**
tor	2,790,524	3,429,516	1,500,840	**7,720,423**
telegram	454,006	900,409	2,129,617	**3,484,332**
Bitcoin	394,131	286,941	764,610	**1,445,682**
discord	12,469	77,245	98,390	**188,104**
hacking	53,890	58,072	51,566	**163,528**
forum	42,183	32,990	46,696	**121,869**
darknet	44,516	51,769	23,466	**119,751**
onions	20,904	19,756	12,820	**53,480**
Total	**6,882,599**	**9,723,007**	**9,501,934**	**26,107,540**

Figure: *An overview of the shift in cybercriminal communication channels from 2022-2024*

By looking at the top ten locations where CybelAngel finds mentions of potential criminal activities directed at our client base, we see what the community might find unexpected. The use of Tor-derived sites is decreasing with cybercriminals preferring to communicate on open-source sites or apps like Telegram.

From 2023 to 2024, **Bitcoin, Discord, and Telegram** channels experienced substantial growth, with **Bitcoin leading at 148.42%, followed by Telegram at 70.54% and Discord at 53.19%**. Conversely Onions, and Darknet channels saw significant declines during the same period, with **Onions by 49.88%, and the Darknet by 38.96%**. Tor channels experienced a **47.74%** decline too.

CybelAngel data highlights the contrasting trends in different online channels, with **cryptocurrency and encrypted messaging platforms** showing significant growth, while some t**raditional dark web communication channels experienced notable declines**.

The image of the dark web certainly shifted further in 2024. For example, the shutdown of notable marketplaces like Rydox, Manson, Hydra, and of course, Lockbit, disrupted criminal communities. We can see this especially in relation to narcotics. Throughout 2024, traffic on dark web marketplaces for drug sales has been declining in favor of regular social media platforms as well as encrypted messaging apps like Telegram or WhatsApp.

Its accessibility meant that Telegram continued to be a popular channel for CybelAngel to monitor. But changes within the platform made for an interesting divergence for cybercriminals.

A Telegram crisis in 2024 spurred a break channel overhaul

In 2024, cybercriminals significantly increased their use of open web services and communication channels, mirroring mainstream users' behavior. This shift occurred with little fear of law enforcement identification, due to either cooperation or inaction by service providers.

The catalyst came in August 2024 when Telegram's CEO, Pavel Durov, was arrested in France on charges related to illegal activities on the platform. This event triggered a series of policy changes that reshaped the digital underground.

In September 2024, Telegram announced a major update to its privacy policy. The new policy mandated that Telegram would share user data, including IP addresses and phone numbers, with authorities in response to valid legal requests. This marked a significant departure from Telegram's previous stance, which only disclosed data in cases involving terrorism.

Despite these changes, the impact on illegal activities has been less pronounced than anticipated. Telegram has attempted to balance privacy and security, implementing AI and user-reported channel moderation to remove illegal and harmful content. However, the platform continues to be a hub for cybercriminal activities, including financial fraud, malware distribution, and data theft.

The long-term effects of Telegram's policy shift remain uncertain. While some criminal groups have begun migrating to alternative platforms, many established cybercrime marketplaces are hesitant to abandon Telegram entirely. The platform's features, such as bot automation and large file-sharing capabilities, continue to make it an attractive option for illicit activities.

How will threat intelligence shape cyber resilience in 2025?

Threat intelligence has historically been miscategorized by those who are driving the market. It extends far beyond traditional metrics like dark web monitoring, indicators of compromise (IOCs), hash values, and isolated security events.

Cyber Threat Intelligence (CTI) is the backbone of modern cybersecurity. However, while CTI has traditionally focused on reactive measures—waiting for indicators of compromise—our approach to it must evolve.

To stay ahead of increasingly complex threats, organizations in 2025 must embrace a proactive mindset. **This means shifting from merely identifying risks to actively preventing them. Proactive threat intelligence leverages continuous monitoring, behavioral analysis, and advanced tools like artificial intelligence to detect and block threats before they escalate. The future of CTI lies in integrating proactive strategies with advanced technologies. This includes systems that correlate data across ecosystems—linking inventories, threat indicators, actor profiles, and risk assessments—to create a comprehensive defense strategy**. Doing so means that organizations can reduce risk exposure, enhance situational awareness, and improve their incident response times—a winning formula for any CISO and SOC team.

As we move further into 2025, the convergence of cybercrime with espionage and geopolitical tensions highlights the need for robust CTI frameworks. Industries like energy and manufacturing are increasingly targeted due to their critical roles in global supply chains.

We all need to invest in systems that not only detect but also neutralize threats in real time. The lesson for 2025 is clear: waiting for signs of compromise is no longer enough. A proactive approach to threat intelligence is the only solution.

Section 8

Here’s to 2025

3 Critical Attack Vectors Targeting Enterprise Infrastructures in 2025

What were the most pertinent threats we uncovered last year that could help you to prioritize the biggest risk vectors?

Of course, our recommendations vary per region and you need to keep geography into account.

Here are three notable patterns we've tracked when sifting through 192 million data points from the biggest threats last year.

1: The increase in the last five years of attacks on the enterprise coming from the supply chain will continue into 2025

The old saying, "**attack at the weakest point**," is more true today than it has ever been. The vast number of partners, vendors, and third parties that either contribute to or are part of the cyber ecosystem of a company nowadays is growing. Attacking these weaker points to pivot has increased and will continue without robust monitoring of the entire ecosystem.

With a 68% year-over-year increase in vulnerable assets, plus an acceleration of ransomware attacks on the supply chain, we are all in dire need of visibility across our cyber ecosystems. You can't protect what you can't see. Understanding the threat vectors, the weaknesses, and the risks associated with the entire enterprise will allow cybersecurity professionals to be proactive and not reactive to events.

2: AI will continue to be a hot topic utilized in attacking and defending but also for data security in 2025

Attackers are using AI-generated malware, automated phishing using personalization and messaging at scale, along with AI-trained and controlled bots. This will increase the attack surface while accelerating the speed and volume of attacks. On the defender side, we see the use of AI to help drive detection and response. It also delivers predictive analytics with threat intelligence and assists SOCs in the ability to triage threats.

The main concern is the way we use AI and feed LLMs. We will see more attacks to exploit these large data sets, hold them ransom and put our IP at risk. We have already seen the fight on which AI platform to use, and now we will see an increased fight to break them.

3: API targeting will increase due to value, lack of monitoring, and inattention by security teams

We will see more automated, AI-driven and business logic-based attacks. These attacks will target the supply chain, the misconfiguration of access by developers, and the ignored and old APIs which still

accept requests but lack security updates and monitoring. Attackers will continue to focus on APIs to gain access, disrupt via ransomware and DOS attacks, and monetize the results (such as data, access, keys, and control).

The increasing reliance on APIs for mobile applications, cloud services, and business operations make this an attractive attack vector. Awareness of APIs in the inventory and their access, purpose, and security coverage is vital moving forward for companies.

CONCLUSION

The Last Word

Let's consider one recent example to put this into perspective.

The European Space Agency (ESA) experienced a significant cyberattack in early 2024. The breach was discovered in the spring when cybersecurity researchers alerted ESA its systems were compromised. The attackers gained access to the agency's cloud infrastructure, a crucial component overseeing ESA's data storage and processing operations. This infrastructure contained critical information, including research data and mission plans, significantly increasing the breach's potential impact.

ESA responded by collaborating with international cybersecurity experts and law enforcement as part of an ongoing investigation to determine the extent of the security compromise. Notably, this incident is not the first security breach for ESA. It faced similar attacks in 2021 and 2022 when several European space-related research institutions experienced a widespread cyber assault. Those attacks were attributed to a group of state-sponsored hackers.

It is suspected that the compromise resulted from exploiting vulnerabilities in the cloud infrastructure, and access may have been illicitly obtained through sophisticated phishing or supply chain attacks.

Could this have been prevented? Was this incident caused by state actors using advanced techniques?

What we can gather from this attack is that history tends to repeat itself.

ESA, being an important and strategic target with valuable data and intellectual property, holds great significance to Europe, its partners, and the global space community.

1. What protections are they using to detect exposed credentials via the dark web, available for sale or exposed via malware?

2. Do they even know what vulnerabilities they have and what can be seen from outside their networks?

3. Do they know their trusted partners and suppliers, or lack thereof, is increasing their risk of the next attack?

4. How many times are you going to do the same activity and expect a different response?

This report has reflected on a challenging year in cybersecurity. Attacks are up, breaches are up, and the resulting impact on business has been felt through fines, investigations, rulings, and market impact. All of this has occurred at a time when the global economy is facing uncertainties, multiplying the impact of these breaches.

We all continue to examine threats across all sectors, assess their impact and probabilities to evaluate our risk while looking for ways to mitigate, pivot and defend. The fight is not only within your teams but your partners must be part of the solution—the team fight.

Challenge your partners to determine what can be done together. Challenge them to address the needs of today's growing threats, from both familiar and new attack vectors. Challenge them to be on the cutting edge of detection technology and ask what they are doing to prevent you from being a target and victim.

At CybelAngel, we pride ourselves on our innovative approach to cybersecurity. We work with our clients to shape our technology to address and tackle today and tomorrow's threats.

About the Author

Todd Carroll joined CybelAngel in 2019 as the CISO & SVP Global Cyber Operations, bringing with him over 20 years of experience in the U.S. Federal Bureau of Investigation's cyber, counterintelligence and counterterrorism branches. In 2024 he was named President of CybelAngel USA.

Mr. Carroll is instrumental in evangelizing CybelAngel's External Attack Surface technology throughout North America and is responsible for managing the Global cyber operations team. Prior to joining CybelAngel, Mr. Carroll served as the Deputy Special Agent in Charge of the FBI's fourth largest field office, in Chicago, where he oversaw investigations related to cyber and physical security, threat intelligence, risk analysis, compliance, insider threat identification and mitigation strategy.

Scan, Prioritize, Resolve External Threats

CybelAngel is the world's leading platform for External Attack Surface Management.

Secure your digital activities with CybelAngel, the only comprehensive threat Intelligence provider.

START NOW