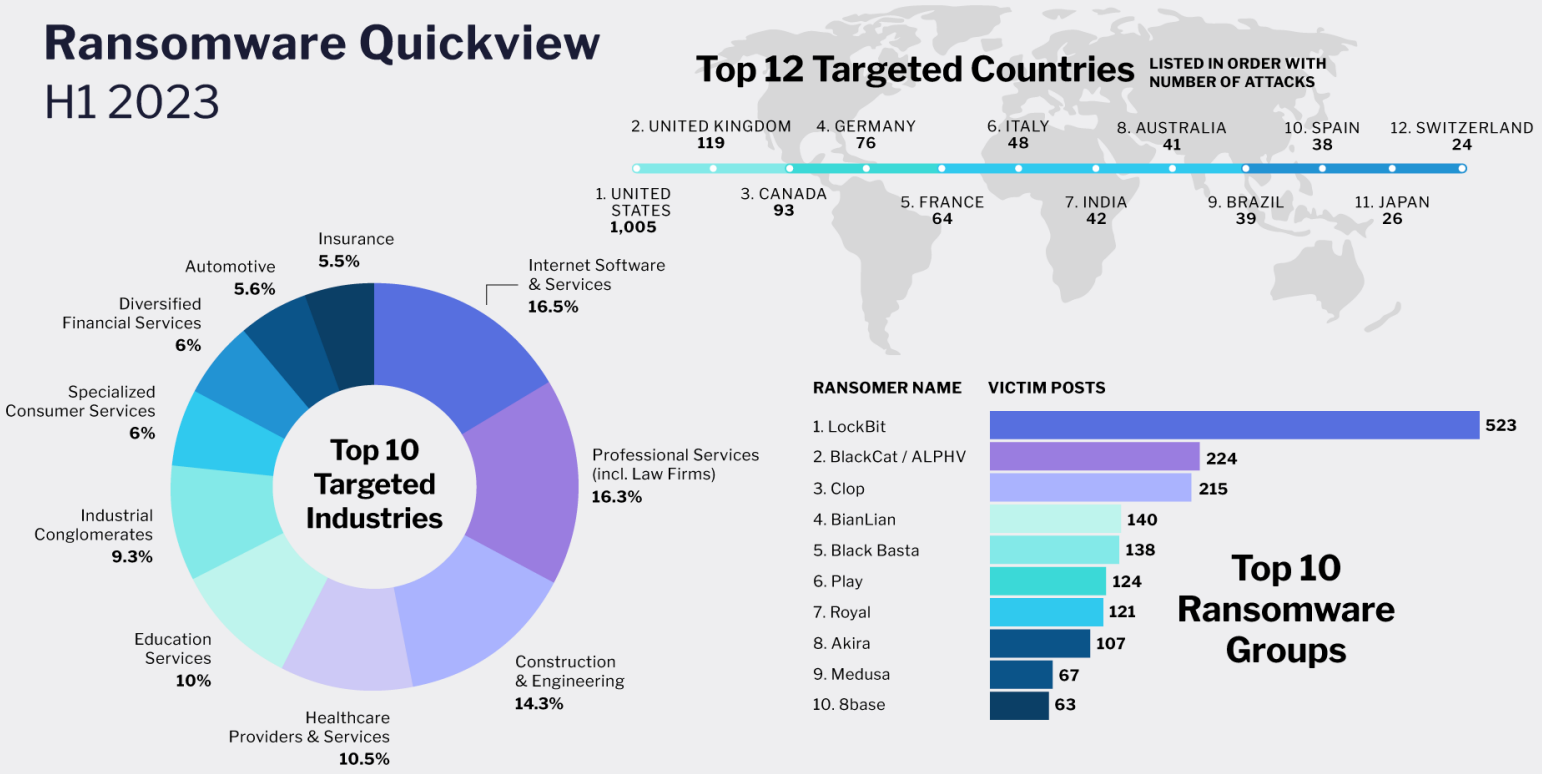
FLASHPOINT

Flashpoint's Cyber Threat Intelligence Index: 2023 Midyear Edition

Data, insights, and analysis on the most impactful events and threats of 2023 so far—from ransomware and vulnerabilities to data breaches and insider threat.



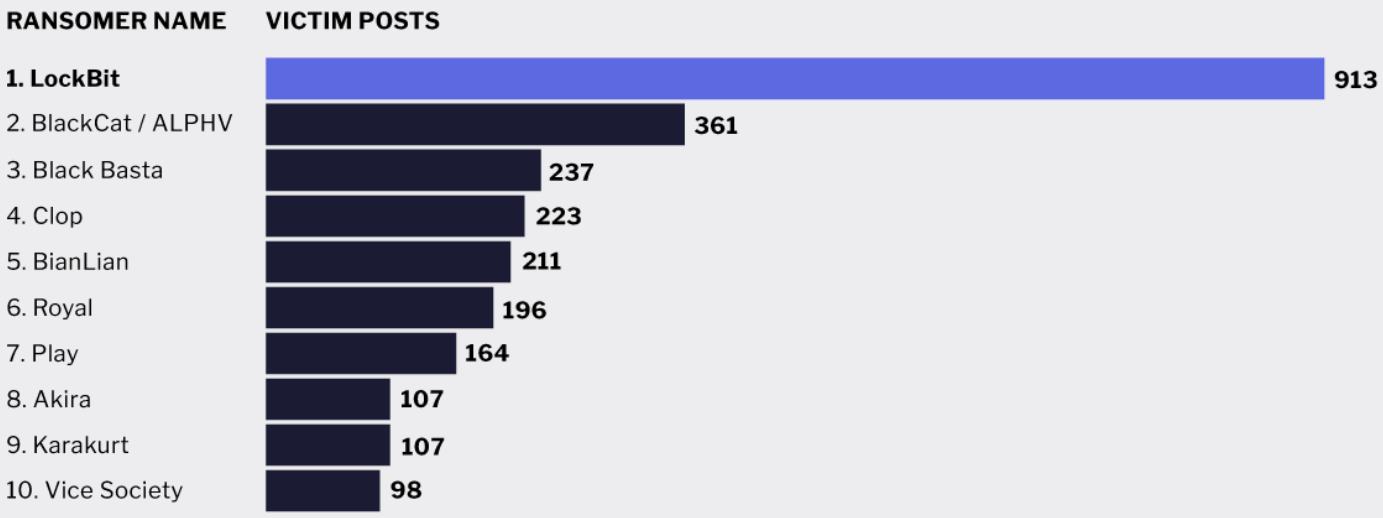
Data as of August 24, 2023.

Ransomware

Did you know?

- The most headline-grabbing cyber extortion event in the first half of 2023 was (and continues to be) the impact of the Clop ransomware group, which began exploiting the MOVEit zero-day vulnerability in May to gain illegal access to a wide range of victims.
- As of August 9, the total number of victims—those posted on Clop's ransomware blog combined with data from Flashpoint's Cyber Risk Analytics (CRA) platform—totaled more than 650. This number includes companies that were directly attacked by Clop as well as third-party victims.
- Still, Clop, at least in terms of the total claimed victims, was not as prolific as LockBit, which was responsible for about 30 percent of all ransomware attacks in H1 (out of the top 10 most active groups). The Ransomware-as-a-Service (RaaS) group was the most productive operator not only in the first half of 2023 but also the trailing year—by far.

Top 10 Ransomware Groups July 2022 - June 2023



Data as of August 24, 2023.

- Diving deeper, Flashpoint analysts found that eight of the top 10 ransomware variants are programmed in C or C++. While alternative programming languages have gained popularity in the malware community, only two variants—ALPHV (Rust) and BianLian (Go)—are composed in such languages.
- All of the top 10 ransomware families use the Advanced Encryption Standard (AES) when encrypting files.

"The Extortion Economy represents a growing risk to organizations that parallels many ransomware threats. Confronted with an escalating array of extortion tactics, many organizations are adapting strategies from ransomware response playbooks to address these lesser-known extortion techniques and building intelligence-led defenses to protect their assets."

Ian Gray, VP of Intelligence at Flashpoint

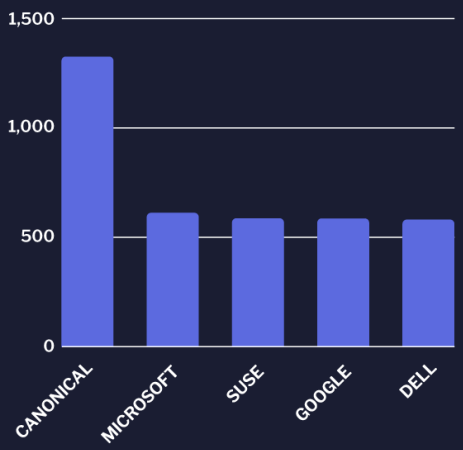
Vulnerability Quickview
H1 2023

14,201 VULNERABILITIES DISCLOSED

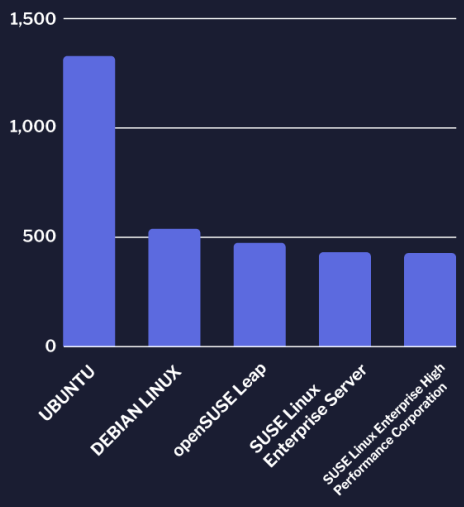
2,189 VULNERABILITIES WITHOUT CVE ID

4,878 HIGH OR CRITICAL (CVSSv2)

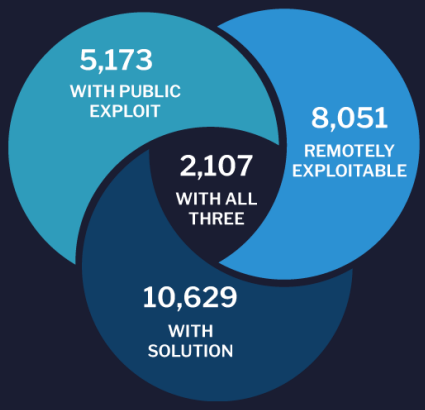
Vulnerabilities By Vendor



Vulnerabilities By Product



Actionable Severity Diagram



Data as of August 2, 2023.

Vulnerabilities

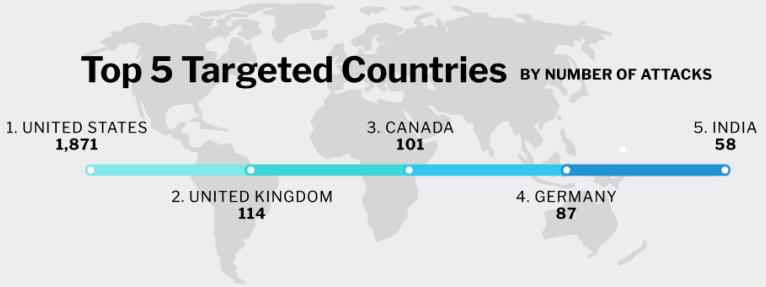
Did you know?

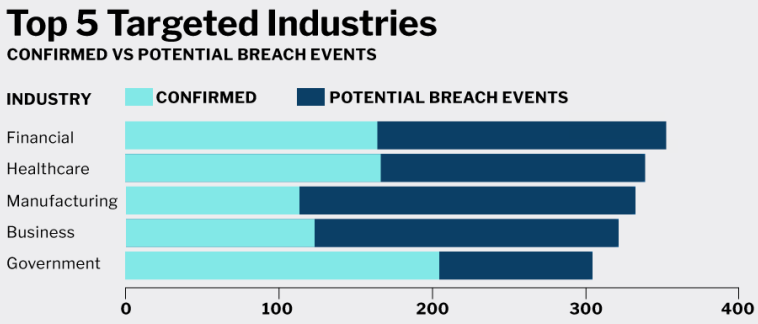
- 14,201 new vulnerabilities were reported in H1 2023, and 2,189 of them were missed by the Common Vulnerabilities and Exposures (CVE) and National Vulnerability Database (NVD).
- Over 36 percent of H1's disclosed vulnerabilities have a working proof-of-concept or a known public exploit, giving low-level attackers an opportunity to compromise vulnerable systems.
- Over 56 percent of H1's vulnerabilities are remotely exploitable, giving threat actors the ability to execute malicious code no matter where a targeted device is located.
- Threat actors sold and sought exploits across the deep and dark web, including the GoAnywhereMFT vulnerability leveraged by the Clop ransomware group. The price for an exploit, omitting free exploits, or those whose price was unknown, ranged from $600 to $30,000.
- Read our report, *Sales and Purchases of Exploits: 2023 Midyear*, to learn more about the entire scope of the market for exploits.

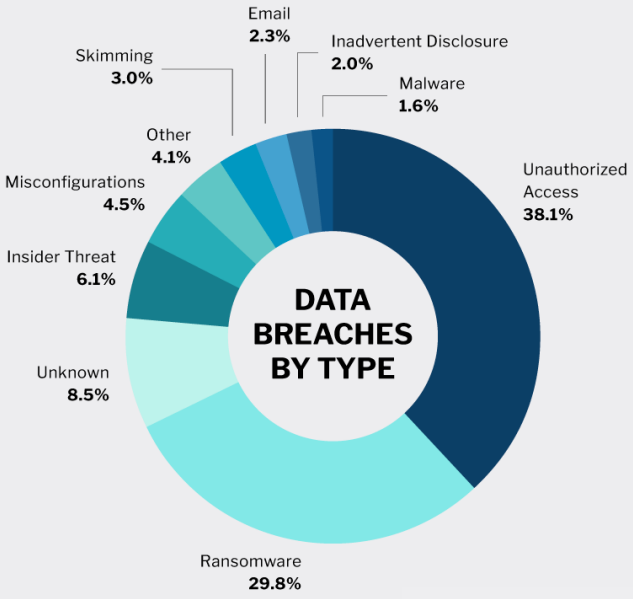
Data Breach Quickview
H1 2023

2,893
DATA BREACHES

5.94 B
STOLEN RECORDS







Data as of August 2, 2023.

Data Breaches

Did you know?

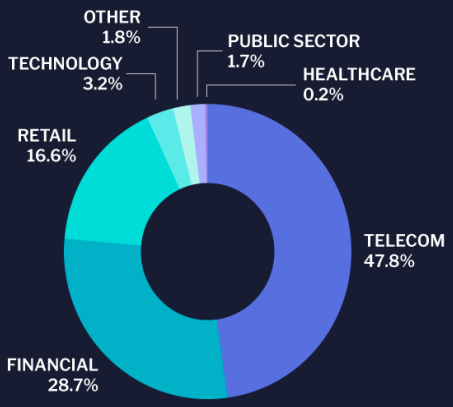
- In H1 2023, Flashpoint analysts identified 2,893 data breach events, resulting in the loss of 5.94B records.
- The highest number of breaches was recorded in the US.
- Unauthorized access, or hacking, was responsible for 38 percent of all recorded data breach events in H1 2023.
- Analysts identified that financial service providers, healthcare organizations, and businesses in the manufacturing sector experienced the largest number of breaches in H1 2023.

Insider Threat Quickview
H1 2023

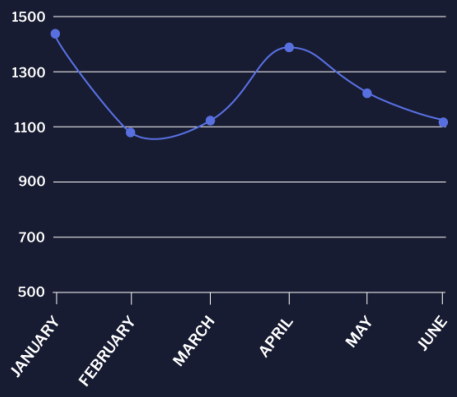
7,405
H1 UNIQUE POSTS

50,480
H1 ALL POSTS

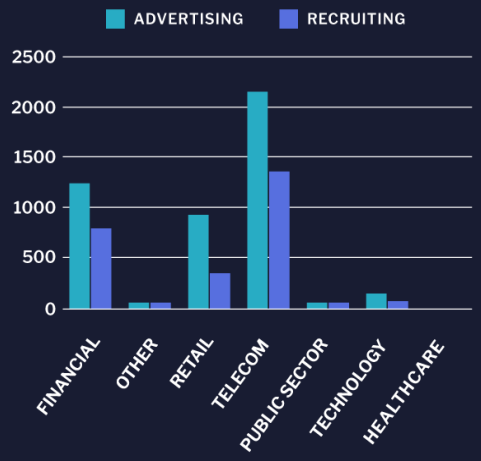
Insider Posts by Industry



Unique Insider Posts



Advertising vs. Recruiting Insiders



Data as of August 2, 2023.

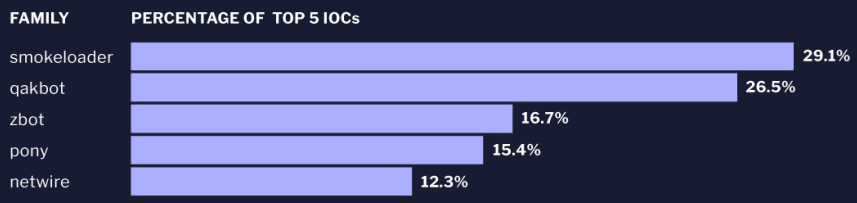
Insider Threat

Did you know?

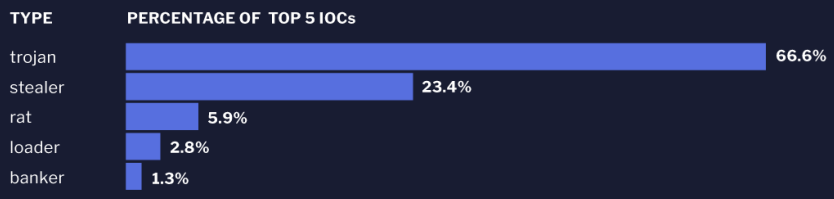
- In the first half of 2023, Flashpoint observed more than 7,400 unique instances of insider recruiting, insider advertising, or general discussions involving insider-related threat activity across our chat collections.
- A majority of these threat actors advertised or sought to recruit insiders working at mobile telecommunications providers, with a focus on conducting fraud operations.
- In fact, 93 percent of all insider threat-related activity was targeted at three sectors: mobile telecommunications providers, financial service providers (including insurers), and retailers.

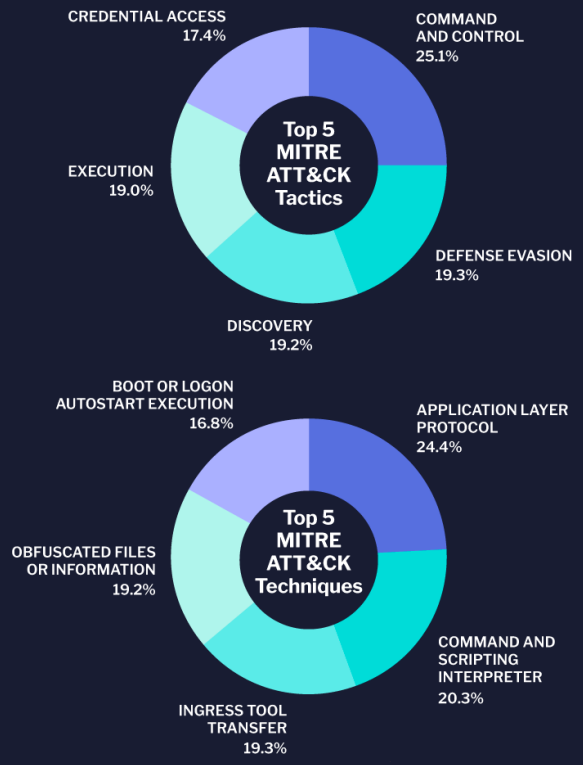
Malware IOCs Quickview
H1 2023

Top 5 Malware Families



Top 5 Malware Types





Data as of August 8, 2023.

Malware IOCs

Did you know?

- Trojan was the malware type most employed by cyber attackers.
- In particular, the smokeloader malware family accounted for about 29 percent of the top 5 indicators of compromise for H1 2023, followed by the banking trojan qakbot, or Qbot (26.5 percent).
- The smokeloader malware—a generic backdoor with a range of capabilities that depend on the modules included in any given build of the malware—frequently tries to hide its C2 activity by generating requests to reputable and legitimate sites. Typically the actual download returns an HTTP 404 but still contains data in the response body.

Data and methodology

This report uses data from Flashpoint intelligence. The infographics in each section show when the data was retrieved and analyzed. It is important to note, however, that details surrounding events like ransomware attacks and data breaches can change as new information becomes available. This report provides the best picture of each threat based on when the data was collected.

About Flashpoint

Trusted by governments, commercial enterprises, and educational institutions worldwide, Flashpoint helps organizations protect their most critical assets, infrastructure, and stakeholders from security risks such as cyber threats, ransomware, fraud, physical threats, and more. Leading security practitioners—including physical and corporate security, cyber threat intelligence (CTI), vulnerability management, and vendor risk management teams—rely on the Flashpoint Intelligence Platform, comprising open-source (OSINT) and closed intelligence, to proactively identify and mitigate risk and stay ahead of the evolving threat landscape.

Learn more at **flashpoint.io** or **sign up for a free trial** today.

FLASHPOINT