

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 23, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

6 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
Akira Ransomware	Annapath
Handala Hack Team	Otech
Brain Cipher Ransomware	Nova Group GBC
Brain Cipher Ransomware	O'Flaherty Law
LeakedData	Kirkland & Ellis
Everest	PwC

VULNERABILITY DISCLOSURES

3 disclosures

CVE-2026-114625

SQL Injection in Arista VeloCloud Orchestrator

CVE-2026-83938

Missing Authentication for Critical Function in Microsoft Azure Kubernetes Configuration Service

CVE-2026-91403

Improper Certificate Validation in Oracle Java SE / GraalVM (JSSE)

DEEP AND DARK WEB INTELLIGENCE

5 findings

VULNERABILITY EXPLOITATION

CRITICAL

Threat Actors Discuss and Share Alleged PHP2Shell Exploits

PHP2Shell—two critical PHP engine vulnerabilities rated 9.2 on CVSS v4.0—drew immediate DDW attention after exploit details leaked ahead of coordinated disclosure on October 21, 2026.

Source: XSS/Exploit **Actor:** sLo0n

HIGH

Alleged Chromium RCE Exploit Targeting Windows 10 and 11 Advertised

On October 21, 2026, untested threat actor "xynapse" advertised an alleged Chromium remote code execution exploit chain targeting Windows on a predominantly English-language DDW forum DarkForums.

Source: DarkForums **Actor:** xynapse

DATA BREACHES & LEAKS

HIGH

Data Allegedly Tied to Meria Advertised

On October 21, 2026, untested threat actor "yurikino" advertised a data set allegedly associated with the France-based financial software Meria on a predominantly Russian-language DDW forum Exploit.

Source: Exploit **Actor:** yurikino

HIGH

Data Allegedly Tied to U.S.-Based Travel Insurance Broker Advertised

On October 21, 2026, well-reputed threat actor "erafohilerafohil" advertised an auction for a dataset allegedly associated with an unnamed U.S.-based travel insurance broker on Exploit.

Source: Exploit **Actor:** erafohilerafohil

HIGH

Data Allegedly Tied to Finary Advertised

On October 21, 2026, untested threat actor "yurikino" advertised a data set allegedly associated with the France-based finance and investing software Finary on Exploit.

Source: Exploit **Actor:** yurikino

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.