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 25, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

7 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
Dark Project	Design-Aire Engineering
Booba Project Ransomware	Chernyy & Associates
LockBit 5.0 Ransomware	ADT
Storm Ransomware	The Cecilian Bank
Storm Ransomware	Pinnacle Hospital
Rhysida Ransomware	Battle Creek Public Schools
CoinbaseCartel Ransomware	Integrated Health Systems

VULNERABILITY DISCLOSURES

4 disclosures

CVE-2026-75501
Missing Authentication Vulnerability for Critical Function in Calix GS7 XGS (GS5239XG) Router

CVE-2026-65770
Remote Code Execution Vulnerability in Microsoft Azure Managed Instance for Apache Cassandra

CVE-2026-20315
Improper Access Control Vulnerability in Cisco Secure Workload

CVE-2026-69836
Remote Code Execution Vulnerability in Microsoft Entra ID

DEEP AND DARK WEB INTELLIGENCE

8 findings

CRITICAL FINDINGS

CRITICAL **Alleged Large-Scale Brazil-Based Organizations' Data Sets Advertised**

On August 24, 2026, untested threat actor "pl4t0v" advertised a collection of over 100 allegedly compromised Brazilian data sets for sale across the predominantly English-language DDW forums PwnForums and DarkForums.

Source: PwnForums/DarkForums **Actor:** pl4t0v

CRITICAL **Alleged U.S. and EU Email Address and Password Data Set Advertised**

On August 24, 2026, untested threat actor "sprite1" advertised an alleged U.S. and EU data set containing email address and password combinations on the predominantly Russian-language DDW forum Exploit.

Source: Exploit **Actor:** sprite1

CRITICAL **2026 Consumer Databases Allegedly Spanning Multiple Countries Advertised**

On August 24, 2026, untested threat actor "Mister777" advertised on Exploit alleged consumer databases dated 2026 collected from various sources.

Source: Exploit **Actor:** Mister777

UNAUTHORIZED ACCESS CLAIMS

HIGH **Network Access Allegedly Tied to Sweden-Based Software Company Advertised**

On August 20, 2026, untested threat actor "stalled" advertised network access with domain user rights allegedly tied to an unnamed Sweden-based software company on PwnForums.

Source: PwnForums **Actor:** stalled

HIGH **Root Access Allegedly Tied to a Large User Experience Research Platform Advertised**

On August 24, 2026, moderately credible threat actor "GeshaRB" advertised on Exploit an auction for root access of a web analytics service allegedly tied to a large user experience research platform.

Source: Exploit **Actor:** GeshaRB

VULNERABILITY EXPLOITATION

CRITICAL **Alleged WordPress Plugin Zero-Day for Unauthorized Email Sending Advertised**

On August 24, 2026, well-regarded threat actor "Baiden" advertised a source code for a zero-day exploit allegedly targeting a popular WordPress plugin on Exploit.

Source: Exploit **Actor:** Baiden

HIGH **One-Day XSS Exploit for Outlook and Zimbra Advertised**

On August 22, 2026, untested threat actor "Bratubrat" advertised an alleged one-day XSS exploit for Outlook and Zimbra on the Exploit forum.

Source: Exploit **Actor:** Bratubrat

PHISHING

HIGH **Alleged Fasa Phishing Kit Advertised for Rent**

On August 22, 2026, untested threat actor "kokolokov2" advertised for rent an alleged phishing platform named Fasa on the predominantly English-language DDW forum BreachForums (breached[.]st).

Source: BreachForums **Actor:** kokolokov2

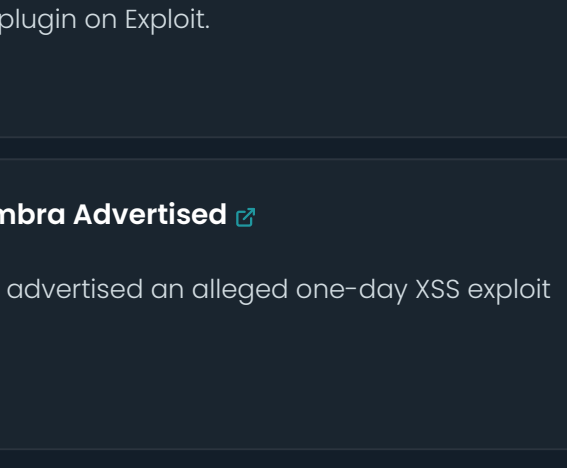
PROCESSED DATA SET STATISTICS

Past 4 Weeks

1.3B	990.28M	1K
CAC RECORDS	BOTNET CAC RECORDS	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.