# 2024

# State of the External Attack Surface Report

## Executive Summary

CybelAngel

# INTRODUCTION BY TODD CARROLL
## CISO & SVP GLOBAL CYBER OPERATIONS

### The State of External Attack Surface Management in 2023

CybelAngel scanned 6 billion data points on the internet each day in 2023 to keep our clients' data secure. During this period the cybersecurity landscape deftly weaved in between new major global challenges.

2023 will be remembered for the magnitude of its technological advancements but also for the stealth and scale of its cybercriminal activity. Attackers have adapted and continue to hone their techniques, as highlighted in this executive summary of our 2024 State of the External Attack Surface Report.

**Here are the most critical data snapshots we uncovered in 2023:**

1. The number of exposed data doubled in 2023, from 740,000 to 1.5 million TBs.
2. 79% of all alerts we processed came from outside our client's  IT perimeter.
3. Exposed data from cloud services increased by 11% over 2022 data.
4. Ransom demands have increased by 40% due to the development of RaaS (ransomware-as-a-service) services.

These data snapshots underscore the critical importance of defending your external attack surface. They also emphasize the critical importance of robust cybersecurity measures to mitigate data exposure risks, confidentiality, integrity, and availability principles to thwart adversaries and safeguard sensitive information.

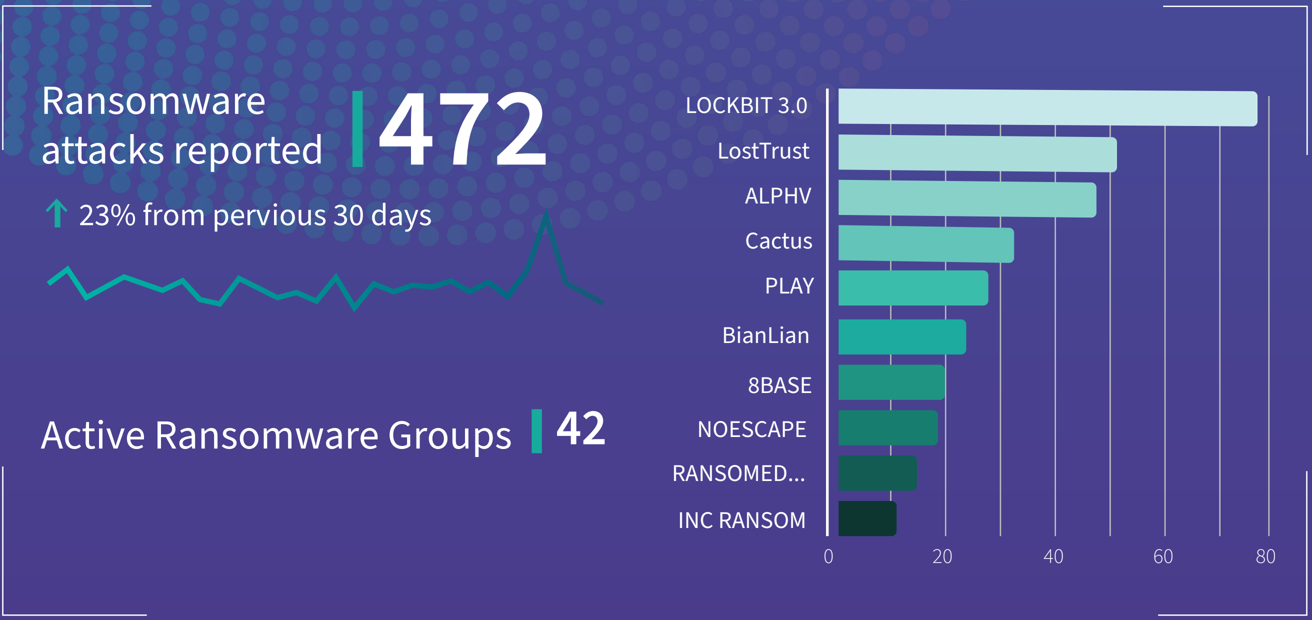
We hope that you will find this executive summary of **CybelAnge's 2024 State of the External Attack Surface Report** a guide for a more secure 2024.

# 3 UNIQUE VANTAGE POINTS:<br>3 MAJOR CYBERSECURITY RISK AREAS

**Here is an executive overview of three trends from three critical areas of cybersecurity, including, ransomware, malware (infostealers), and third party threats. To unveil all of the trends featured in our annual report, download it here.**

## Ransomware

In 2023, CybelAngel identified and tracked 62 active ransomware groups involved in over 5,000 known and reported attacks across 132 countries.



Ransomware attacks reported | 472

↑ 23% from pervious 30 days

Active Ransomware Groups | 42

*Figure: An example of internal data concerning ransomware reporting by CybelAngel in September 2023.*

### Trend

Ransomware incidents are being underreported as more companies opt to pay the ransom and assume the associated risks instead of addressing the underlying problems. However, identifying the vulnerabilities in the first place can significantly reduce the threat.

As Ransomware-as-a-Service (RaaS) gains popularity and more data, cloud shares, and databases become exposed, this trend will continue to rise. Expect attackers to explore new and increasingly sophisticated methods, such as data alteration and leveraging increased computing power, in their ransomware attacks.

## Infostealer Malware

In one month alone, September 2023, CybelAngel was able to detect, capture and alert our customers on over 7,500 exposed and compromised credentials.

Infostealer malware, such as Redline, Vidar, Racoon, Steal, Cryptbot, Azorult, Aurora, and others, capture data and transmit it in bulk to malicious actors.

**7.6K** **Exposed & Compromised Credentials Per Month**

### Trend

Infostealers is a prime example of cybersecurity companies using technology to capture data quickly, provide it to clients and help reduce the impact from this threat vector. It has been and always will be a race between malicious actors and providers to report and secure it before this data can be exploited. Monitoring these groups, channels, and forums for any mentions of your company or organization can be arduous and time-consuming, especially with the rise of ransomware and data on the dark web. To exacerbate the issue, some groups rent out their tools and services through Ransomware-as-a-Service (RaaS), making it difficult to determine the identity and motives of the attackers.

# Third Party Threats

Out of the over 5,000 alerts sent to clients covering data breach prevention in 2023, 79% of the causes of origin came from outside the perimeter. This means that data was exposed by partners, suppliers, law firms, HR providers, insurance, and other third parties, all in violation of the data security clause inside every single MSA.

One area of increasing concern (and one that CybelAngel monitors) are exposed codeshare repositories. These platforms and websites serve as spaces where our coders, engineers, and other professionals come together to share ideas, post questions, and showcase their results. However, there is often a risk of oversharing sensitive information. Examples of such platforms include Github, which CybelAngel continuously scans 24/7 to identify exposed API keys, passwords, access credentials, and other potential vulnerabilities.

Github, boasting a user base of over 94 million, is of particular interest. In October 2023 alone, CybelAngel detected an average of over 37,000 keyword mentions in repositories per customer. However, it is important to note that 98% of these instances are false positives, simply mentioning the client without any actual risk present. CybelAngel's advanced technology enables us to filter through the noise and deliver only actionable alerts to our clients, specifically identifying genuine risks. As a result, we have observed an 11% increase in true positive alerts reported to our client base in 2023 compared to 2022, solely attributable to findings on Github.

**79%** of the causes of origin came from outside the perimeter.

## Trend

As developers are pressured to produce more code and APIs within time constraints, we can anticipate that these numbers will either increase or stay relatively close. CybelAngel will continue to monitor and scan new areas where this type of information is inadvertently shared and provide access points into the infrastructure.

# RECOMMENDATIONS FOR 2024

The state and size of the external attack surface are attack vectors that cannot be ignored. This vector of attack is growing year over year. CybelAngel and other organizations have demonstrated the scope and depth of the attack surface resulting from the expansion of the supply chain, third-party involvement, increased applications, and new technologies, which is now larger than ever.

**So, what can be done about this?**

Risk identification, management, and mitigation must consider the external attack surface in all cybersecurity programs.

## Multiple Solutions to Reduce This Risk

1 **Cyber Insurance/Risk Transfer**
Not so fast ... Lloyd's of London issued a warning about a major cyber attack on a global payments system that could potentially cost the world economy $3.5 trillion. This warning highlights growing concerns among insurers and policymakers about the insurability of cyber attacks, with some calling for state-backed solutions in case of wide-ranging or infrastructure-affecting attacks. Although cyber insurance is a rapidly growing market, expected to reach up to $25 billion in premiums by 2025, it still represents a small portion of potential economic losses from cyber threats.

2 **Ignore the Risk/Risk Acceptance**
As mentioned previously, why take the risk? In a world where it's not a matter of if, but when, it's wise to be proactive and prevent leaks from turning into breaches by utilizing an affordable and preventative service.

3 **Wait and See - High Costs That Keep Increasing**
In 2023, the average cost of a data breach reached a record high of approximately $4.45 million according to the Ponemon Institute and IBM Security, as published in their "The Cost of a Data Breach Report 2023." This represents a 2.3% increase from the previous year. Is this a cost you are willing to absorb? Are you willing to gamble on an impact which cannot be quantified?

4

### Risk Avoidance

It's not really feasible to completely halt the sharing of data outside the network, to cease relying on third parties, to dismantle your supply chain, or to stop leveraging the internet to improve efficiencies. However, gaining visibility into what is happening outside your immediate scope is an option that can help mitigate this risk.

5

### Risk Sharing

While the approach involves collaboration and partnerships, do we believe that the current processes such as questionnaires and limited vulnerability scans are sufficient? How many of the companies listed in this report included these actions as part of their risk mitigation strategy? I would venture to guess that all of them did. How did that ultimately work out for them?

6

### Patch Management/Training/Awareness

These are the backbone of cybersecurity programs and part of what is called good cyber hygiene. They are crucial activities that serve as building blocks for developing comprehensive programs, but it's important to note that they are not the ultimate solution.

7

### Continuous Monitoring and Detection

Ongoing monitoring of internal systems has long been a fundamental aspect of cybersecurity programs. However, in today's environment, this alone is not sufficient or the final solution. Obtaining both an internal and external view of your company's cyber "ecosystem" enables you to identify risks that extend beyond your immediate environment. It provides valuable insights into your interconnectedness, how you may be affected, and where your highest risks may lie.

# 3 CRITICAL THREATS TO WATCH OUT FOR REGARDING EASM IN 2024

As we prepare our projections for 2024 and beyond, we all seek to understand the future and what may be the next threat on the horizon. At CybelAngel, we have tracked the increase of the risk and attacks coming from the external attack surface and we have little doubt that this trend will subside.

**Here are three of the most critical threats to be aware of:**

## 1. The external attack surface will continue to be the hacker's playground.

This problem will persist and worsen. If we look at the trends in this report alone, the attack surface is expanding rather than shrinking. The more we rely on remote employees, cloud storage and connected infrastructure, the more vulnerabilities there will be in these services, offerings and the human behind them who can be targeted.

## 2. The increase of attacks on corporate networks via third parties is a significant concern.

This can be attributed to the old saying "path of least resistance" or "attack the weakest link." The past few years have demonstrated that this is a viable and actionable vector for attacks, leading to major breaches and incidents. This pattern will continue and even intensify in 2024.

## 3. Ransomware attacks and their impact on companies will increase in 2024.

Enforcement and shutting down of ransomware groups will not be enough to slow down this trend. As these groups seek to exploit stolen data further, they will explore new means to monetize it at the time of the attack or through subsequent releases. The solution to ransomware lies in understanding what is not adequately protected and publicly exposed, so that it can be secured appropriately.

# Scan, Prioritize, Resolve External Threats

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

Secure your digital activities against cyberattacks and cyber breaches.

**Learn more:** https://cybelangel.com/
**Dive deeper:** https://cybelangel.com/blog/

**Stay connected** in X

START NOW