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

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.