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 29, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

8 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
CoinbaseCartel	accesso
Everest	Stadler Rail
SafePay	Der Paritätische NRW
NightSpire	TFG Benefits
ExfilSquad	City of Atlanta
ExfilSquad	Frontier Airlines
ExfilSquad	Allstate
ExfilSquad	Microsoft

VULNERABILITY DISCLOSURES

2 disclosures

CVE-2026-61511
Unauthenticated Remote Code Execution Vulnerability in vBulletin

CVE-2026-16812
OS Command Injection Vulnerability in Arista VeloCloud Orchestrator On-Prem

DEEP AND DARK WEB INTELLIGENCE

6 findings

CRITICAL FINDINGS

CRITICAL **Data Allegedly Associated with Shopee Customers Advertised**

On July 28, 2026, untested threat actor "666op" advertised to sell data allegedly associated with Shopee on the predominantly English-language deep and dark web forum DarkForums.

Source: DarkForums **Actor:** 666op

CRITICAL **Alleged Lenovo Corporate Credentials Advertised**

On July 28, 2026, an untested threat actor "cha3bauf" advertised to sell a collection of email and password combinations associated with multiple Lenovo services and internal portals, on the predominantly Russian-language deep and dark web forum Exploit.

Source: Exploit **Actor:** cha3bauf

CRITICAL **Data Allegedly Associated with Euroins Advertised**

On July 28, 2026, credible threat actor "Jurak" advertised the sale of a database allegedly associated with Euroins on the predominantly English-language deep and dark web forum PwnForums.

Source: PwnForums **Actor:** Jurak

UNAUTHORIZED ACCESS CLAIMS

CRITICAL **SSH Access Allegedly Tied to U.S.-Based Healthcare Insurance Company Advertised**

On July 28, 2026, an untested threat actor "khosi" advertised to sell SSH access allegedly associated with an unnamed U.S.-based healthcare insurance company on the predominantly English-language deep and dark web forum PwnForums.

Source: PwnForums **Actor:** khosi

HIGH **Network Access Allegedly Tied to UAE-Based Retail Company Advertised**

On July 28, 2026, a moderately credible threat actor "personX" advertised to sell network access with local administrator rights allegedly associated with an unnamed UAE-based retail company on the predominantly Russian-language deep and dark web forum Exploit.

Source: Exploit **Actor:** personX

CRITICAL **RDP Access Allegedly Tied to UAE-Based Aerospace and Defense Company Advertised**

On July 28, 2026, a well-regarded threat actor "sudo" advertised to sell RDP access allegedly associated with an unnamed UAE-based aerospace and defense company on the predominantly Russian-language deep and dark web forum Exploit.

Source: Exploit **Actor:** sudo

COLLECTED, PROCESSED DATA BREACHES

4 entries

VICTIM	SOURCE	THREAT ACTOR	PROCESSED RECORDS
Arbeiterwohlfahrt Berlin Kreisverband Südost (awo-südost[.]de)	PwnForums	henrymartin	1.98K
MagMutual	PwnForums	henrymartin	242.25K
Open English (openenglish[.]com)	DarkForums	galacticcatalyst	387.11K
Defensores de la Patria (defensoresdelapatria[.]com)	PwnForums	Tig3r	897.32K

PROCESSED DATA SET STATISTICS

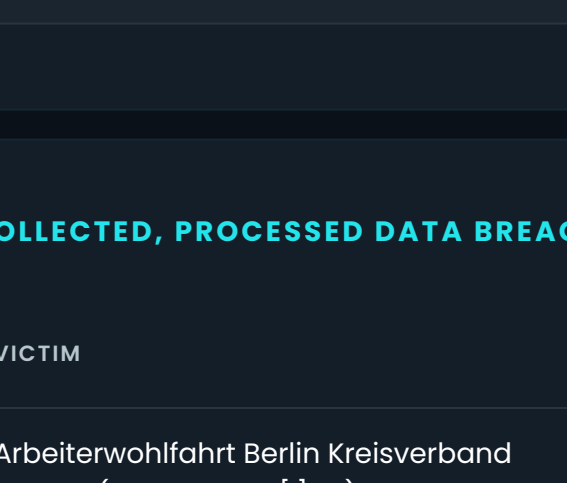
Past 4 Weeks

272.08M CAC RECORDS

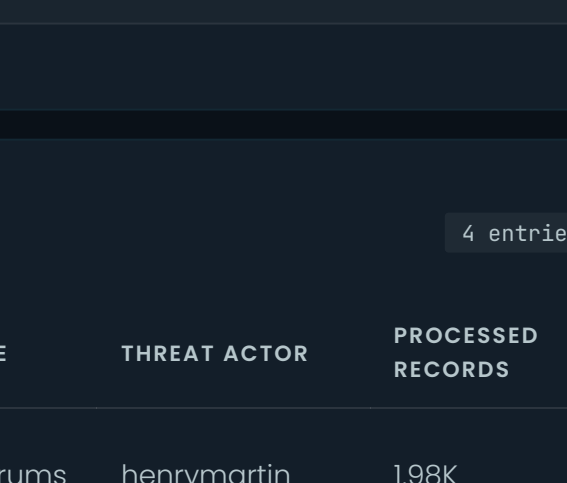
1.05B BOTNET CAC RECORDS

801 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.