KELA

2025

Midyear Cyber Threat Snapshot

H1 Recap on Ransomware, Infostealers & Exploited Vulnerabilities

The Big Picture in H1

3,662 ransomware victims
54% increase YoY.

2.67M+ machines infected by infostealers
204M+ credentials stolen

1.3B credentials shared from infostealer logs

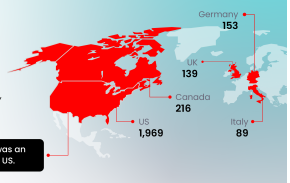
Attackers discuss new CVEs within **1-2 days**

Ransomware & Extortion

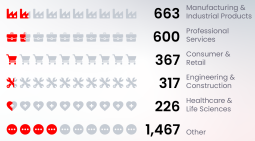
The Victims

BY REGION
The US accounted for the majority of ransomware victims, representing more than 50% of the total number of victims.

Compared to H1 2024, there was an increase of almost 63% in the US.

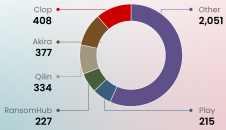


BY SECTOR
Manufacturing & Industrial Products and Professional Services are the most affected sectors this year. This is consistent with H1 2024.



The Actors

Clop leads with 408 victim claims (+2300% YoY) via supply-chain exploits



Infostealers: The Silent Entry Point

Scale

2.67M infected devices

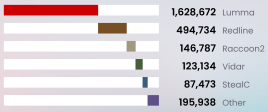
204M+ credentials

The Victims

The countries that experienced the highest rates of infostealer infections include: India, Brazil, Indonesia, United States, and Vietnam.

Top families

Lumma, Redline, Raccoon2 = ~85% of infections.



New Tricks

The "Macs are safe" myth is busted with the Atomic macOS Stealer (AMOS).

Vulnerabilities: Exploitation at Record Speed

Top exploited CVEs:
Ivanti (CVE-2025-0282),
Palo Alto (CVE-2025-0108),
Microsoft File Explorer (CVE-2025-24071)

4 of top 5 most discussed CVEs on cybercrime forums were already exploited in the wild

Attackers discuss **new CVEs within 1-2 days;** some same-day.

The Road Forward

To learn how organizations can mitigate these growing risks, read the Midyear Report or reach out to KELA to learn more.

KELA