

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 14, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

5 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
n0n Ransomware	MarieBelle New York
n0n Ransomware	Pure Options
Qilin Ransomware	RingSide Creative
Metaencryptor Ransomware	MyMichigan Health
Dark Project Ransomware	Franklin Miller

VULNERABILITY DISCLOSURES

5 disclosures

CVE-2026-96951

Mark of the Web Security Feature Bypass via Command Injection in Microsoft Windows Shell

CVE-2026-108398

Security Feature Bypass Vulnerability in Microsoft .NET Framework

CVE-2026-105445

Incorrect Privilege Assignment Vulnerability in Docker Hub

CVE-2026-104935

Authentication Bypass Vulnerability by Spoofing in Ivanti Connect Secure

CVE-2026-89111

SSRF Vulnerability in SAP Cloud SDK for Python

DEEP AND DARK WEB INTELLIGENCE

6 findings

DATA BREACHES & LEAKS

HIGH

Data Allegedly Associated with Geidea Advertised

On October 13, 2026, moderately credible threat actor "bytetobreach" advertised data allegedly associated with Geidea on a predominantly English-language DDW forum PwnForums.

Source: PwnForums **Actor:** bytetobreach

HIGH

Data Allegedly Tied to U.S.-Based Business Insurance Provider NEXT Insurance Advertised

On October 12, 2026, untested threat actor "nineteen" advertised a data set allegedly associated with NEXT Insurance on a predominantly Russian-language DDW forum Exploit.

Source: Exploit **Actor:** nineteen

UNAUTHORIZED ACCESS CLAIMS

HIGH

Fortinet Access Allegedly Tied to UK-Based Financial Services Company Advertised

On October 12, 2026, well-reputed threat actor "Big-Bro" advertised an auction for Fortinet access with domain administrator rights allegedly associated with an unnamed UK-based financial services company on Exploit.

Source: Exploit **Actor:** Big-Bro

HIGH

Fortinet Access Allegedly Tied to U.S.-Based Insurance Company Advertised

On October 12, 2026, well-reputed threat actor "Big-Bro" advertised an auction for Fortinet access with domain administrator rights allegedly associated with an unnamed U.S.-based insurance company on Exploit.

Source: Exploit **Actor:** Big-Bro

HIGH

Web Panel Access Allegedly Tied to Nigeria-Based Banking/Financial Platform Finova Advertised

On October 13, 2026, untested threat actor "Papurubatafurai" advertised an auction for web panel access with administrator rights allegedly associated with Finova on Exploit.

Source: Exploit **Actor:** Papurubatafurai

NEW LEAKSITES, MARKETPLACES, FORUMS

HIGH

New Ransomware Leak Site Emerges

On October 14, 2026, ZeroFox observed a new ransomware leak site named "HYFLOCK".

Source: Leak Site **Actor:** HYFLOCK

COLLECTED, PROCESSED DATA BREACHES

1 entries

VICTIM	SOURCE	THREAT ACTOR	PROCESSED RECORDS
caeff.com[.]py	DarkForums	Tanaka	963

PROCESSED DATA SET STATISTICS

Past 4 Weeks

433.12M

CAC RECORDS

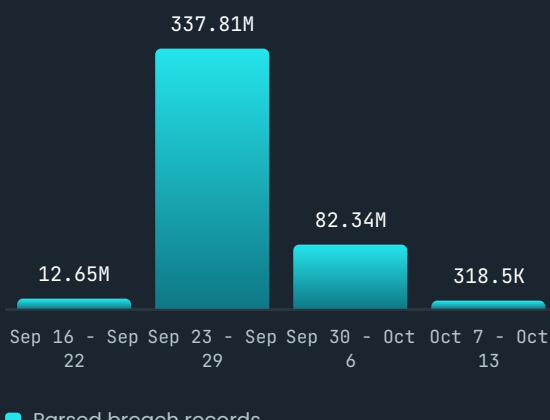
1.13B

BOTNET CAC RECORDS

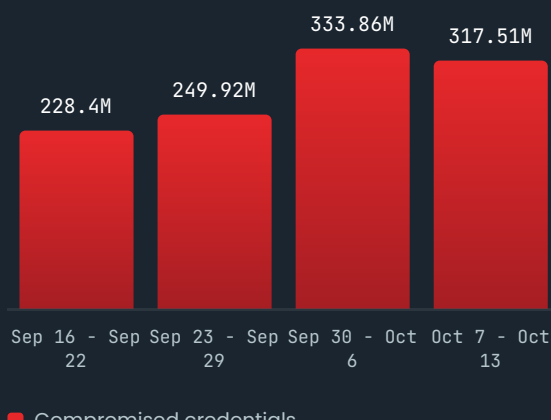
978

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.