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.

August 14, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

5 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
Storm Ransomware	Rood & Riddle Equine Hospital
Clop Ransomware	ALDO Group
Clop Ransomware	Fiserv
Clop Ransomware	GE Aerospace
Clop Ransomware	Philips

VULNERABILITY DISCLOSURES

3 disclosures

CVE-2026-62832
Elevation of Privilege Vulnerability in Microsoft Windows User Profile Service

CVE-2026-71398
Incorrect Authorization Vulnerability in Adobe Campaign Classic

CVE-2026-48362
OS Command Injection Vulnerability in Adobe ColdFusion

DEEP AND DARK WEB INTELLIGENCE

9 findings

CRITICAL FINDINGS

CRITICAL **Actor Claims DDoS Attack Targeting Github**

On August 12, 2026, a pro-Palestinian threat actor group "313 Team" claimed to have conducted DDoS attack targeting unspecified "vulnerable endpoints" within GitHub's infrastructure.

Source: Telegram **Actor:** 313 Team

CRITICAL **Alleged Ledger Wallet Zero-Day Exploit Advertised**

On August 14, 2026, untested threat actor "aura" advertised an alleged zero-day exploit targeting the Ledger Wallet desktop application (formerly known as Ledger Live) on Exploit.

Source: Exploit **Actor:** aura

HIGH **Data Allegedly Associated with Direction générale des Finances publiques Advertised**

On August 12, 2026, moderately credible threat actor "ZeroBytes" advertised a database allegedly associated with Direction générale des Finances publiques on the predominantly English-language DDW forum PwnForums.

Source: PwnForums **Actor:** ZeroBytes

HIGH **16 New Victims Listed**

On August 14, 2026, ZeroFox observed that The Gentlemen ransomware group listed 16 new victims on their leak site.

Source: The Gentlemen Ransomware

UNAUTHORIZED ACCESS CLAIMS

CRITICAL **Actor Claims Access to Multiple Solar Plant Surveillance Systems in Europe**

On August 13, 2026, a pro-Russian threat actor group, "Shadow ClawZ 404," claimed to have accessed surveillance systems at multiple solar power plants across Europe, via their Telegram channel.

Source: Telegram **Actor:** Shadow ClawZ 404

CRITICAL **Actor Claims Access to ICS at Ukrainian Water Pumping Station and German Biogas Plant (NoName057(16))**

On August 13, 2026, a pro-Russian threat group, "NoName057(16)," published two posts on their Telegram channel claiming unauthorized access to industrial control system (ICS) interfaces at two facilities.

Source: Telegram

HIGH **Network Access Allegedly Tied to Six Nigeria-Based Government Websites Advertised**

On August 12, 2026, moderately credible threat actor "BigBrother" advertised network access with administrator rights allegedly tied to six Nigeria-based government websites on the predominantly English-language DDW forum DarkForums.

Source: DarkForums **Actor:** BigBrother

DATA BREACHES & LEAKS

HIGH **Data Allegedly Associated with Barsheshet Eilon Advertised**

On August 13, 2026, moderately credible threat actor "HelluvaHack" advertised a dataset allegedly associated with Barsheshet Eilon, an Israel-based company that provides professional accounting, auditing, tax representation, financial reporting, and related services, on the predominantly Russian-language DDW forum Exploit.

Source: Exploit **Actor:** HelluvaHack

HIGH **Data Allegedly Tied to Pantera Capital Advertised**

On August 13, 2026, untested threat actor "bamboozle" advertised a dataset allegedly associated with Pantera Capital, a U.S.-based venture capital and hedge fund company, on Exploit.

Source: Exploit **Actor:** bamboozle

COLLECTED, PROCESSED DATA BREACHES

4 entries

VICTIM	SOURCE	THREAT ACTOR	PROCESSED RECORDS
Saint-Herblain	PwnForums	misere	1.19K
Banco Agromercantil de Guatemala	PwnForums	Blastoise	315.41K
Dürninger	PwnForums	Sophia	6.03K
Productly	PwnForums	weykofa	57.16K

PROCESSED DATA SET STATISTICS

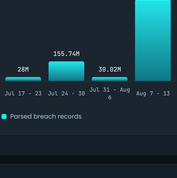
Past 4 Weeks

875.5M CAC RECORDS

948.73M BOTNET CAC RECORDS

943 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.