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 72 hours.

August 31, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

7 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
Rhysida Ransomware	City of Berlin
ShinyHunters	McKesson Corporation
ShinyHunters	Jack Henry & Associates
LockBit 5.0 Ransomware	The Heart Center of Memphis
Eclipse Ransomware	ETNA Software
Storm Ransomware	Our Hospice of South Central Indiana
EMPERADOR Ransomware	Hanwha Renewables

VULNERABILITY DISCLOSURES

4 disclosures

CVE-2026-60804
Remote Code Execution Vulnerability via Git Hook Injection in Gitea

CVE-2026-18885
Code Injection Vulerability in ServiceNow AI Platform

CVE-2026-82222
PHP Object Injection Vulnerability via Unsafe Deserialization in StellarWP GiveWP

CVE-2026-19598
Unauthenticated Privilege Escalation Vulnerability in Pods–Custom Content Types and Fields for WordPress

DEEP AND DARK WEB INTELLIGENCE

6 findings

CRITICAL FINDINGS

CRITICAL **Multiple Alleged Zero-Day Vulnerabilities Tied to Wordpress and Apache Advertised**

On August 30 and 31, 2026, untested threat actor "byte" advertised multiple alleged unpatched vulnerabilities and zero-day exploits targeting widely used WordPress plugins and an Apache Fineract, an enterprise microfinance platform, across three separate forum posts on Exploit.

Source: Exploit **Actor:** byte

NEW LEAKSITES, MARKETPLACES, FORUMS

CRITICAL **New Data Leak Site Emerges**

On August 28, 2026, ZeroFox observed a new data leak site operating under the name "Meowciety403." As of this report, the leak site lists three entities as victims and is accessible via the following dark web address: hXXp://hqhx32msbc545v233d55cvjedj5rqnv55bvzkavjv2q46qwuuannc4id[.]onion/

Source: Leak Site **Actor:** Meowciety403

CRITICAL **New Data Leak Site Emerges**

On August 31, 2026, ZeroFox observed a new data leak site operating under the name "ZaWoo." As of this report, the site lists 16 alleged victims—12 named entries with published data and 4 unnamed entries identified only by randomized company IDs. The leak site is accessible via the following dark web address:hXXps://fyenuhkq3pfhnbpidj5jm2fl2lryxip4byhg6eozynrnlomu4szf2nyd[.]onion

Source: Leak Site **Actor:** ZaWoo

UNAUTHORIZED ACCESS CLAIMS

HIGH **Network Access Allegedly Tied to U.S.-Based AI FinTech Company Advertised**

On August 27, 2026, well-regarded threat actor "888" advertised network access allegedly associated with an unnamed U.S.-Based AI FinTech company on the predominantly English-language DDW forum PwnForums.

Source: PwnForums **Actor:** 888

HIGH **Shell Access Allegedly Tied to UAE-Based Transportation Company Advertised**

On August 28, 2026, negatively reputed threat actor "SilentHex" advertised shell access with domain administrator rights allegedly tied to an unnamed UAE-based transportation company on Exploit.

Source: Exploit **Actor:** SilentHex

HACKTIVISM

HIGH **Actor Claims DDoS Attack Targeting FBI's National Instant Criminal Background Check System and eFAWATEERcom**

On August 30, 2026, a pro-Palestinian threat actor group "313 Team" claimed to have conducted a Distributed Denial-of-Service (DDoS) attack against the FBI's National Instant Criminal Background Check System (NICS).

Source: Telegram **Actor:** 313 Team

COLLECTED, PROCESSED DATA BREACHES

7 entries

VICTIM	SOURCE	THREAT ACTOR	PROCESSED RECORDS
clcv[.]org	Pwnforums	cyberjuif	11.84K
promobit[.]com	Pwnforums	Blastoise	2.04M
fanlore[.]org	PwnForums	584	158.33K
ozhairandbeauty[.]com	xpl0itrs	xpl0itrs	2M
service-civique[.]gouv[.]fr	PwnForums	efraim	58.71K
linea101[.]it	DarkForums	Sophia01	389
mvision[.]fr	PwnForums	2019	1.88K

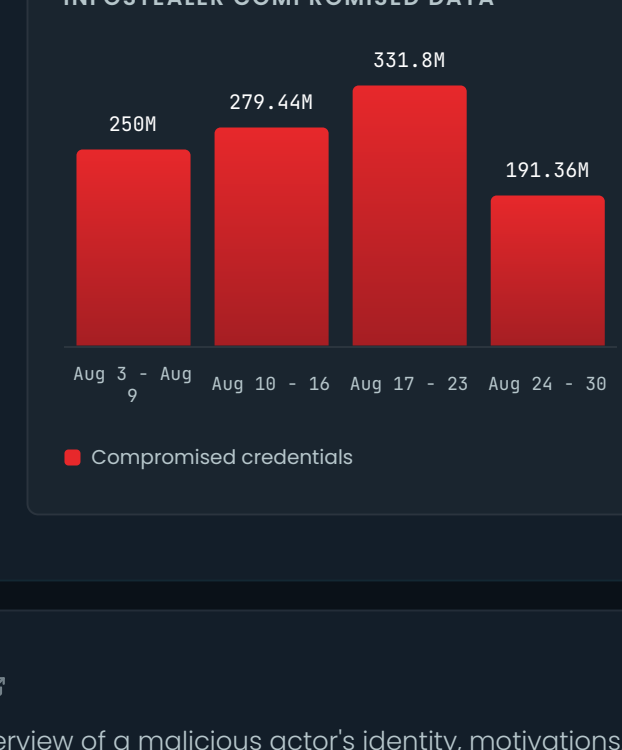
PROCESSED DATA SET STATISTICS

Past 4 Weeks

1.18B
CAC RECORDS

1.05B
BOTNET CAC RECORDS

972
RANSOMWARE & DIGITAL EXTORTION



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.