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 30, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

6 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
Akira Ransomware	Northwood Country Club
Leaknet	NYC Health + Hospitals
CRPx0 Ransomware	Summit Hill Insurance
ExfilSquad	City of Houston
ExfilSquad	Zenith Bank
Booba Project Ransomware	Incredible Technologies

VULNERABILITY DISCLOSURES

4 disclosures

CVE-2026-59309
Authentication Bypass Vulnerability in VMware vCenter Server

CVE-2026-66066
Arbitrary File Read and Remote Code Execution in Ruby on Rails Active Storage

CVE-2026-59726
Missing Authentication Vulnerability for Critical Function in Ruflo MCP Bridge

CVE-2026-20316
Use of Hard-coded Password in Cisco Secure Firewall Management Center

DEEP AND DARK WEB INTELLIGENCE

5 findings

CRITICAL FINDINGS

CRITICAL **Data Allegedly Associated with CUF Advertised**

On July 30, 2026, untested threat actor "Databroker1" advertised a data set allegedly associated with CUF, a Portugal-based healthcare organization, on the predominantly English-language deep and dark web (DDW) forum DarkForums.

Source: DarkForums **Actor:** Databroker1

UNAUTHORIZED ACCESS CLAIMS

HIGH **Citrix Access Allegedly Tied to Undisclosed U.S.-Based Company Advertised**

On July 28, 2026, untested threat actor "Focus" advertised Citrix access with domain user rights allegedly associated with an undisclosed U.S.-based company on the predominantly Russian-language deep web forum DUTY-FREE.

Source: DUTY-FREE **Actor:** Focus

DATA BREACHES & LEAKS

CRITICAL **Data Allegedly Associated with MiCasino Advertised**

On July 28, 2026, well-regarded threat actor "betway" advertised a data set allegedly associated with MiCasino, a Spain-based gambling company, on the predominantly Russian-language DDW forum Exploit.

Source: Exploit **Actor:** betway

CRITICAL **Data Allegedly Associated with France-Based Individuals Advertised**

On July 29, 2026, untested threat actor "Goldstones" advertised a data set allegedly associated with France-based individuals on Exploit.

Source: Exploit **Actor:** Goldstones

CRITICAL **Data Allegedly Associated with U.S.-Based Patients Advertised**

On July 29, 2026, moderately credible threat actor "Galaher" advertised a data set allegedly associated with an unnamed U.S.-based healthcare company on the predominantly Russian-language DDW forum XSS.

Source: XSS **Actor:** Galaher

COLLECTED, PROCESSED DATA BREACHES

8 entries

VICTIM	SOURCE	THREAT ACTOR	PROCESSED RECORDS
Fonds de Dotation pour l'Enfance (fonds-dotation-enfance[.]com)	PwnForums	Angel_Batista	21.18K
X-Copper (xcopper[.]com)	PwnForums	henrymartin	218.66K
Pixartprinting (pixartprinting[.]com)	PwnForums	ChimeraZ	141.42K
Ente Nazionale per l'Aviazione Civile (ENAC) (certificazioniavsec-enac[.]it)	PwnForums	NightBroker	2.24K
ESGI (esgi[.]fr)	PwnForums	84City	15.09K
justclean (justclean[.]com)	BreachForums	Tanaka	33.61K
Milwaukee Tool Hong Kong (milwaukeetool[.]com[.]hk)	PwnForums	chinabase	769
PayLow Pro (paylowpro[.]com)	PwnForums	Joker998	355.61K

PROCESSED DATA SET STATISTICS

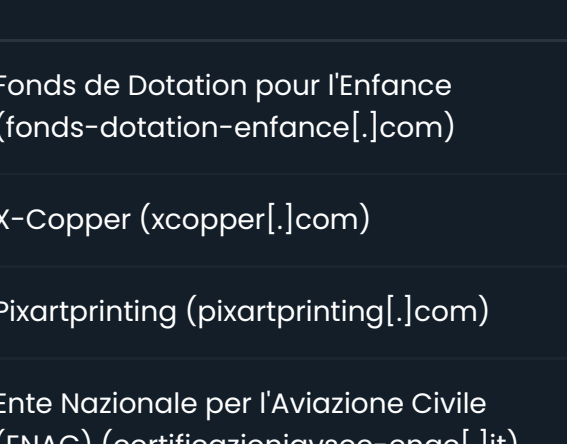
Past 4 Weeks

281.62M CAC RECORDS

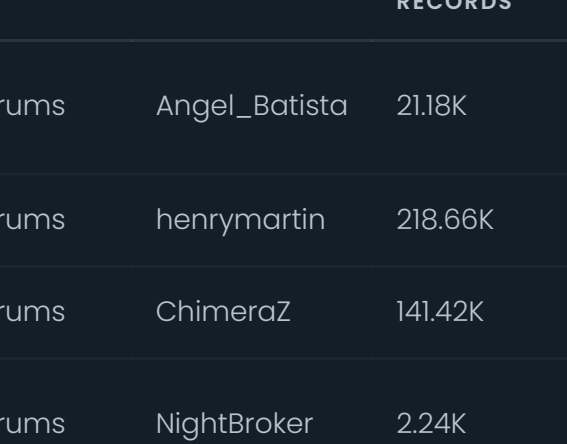
1.09B BOTNET CAC RECORDS

830 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.