

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 13, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

5 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
OROVA Ransomware	The Park Lane Hong Kong
Termite Ransomware	iDentalSoft
NightSpire Ransomware	KP Industries
Chaos Ransomware	Astrana Health
INTERLOCK Ransomware	Nu-Quest Distribution

VULNERABILITY DISCLOSURES

2 disclosures

CVE-2026-85097

Unauthenticated Arbitrary File Upload Vulnerability Leading to Remote Code Execution in Bricksforge for WordPress

CVE-2026-97229

Integer Overflow in GitLab CE/EE CI/CD Regular Expression Compiler

DEEP AND DARK WEB INTELLIGENCE

6 findings

CRITICAL FINDINGS

HIGH

Surge in Activity with 38 New Victims Added

On October 13, 2026, ZeroFox observed that n0n ransomware group listed 38 new victims on their leak site.

Source: n0n Ransomware Actor: n0n

DATA BREACHES & LEAKS

HIGH

Data Allegedly Associated with Ampath Laboratories Advertised

On October 13, 2026, moderately credible threat actor "bytetobreach" advertised data allegedly associated with Ampath Laboratories, a South Africa-based pathology laboratory and diagnostic services provider on a predominantly English-language DDW forum PwnForums.

Source: PwnForums Actor: bytetobreach

HIGH

Data Allegedly Associated with SoftBank Corp. Advertised

On October 10, 2026, untested threat actor "tet" advertised data allegedly associated with SoftBank Corp. on a predominantly English-language DDW forum DarkForums.

Source: DarkForums Actor: tet

HIGH

Data Set Allegedly Containing U.S. Notary Records Advertised

On October 11, 2026, well-reputed threat actor "erafohilerafohil" advertised an auction for a data set titled "National Register of Notaries of the United States," allegedly containing 94,202 records, on a predominantly Russian-language DDW forum Exploit.

Source: Exploit Actor: erafohilerafohil

VULNERABILITY EXPLOITATION

HIGH

Alleged WordPress Plugin Zero-Day Enabling Web Shell Upload and Administrator Account Creation Advertised

On October 13, 2026, untested threat actor "unspoken" advertised an alleged zero-day vulnerability affecting a widely used WordPress plugin on Exploit.

Source: Exploit Actor: unspoken

UNAUTHORIZED ACCESS CLAIMS

HIGH

Network Access Allegedly Tied to Brazil-Based Bank Advertised

On October 11, 2026, untested threat actor "TesseractService" advertised network access allegedly associated with an unnamed Brazil-based bank on Exploit.

Source: Exploit Actor: TesseractService

COLLECTED, PROCESSED DATA BREACHES

4 entries

VICTIM	SOURCE	THREAT ACTOR	PROCESSED RECORDS
eazytick[.]com	PwnForums	testhack90	12.93K
fansports[.]com	DarkForums	jail	9.17K
fitness-kpi[.]com	PwnForums	Syrv4x	1.85K
lsp.smknlabang.sch[.]id	DarkForums	LIVOR	983

PROCESSED DATA SET STATISTICS

Past 4 Weeks

433.12M

CAC RECORDS

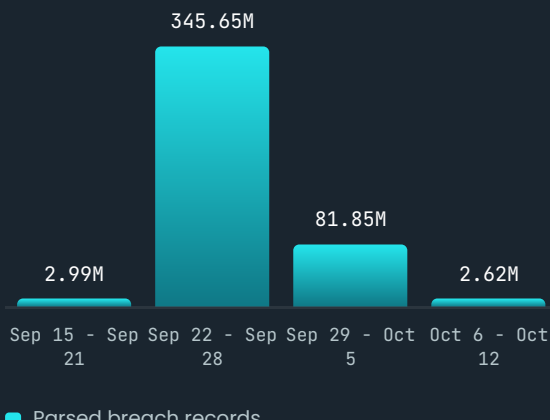
1.16B

BOTNET CAC RECORDS

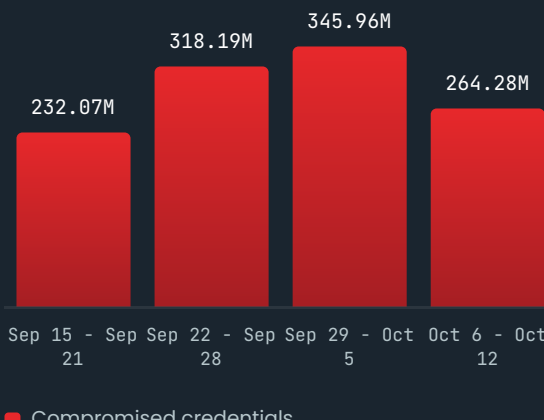
907

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.