ZEROFOX

Deep and Dark Web Intelligence Reporting

Here is a curated list of critical incidents and compromised data observed on deep and dark web ransomware sites, forums, and marketplaces ingested into the ZeroFox Platform in the past 24 hours.

July 23, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

5 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
DragonForce Ransomware	Koshkaryan Law Group
Nova Ransomware	La Financière d'Orion
Everest Ransomware	Rx Networks
Everest Ransomware	Al-Futtaim
CoinbaseCartel Ransomware	Colliers

VULNERABILITY DISCLOSURES

2 disclosures

CVE-2026-8933

Local Privilege Escalation Vulnerability in Canonical snapd (snap-confine)

CVE-2026-48294

Universal Cross-Site Scripting (UXSS) Vulnerability in Adobe Acrobat PDF Extension for Chrome

DEEP AND DARK WEB INTELLIGENCE

4 findings

CRITICAL FINDINGS

CRITICAL

Alleged Multi-Platform Data Exposure Likely Aggregated from Historical Breaches and Infostealer Logs

ZeroFox observed multiple well-known organizations listed across deep and dark web (DDW) forums, with threat actors claiming to have breached databases containing millions of user records.

Source: DarkForums

CRITICAL

Flight Record Data Allegedly Tied to El Al and Turkish Airlines Advertised

On July 23, 2026, untested threat actor "jamboman" advertised data allegedly associated with El Al Israel Airlines and Turkish Airlines on the predominantly Russian-language DDW forum Exploit.

Source: Exploit **Actor:** jamboman

CRITICAL

Shipping Labels Allegedly Associated with UPS and FedEx Advertised

On July 23, 2026, untested threat actor "Dolus1" advertised shipping labels allegedly associated with UPS and FedEx on Exploit.

Source: Exploit **Actor:** Dolus1

VULNERABILITY EXPLOITATION

MEDIUM

Alleged Zero-Day Windows LPE and Linux RCE Advertised for Sale

On July 22, 2026, untested threat actor "Mikeclover" advertised alleged Windows Local Privilege Escalation (LPE) and Linux Remote Code Execution (RCE) zero-day exploits on Exploit and XSS.

Source: Exploit/XSS **Actor:** Mikeclover

COLLECTED, PROCESSED DATA BREACHES

4 entries

VICTIM	SOURCE	THREAT ACTOR	PROCESSED RECORDS
bienici[.]com	PwnForums	0xSec	3.45K
shreetransport[.]co	PwnForums	Sensitive2025	519
virtualconvocation.amizone[.]net	PwnForums	Sensitive2025	16.94K
navoy[.]io	PwnForums	NightBroker	749

PROCESSED DATA SET STATISTICS

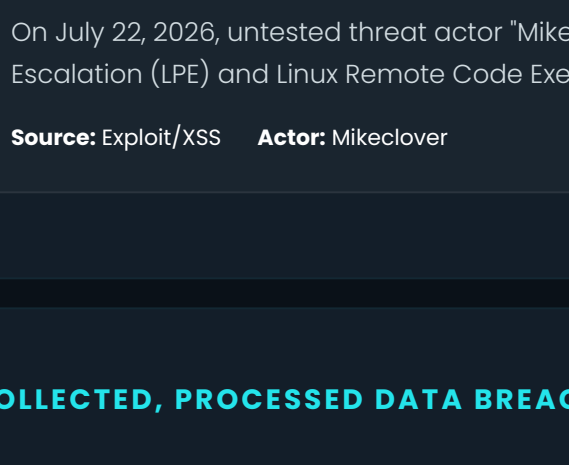
Past 4 Weeks

193.49M CAC RECORDS

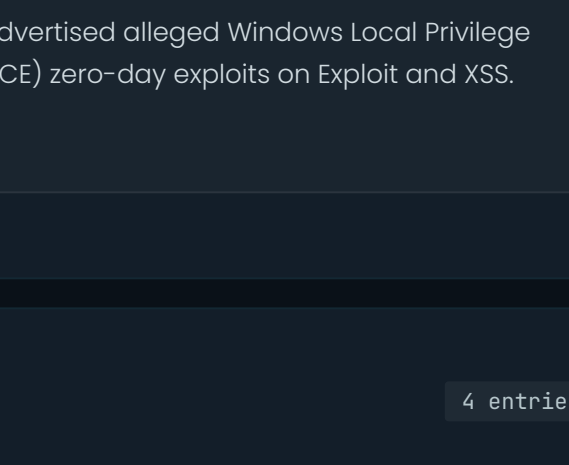
1.13B BOTNET CAC RECORDS

763 RANSOMWARE & DIGITAL EXTORTION

PROCESSED DATA BREACH RECORDS



INFOSTEALER COMPROMISED DATA



Previously Published Threat Actor Profiles

A threat actor profile provides a comprehensive overview of a malicious actor's identity, motivations, targeted sectors, and operational tactics, techniques, and procedures (TTPs).

Previously Published Monthly Threat Spotlight

The Monthly Threat Spotlight highlights unusual threat actor behaviors and TTPs, as well as significant operational spikes that deviate from the baseline threat landscape.