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.

September 1, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

7 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
The Gentlemen Ransomware	Glassdoor
Wallstreet Ransomware	WMDN
Wallstreet	Black Hills Bentonite
Dire Wolf Ransomware	Erdem Hospital
LockBit 5.0 Ransomware	American Plan Administrators
INC Ransomware	New Century Ophthalmology
Brain Cipher Ransomware	Comprehensive Care Services

DEEP AND DARK WEB INTELLIGENCE

8 findings

CRITICAL FINDINGS

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

On August 30, 2026, untested threat actor "renn" advertised data allegedly associated with Sugarwish, a U.S.-based gifting service company on the predominantly Russian-language DDW forum Exploit.

Source: Exploit **Actor:** renn

CRITICAL **Alleged Web-App, Windows LPE, macOS LPE, and RCE Zero-Day Exploits Advertised**

On August 31, 2026, untested threat actor "Palatan" advertised various alleged zero-day exploits on Exploit.

Source: Exploit **Actor:** Palatan

DATA BREACHES & LEAKS

CRITICAL **Database Allegedly Associated with flydubai Advertised**

On August 31, 2026, untested threat actor "SilentHex" advertised a database allegedly associated with flydubai, UAE-based airline, on Exploit.

Source: Exploit **Actor:** SilentHex

HIGH **Data Allegedly Associated with Canada-Based Technology Company Advertised**

On August 31, 2026, untested threat actor "512bit" advertised data allegedly associated with an unnamed Canada-based technology company on Exploit.

Source: Exploit **Actor:** 512bit

HIGH **Database Allegedly Associated with Undisclosed Fintech Banking Platform Advertised**

On September 1, 2026, untested threat actor "brokering" advertised a database allegedly associated with an undisclosed fintech banking platform, serving startups and commercial businesses, on Exploit.

Source: Exploit **Actor:** brokering

UNAUTHORIZED ACCESS CLAIMS

HIGH **Unauthorized Webmail Access Allegedly Associated with the Italian Police Advertised**

On August 31, 2026, untested threat actor "franceOr" advertised unauthorized webmail access allegedly associated with Polizia di Stato, the Italian State Police, on the predominantly English-language DDW PwnForums.

Source: PwnForums **Actor:** franceOr

HIGH **VPN Access Allegedly Tied to Iran-Based Pharmaceutical Company Advertised**

On August 31, 2026, moderately credible threat actor "personX" advertised VPN access with local administrator rights allegedly associated with an unnamed Iran-based pharmaceutical company on Exploit.

Source: Exploit **Actor:** personX

HIGH **VPN Access Allegedly Tied to U.S.-Based Production Company Advertised**

On August 30, 2026, moderately credible threat actor "Ellnoir" advertised an auction for VPN access with domain user rights allegedly associated with an unnamed U.S.-based production company on Exploit.

Source: Exploit **Actor:** Ellnoir

COLLECTED, PROCESSED DATA BREACHES

7 entries

VICTIM	SOURCE	THREAT ACTOR	PROCESSED RECORDS
resamania[.]fr	PwnForums	84City	2.91M
lojanegociosdigital[.]com[.]br	PwnForums	Sensitive2025	7.03K
silvi[.]ai	PwnForums	NightBroker	15.43K
wydawnictwowam[.]pl	PwnForums	888	71.2K
supremebody[.]fr	DarkForums	Sophia01	775
ling-app[.]com	PwnForums	GoreTurbine	2.38M
innersense[.]co[.]in	PwnForums	0xSec	9.14K

PROCESSED DATA SET STATISTICS

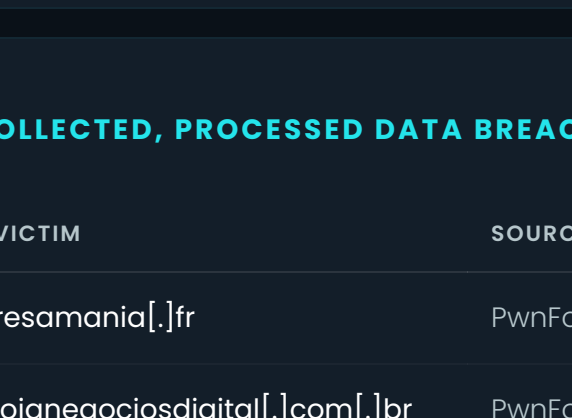
Past 4 Weeks

1.19B CAC RECORDS

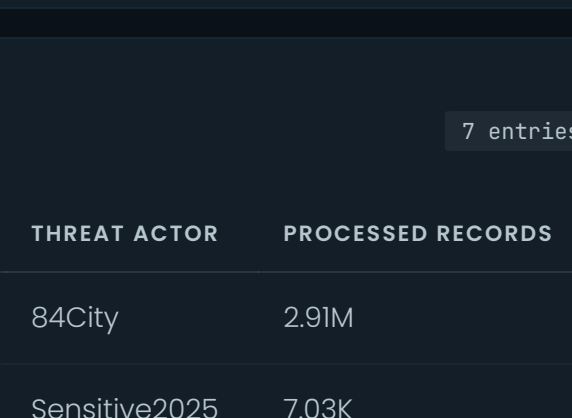
1.05B BOTNET CAC RECORDS

1.01K 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.