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 4, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

5 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
Storm Ransomware	Petrocare
Storm Ransomware	Star Aviation
Vexy Ransomware	McDonald's
SETTRA Ransomware	NeoLife International
SETTRA Ransomware	MedEvolve

VULNERABILITY DISCLOSURES

5 disclosures

CVE-2026-83548
SSRF Vulnerability in SonicWall SMA1000 Appliance WorkPlace

CVE-2026-83549
OS Command Injection Vulnerability in SonicWall SMA1000 Appliance Management Console

CVE-2026-59822
Improper Authentication Vulnerability in BerriAI LiteLLM

CVE-2026-49869
Authentication Bypass Leading to Remote Code Execution Vulnerability in Kestra OSS

CVE-2026-32475
Unrestricted File Upload Vulnerability in Elementor Elementor Pro

DEEP AND DARK WEB INTELLIGENCE

8 findings

CRITICAL FINDINGS

CRITICAL **Gorz Rostam Claims Responsibility for Disruptions to ChatGPT and Claude AI**

On September 3, 2026, a pro-Iran threat actor group "Gorz Rostam" published a post in their Telegram channel claiming responsibility for disruptions to artificial intelligence platforms, specifically naming ChatGPT and Claude AI, as part of what they describe as "Operation Haft Khan Wave Two."

Source: Telegram

CRITICAL **Alleged Microsoft Office Remote Command Injection Zero-Day Advertised**

On September 3, 2026, untested threat actor "drlogin" advertised alleged zero-day remote command injection vulnerability affecting multiple Microsoft Office products on the predominantly Russian-language DDW forum Exploit.

Source: Exploit **Actor:** drlogin

CRITICAL **Data Allegedly Associated with Laboratorio Reig Jofré Advertised**

On September 1, 2026, untested threat actor "sta6" advertised data allegedly associated with Laboratorio Reig Jofre on the predominantly English-language DDW forum PwnForums.

Source: PwnForums **Actor:** sta6

HIGH **Data Allegedly Associated with Unnamed Spain-Based Insurtech Platform Advertised**

On September 3, 2026, untested threat actor "SantaServices" advertised data allegedly exfiltrated from an unnamed Spain-based Insurtech platform on the predominantly Russian-language DDW forum XSS.

Source: XSS **Actor:** SantaServices

HIGH **Alleged Windows Server 2025 LPE Zero-Day Advertised**

On September 3, 2026, untested threat actor "Apollinaris" advertised an alleged zero-day privilege escalation (LPE) exploit for Windows Server 2025 on Exploit.

Source: Exploit **Actor:** Apollinaris

UNAUTHORIZED ACCESS CLAIMS

HIGH **Network Access Allegedly Tied to Three American Education Entities Advertised**

On September 2, 2026, untested threat actor "bianlianbo" advertised network access allegedly associated with Edge devices of three unnamed American (likely U.S.-based) education entities on PwnForums.

Source: PwnForums **Actor:** bianlianbo

HIGH **Access Allegedly Tied to Over 7,500 Internet Providers Advertised**

On September 3, 2026, untested threat actor "origin" advertised administrator credentials and database access allegedly associated with over 7,500 internet service providers (ISPs) on the predominantly English-language DDW forum DarkForums.

Source: DarkForums **Actor:** origin

VULNERABILITY EXPLOITATION

MEDIUM **Alleged SQL Injection Vulnerability Affecting IsiGéo Advertised**

On September 2, 2026, untested threat actor "HollowCrimeCorp" advertised an alleged zero-day SQL injection vulnerability affecting IsiGéo on the predominantly English-language DDW forum BreachForums (breached[.]st).

Source: BreachForums **Actor:** HollowCrimeCorp

COLLECTED, PROCESSED DATA BREACHES

2 entries

VICTIM	SOURCE	THREAT ACTOR	PROCESSED RECORDS
voxaly[.]fr	PwnForums	Sophia	5.35K
agenda[.]be	PwnForums	misere	1.52K

PROCESSED DATA SET STATISTICS

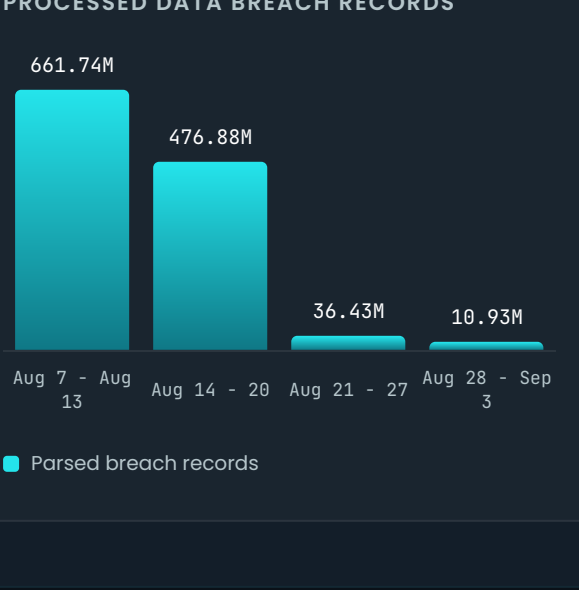
Past 4 Weeks

1.19B CAC RECORDS

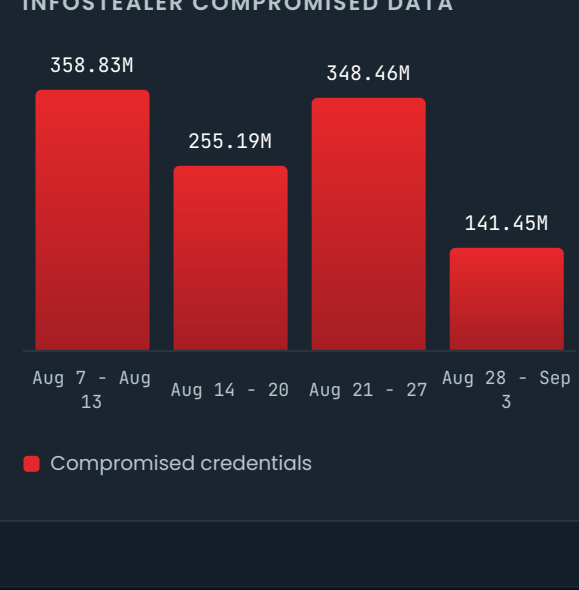
1.1B BOTNET CAC RECORDS

1.06K 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.