FLASHPOINT

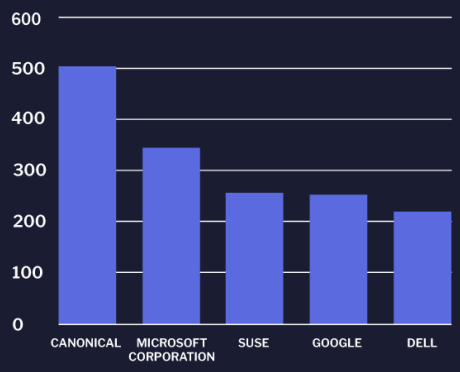
Flashpoint's Cyber Threat Intelligence Index: Q3 2023 Edition

Data, insights, and analysis on the most impactful events and threats of Q3 2023—from ransomware and vulnerabilities to data breaches and insider threat.

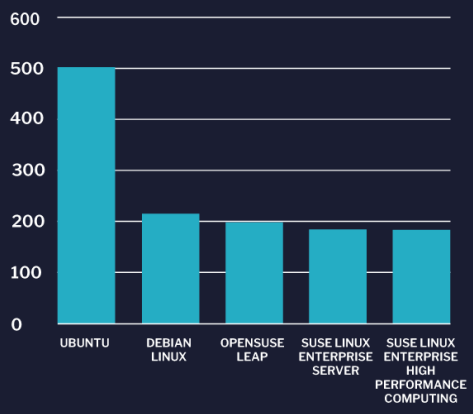
Vulnerability Quickview
Q3 2023

7,373	1,167	23,268	2,752
VULNERABILITIES DISCLOSED	VULNERABILITIES WITHOUT CVE ID	VULNERABILITIES YTD	HIGH OR CRITICAL (CVSSv2)

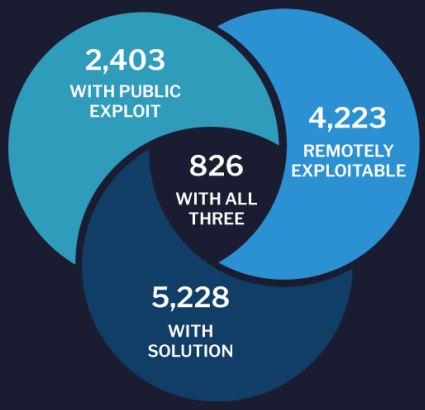
Vulnerabilities By Vendor



Vulnerabilities By Product



Actionable Severity Diagram



Vulnerabilities

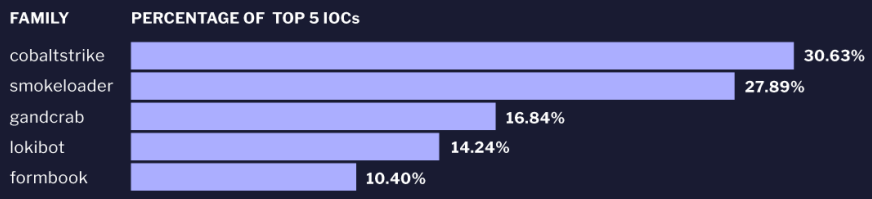
Did you know?

- 7,373 new vulnerabilities were reported in Q3 2023, and 1,167 of them were missed by the Common Vulnerabilities and Exposures (CVE) and National Vulnerability Database (NVD).
- Over 37 percent of Q3's vulnerabilities are rated high (7.0 - 10.0) according to CVSSv2. Using CVSSv3, 53 percent of Q3's vulnerabilities would be scored high to critical.
- Using a comprehensive source of vulnerability intelligence can help organizations better prioritize by up to 88 percent. This can be achieved by focusing on remotely exploitable issues that have public exploits and a verifiable solution.

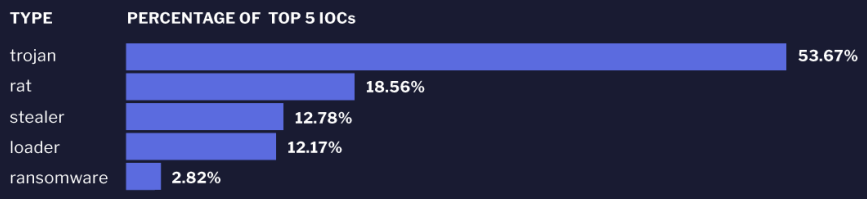
FLASHPOINT

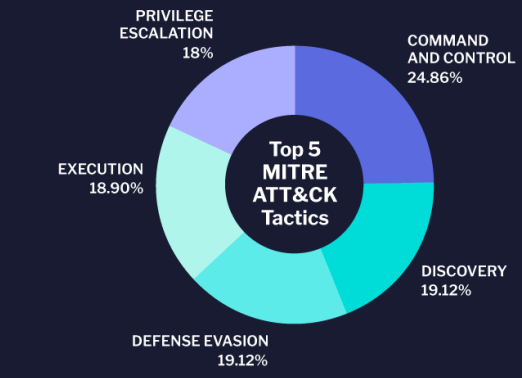
Malware IOCs Quickview
Q3 2023

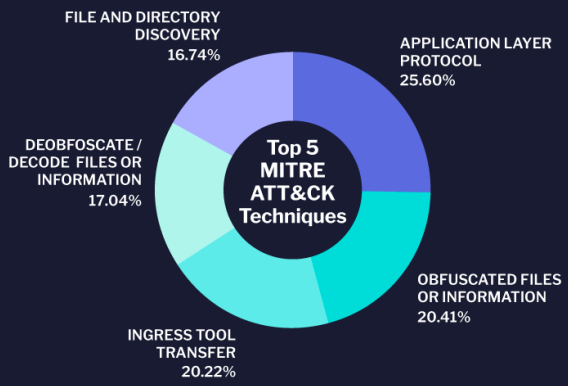
Top 5 Malware Families



Top 5 Malware Types







Malware IOCs

Did you know?

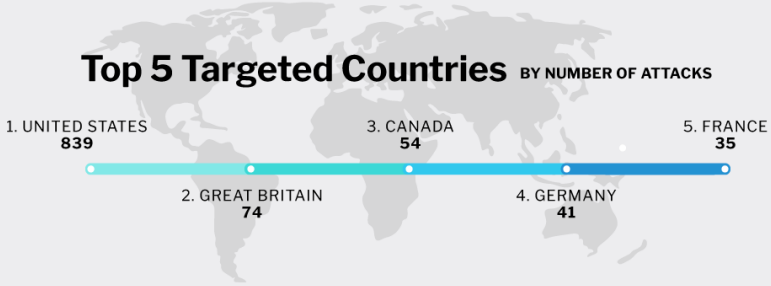
- Trojan continues to be the most used malware family leveraged by threat actors.
- In particular, CobaltStrike accounted for 30.63% of the top 5 indicators of compromise for Q3 2023, followed by SmokeLoader (27.89%).

FLASHPOINT

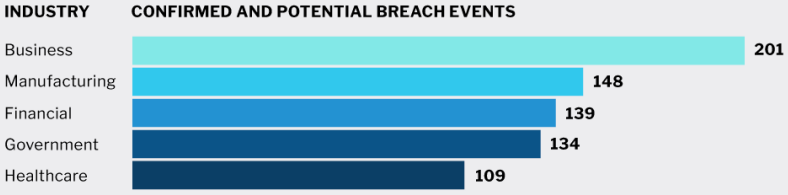
Data Breach Quickview
Q3 2023

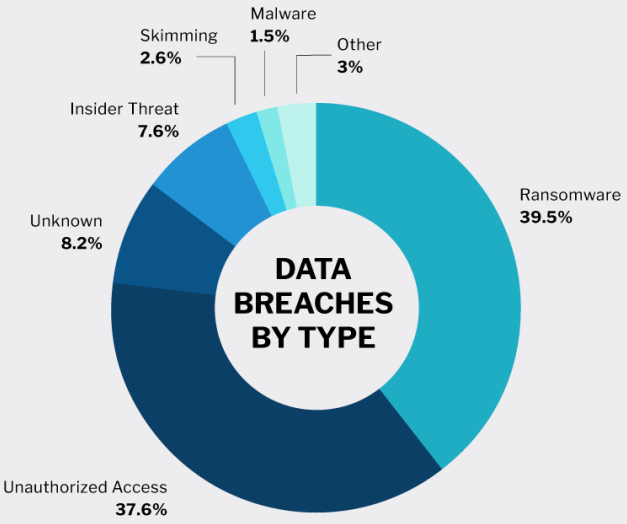
1,422	639M	4,177	6.2B
DATA BREACHES	STOLEN RECORDS	DATA BREACHES YTD	STOLEN RECORDS YTD

Top 5 Targeted Countries BY NUMBER OF ATTACKS



Top 5 Targeted Industries

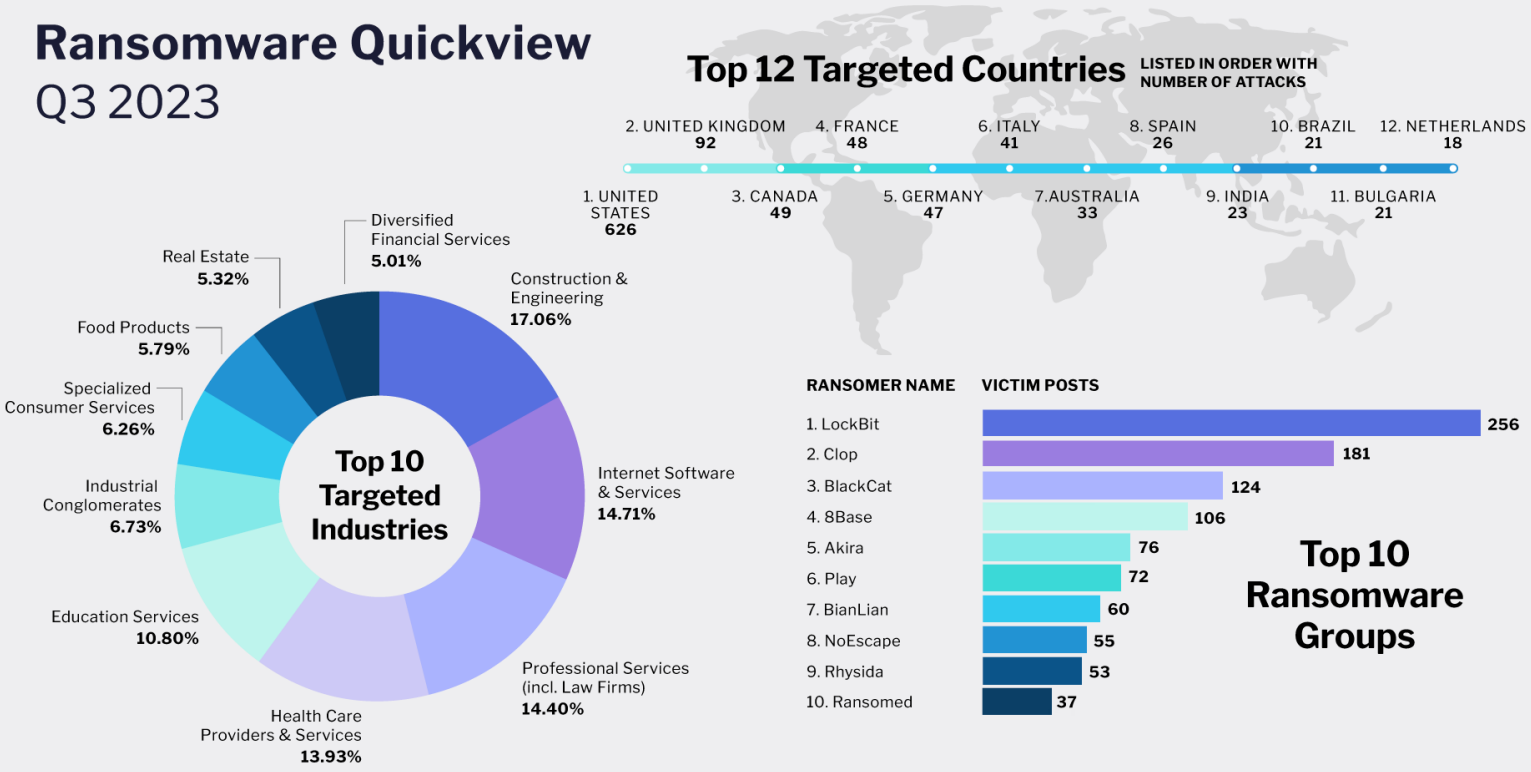




Data Breaches

Did you know?

- In Q3 2023, Flashpoint identified 1,422 data breaches that resulted in 639 million records being stolen or leaked.
- The United States continues to experience the highest number of data breaches.
- Ransomware surpasses unauthorized access (hacking) as the leading cause of data breaches in Q3. This may be a momentary trend, as hacking historically has been the number one source of breaches.



Ransomware

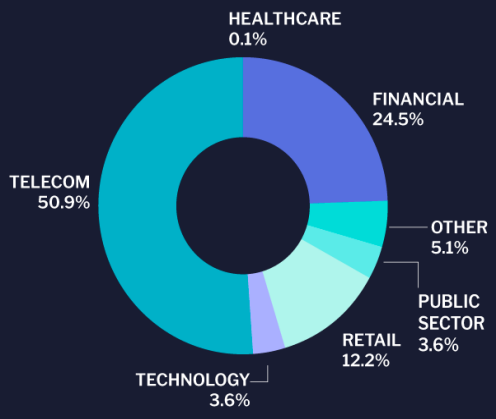
Did you know?

- The Construction and Engineering industry overtook Internet Software and Services as the most targeted industry for ransomware.
- LockBit continues to be the most prolific Ransomware-as-a-Service (RaaS) group.

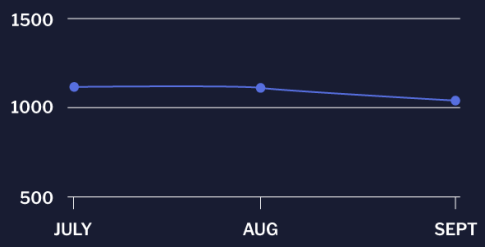
Insider Threat Quickview
Q3 2023

3,277	21,465	10,682	71,945
Q3 UNIQUE POSTS	Q3 ALL POSTS	YTD UNIQUE POSTS	YTD ALL POSTS

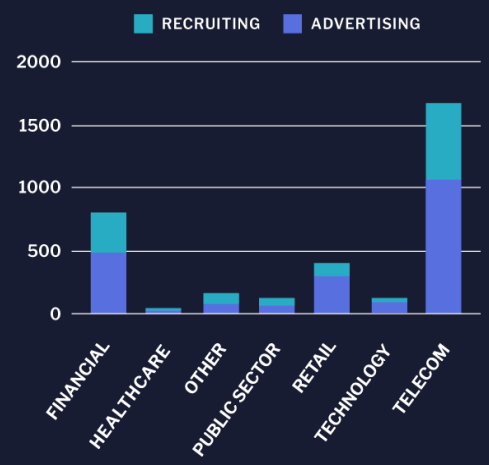
Insider Posts by Industry



Unique Insider Posts



Recruiting vs. Advertising Insiders



Insider Threat

Did you know?

- In Q3 2023, Flashpoint observed more than 3,277 unique instances of insider recruiting, insider advertising, or general discussions involving insider-related threat activity across our chat collections.
- The majority of insider threat activity came from individuals advertising their services to malicious actors. Most of this activity is attributed to the Telecom industry.

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