FLASHPOINT

Flashpoint's Cyber Threat Intelligence Index: 2024 Midyear Edition

Data, insights, and key takeaways on the most impactful, persistent, and emerging cyber threats of 2024—from vulnerabilities and ransomware to infostealers and insider threats.

Table of Contents

Enhance Security Readiness

The cyber threat landscape is a volatile and ever-changing arena where new threats constantly emerge and old ones evolve at a rapid pace. As a cybersecurity practitioner on the front lines, staying ahead of these threats is not just a goal, but a necessity.

Flashpoint's *Cyber Threat Intelligence Index: 2024 Midyear Edition* presents critical data and trends surrounding both persistent and emerging cyber threats observed from January 1 to June 30, 2024. Using this intelligence, organizations can identify areas of opportunity to fortify their defenses and set up teams for success in anticipating potential threats—helping them to better protect people and assets alike.

Vulnerabilities

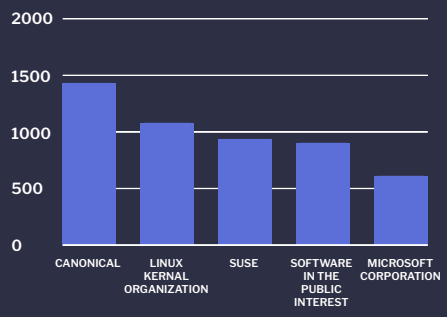
Vulnerabilities continue to be a rising threat vector as 2024 unfolds, as witnessed in the headlines and reflected in Flashpoint's data. So far this year, vulnerabilities have risen by 11% and the availability of publicly known exploits has increased by 6%. To mitigate the risk of exploitation, organizations must continue to harden exposure management programs that prevent unauthorized access and the installation of malicious software such as infostealers and ransomware.

Vulnerability Quickview

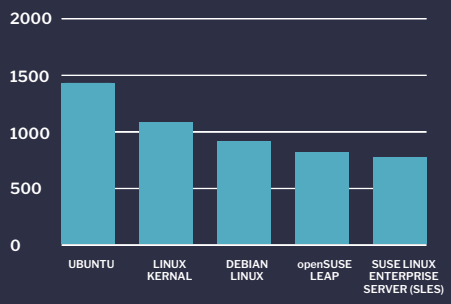
Midyear 2024

17,518	936	22,032	7,993
VULNERABILITIES DISCLOSED	VULNERABILITIES WITHOUT CVE ID	VULNERABILITIES YTD	HIGH OR CRITICAL (CVSSv2)

Vulnerabilities by Vendor



Vulnerabilities by Product



Actionable Severity Diagram

Key Takeaways

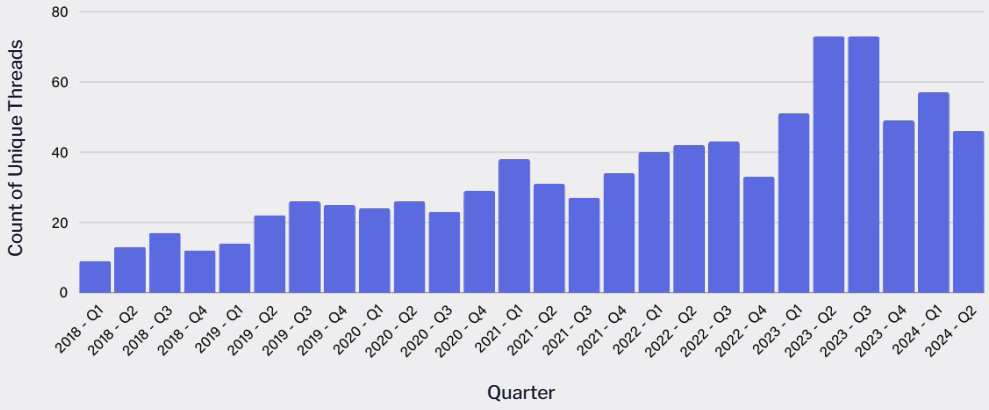
- Flashpoint aggregated and enriched 17,518 newly disclosed vulnerabilities in H1 2024. 936 of them were **missed by CVE and NVD**.
- Over 45% of all vulnerabilities disclosed in H1 2024 are rated high to critical in CVSSv3. In order to prioritize effectively, organizations will need to avoid a top-down patching approach.
- Vulnerability management teams can potentially reduce their critical vulnerability workloads up to 83% by focusing on remotely exploitable issues that have public exploits and a verifiable solution. However, given the **current NVD slowdown**, organizations will need a **quality source of vulnerability intelligence** for a comprehensive view.

Information-Stealing Malware

Flashpoint has been observing a significant rise in the use of **infostealer malware**. It is simple, effective, easy to obtain, and inexpensive for threat actors to purchase. This has propelled infostealers to become an increasingly primary vector for ransomware and other high-impact **data breaches**.

The Rise of Infostealers:

Unique Threads on Illicit Marketplaces by Quarter

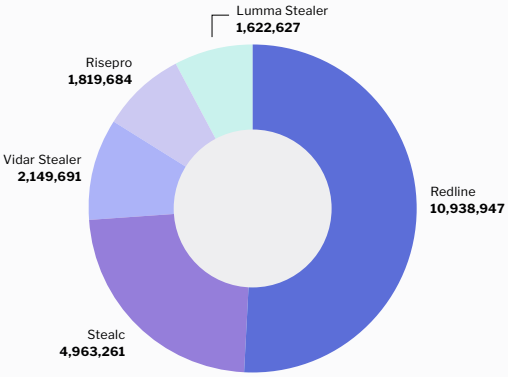


Infostealer Quickview

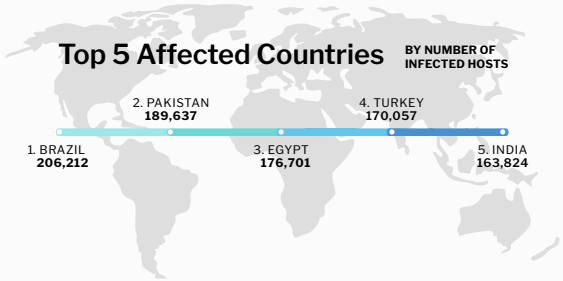
Midyear 2024

4.8 Million	13 Million	25 Million	53 Million
TOTAL INFECTED HOSTS	TOTAL INFECTED HOSTS YTD	UNIQUE STOLEN CREDENTIALS	TOTAL STOLEN CREDENTIALS

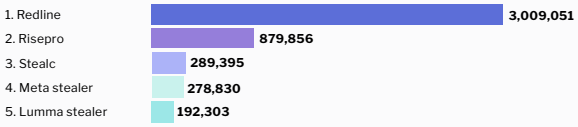
Stolen Credentials Sourced by Infostealer Family



Top 5 Affected Countries BY NUMBER OF INFECTED HOSTS



Top 5 Most Prolific Infostealers BY NUMBER OF INFECTED HOSTS



Key Takeaways

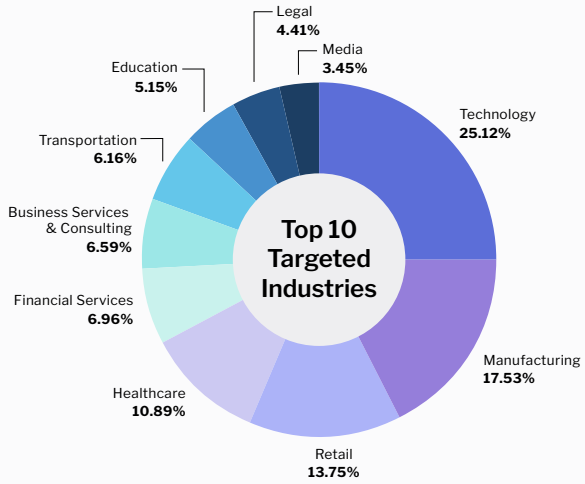
- Information-stealing malware poses one of the most significant threats in 2024. Cybercriminals have used this malware globally, infecting more than 13 million devices and compromising over 53 million credentials. This stolen data fuels increasingly complex and damaging ransomware attacks.
- Redline has been the most prolific infostealer, infecting over 3 million hosts and exfiltrating over 10 million stolen credentials.
- In total, Flashpoint has collected over 456 million stolen or leaked credentials.

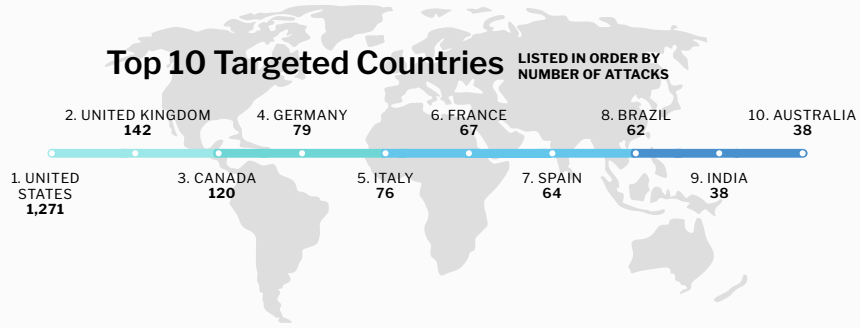
Ransomware

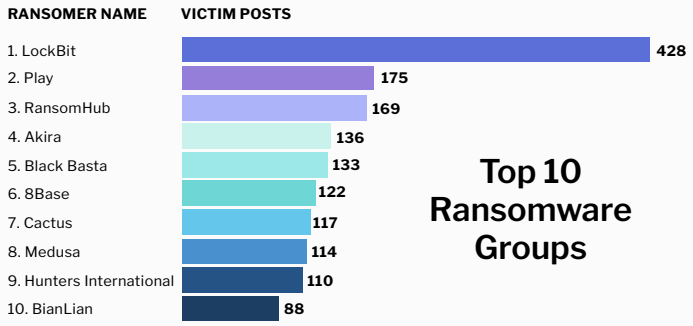
Ransomware is a vital part of any organization's risk landscape awareness. As threat actors and their tactics, tools, and procedures become more advanced, ransomware groups such as **LockBit** and **Black Basta** have become more aggressive in their endeavors.

Ransomware Quickview

Midyear 2024







Key Takeaways

- The United States remains the primary target for ransomware groups, followed by the United Kingdom and Canada. This sustained focus is driven by factors such as availability of high-profile targets, the potential for lucrative ransom payments, and overall challenges in dismantling sophisticated ransomware operations.
- The technology industry was the most targeted industry for ransomware, followed by manufacturing. Technology firms are high-value targets because they provide critical infrastructure, while manufacturing companies combine access to important supply chain components with a tendency to rely on more outdated and vulnerable systems.
- LockBit continues to be the most prolific ransomware group, claiming 428 victims in the first half of 2024.

Insider Threat

Insider threats encompass a spectrum from accidental data breaches to calculated infiltrations. Recognizing and mitigating insider threats demands a comprehensive source of threat intelligence that can monitor activity on the deep and dark web—in addition to illicit marketplaces and forums.

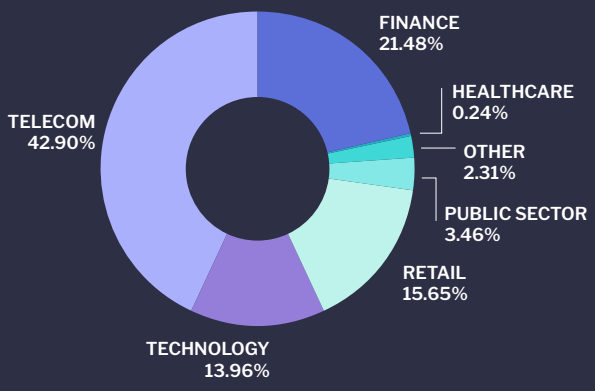
Insider Threat Quickview

Midyear 2024

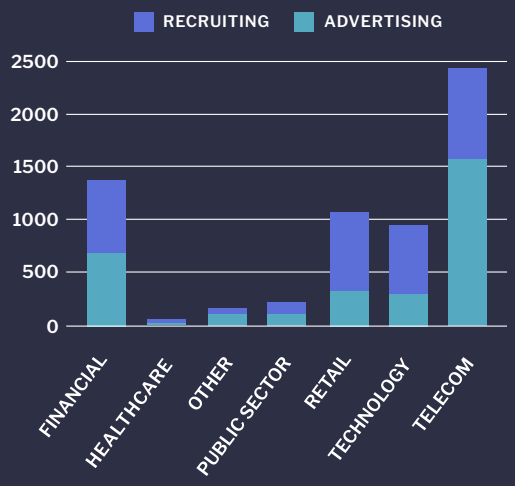
8,497 UNIQUE POSTS

43,749 TOTAL POSTS

Insider Posts by Industry



Recruiting vs. Advertising Insiders



Key Takeaways

- Flashpoint observed more than 8,497 unique instances of insider recruiting, advertising, or general discussions involving insider-related threat activity across our chat collections.
- The vast majority of insider threat activity came from individuals advertising their services to malicious actors. Most of this activity occurred in the telecom industry, where employees solicited to perform SIM swaps for threat actors.
- The finance industry is seeing an increasing number of insider threats where insiders are offering their positions or expertise—helping threat actors bypass security measures or facilitating illegal transactions.

Foresight Informs Preparedness

The data in this report, collected from January 1 to June 30, 2024, offers a snapshot of the most critical threats as organizations head into the remaining months of the year. Staying ahead of threat actors requires more than just reacting to incidents as they occur and foresight is the key to preparedness.

Foresight is only actionable through comprehensive intelligence. As such, this midyear report serves as a catalyst for organizations to proactively assess their security posture, priorities, and opportunities for enhancement. By becoming aware of the trends, tactics, and targets of today's cybercriminals, security teams can identify and address potential weaknesses in their defenses, anticipate potential threats, and empower themselves to proactively respond.

To better navigate the evolving cyber threat landscape, we encourage organizations to explore the Flashpoint 2024 Global Threat Intelligence Report for deeper insights and actionable strategies to safeguard critical assets.

Download the 2024 Global Threat Intelligence Report

About Flashpoint

Flashpoint is the leader in threat data and intelligence. We empower mission-critical businesses and governments worldwide to decisively confront complex security challenges, reduce risk, and improve operational resilience amid fast-evolving threats. Through the Flashpoint Ignite platform, we deliver unparalleled depth, breadth and speed of data from highly relevant sources, enriched by human insights. Our solutions span cyber threat intelligence, vulnerability intelligence, geopolitical risk, physical security, fraud and brand protection. The result: our customers safeguard critical assets, avoid financial loss, and protect lives.

Discover more at **flashpoint.io**

FLASHPOINT