

Deep and Dark Web Intelligence Reporting

Here is a curated list of critical incidents and compromised data observed on DDW ransomware sites, forums, and marketplaces ingested into the ZeroFox Platform in the past 24 hours.

October 22, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

6 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
LeakedData Ransomware	Porter Hedges
INTERLOCK Ransomware	Coastal Alabama Community College
Akira Ransomware	Flextron Circuit Assembly
Everest	The PLD Group
Everest	Lanham Associates
Uways Qarani	Mohammed Hadi Al-Rasheed & Partners Co.

VULNERABILITY DISCLOSURES

7 disclosures

CVE-2026-109619
Use After Free Vulnerability in PHP
CVE-2026-109618
Use After Free Vulnerability in PHP
CVE-2026-96652
Server-Side Request Forgery Vulnerability in Plex Media Server
CVE-2026-96656
Arbitrary File Write Vulnerability in Plex Media Server
CVE-2026-96655
Server-Side Request Forgery Vulnerability in Plex Media Server
CVE-2026-96654
Improper Neutralization of Encoded URI Schemes Vulnerability in Plex Media Server
CVE-2026-110264
Integer Overflow Vulnerability in GitLab CE/EE

DEEP AND DARK WEB INTELLIGENCE

6 findings

THREAT ACTOR PROFILE

HIGH

Threat Actor Profile: Rhysida Raas

Rhysida, a financially motivated ransomware-as-a-service (RaaS) operation, very likely remains an active and steady threat, with a posting tempo that has recovered after a quieter period earlier this year. The group likely continues to primarily target organizations that face public and regulatory pressure after a breach, including public-sector bodies, schools, and hospitals, and ZeroFox has observed a recent shift toward targeting legal services providers.

Actor: Rhysida

HIGH

Threat Actor Profile: Gunra Raas

ZeroFox assesses that Gunra, a financially motivated double-extortion ransomware-as-a-service (RaaS) operation built on leaked Conti source code, will very likely continue operating in the near term.

Actor: Gunra

CRITICAL FINDINGS

CRITICAL

Alleged PII Databases Associated with EU and U.S. Organizations Advertised

On October 20, 2026, untested threat actor “ErnestoCheGuevar” advertised alleged personally identifiable information (PII) databases associated with organizations in the European Union and the United States on a predominantly Russian-language DDW forum Exploit.

Source: Exploit **Actor:** ErnestoCheGuevar

NEW LEAKSITES, MARKETPLACES, FORUMS

CRITICAL

New Data Leak Site Emerges

On October 22, 2026, ZeroFox observed a new data leak site named “Mimori.” As of this report, the leak site listed two entities.

Actor: Mimori

DATA BREACHES & LEAKS

HIGH

Data Allegedly Tied to Switzerland-Based Marketplace Ricardo Advertised

On October 21, 2026, an untested threat actor “EnricoIII” advertised an auction for a data set allegedly associated with the Switzerland-based marketplace Ricardo, owned by SMG Swiss Marketplace Group, on Exploit.

Source: Exploit **Actor:** EnricoIII

UNAUTHORIZED ACCESS CLAIMS

HIGH

VPN and RDP Access Allegedly Tied to U.S.-Based Commercial & Residential Construction Company Advertised

On October 21, 2026, an untested threat actor “Delacroix” advertised an auction for VPN and RDP access with domain user rights allegedly tied to an unnamed U.S.-based commercial and residential construction company on Exploit.

Source: Exploit **Actor:** Delacroix

COLLECTED, PROCESSED DATA BREACHES

5 entries

VICTIM	SOURCE	THREAT ACTOR	PROCESSED RECORDS
sxcrani[.]org	PwnForums	Sensitive2025	7.33K
orait[.]it	DarkForums	Sophia01	3.95K
upntabasco.edu[.]mx	DarkForums	Lvn4tlk0	361
sanpedro-valle.gov[.]co	DarkForums	Azelmodsx677	15.11K
cultura.gob[.]mx	DarkForums	Frouzenx	203

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.