ZEROFOX

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.

November 4, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

5 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
Booba Project Ransomware	City of Edgewater
Climax Inc. Ransomware	Setai Hotel Group
INTERLOCK Ransomware	Indiana Area School District
FALCON	Buchanan Ingersoll & Rooney PC
Booba Project Ransomware	Boardman Township Park

VULNERABILITY DISCLOSURES

3 disclosures

CVE-2026-111560
OS Command Injection Vulnerability in Multiple Barracuda Products

CVE-2026-81648
Missing Authorization Vulnerability in CryptoPayment Gateway WordPress Plugin

CVE-2026-116606
Authentication Bypass Vulnerability in Barracuda Email Security Gateway

DEEP AND DARK WEB INTELLIGENCE

11 findings

DATA BREACHES & LEAKS

HIGH **Data Allegedly Associated with Pegasus Airlines Advertised**

On November 3, 2026, untested threat actor “AckLine” advertised data allegedly associated with Pegasus Airlines on a predominantly English-language DDW forum PwnForums.

Source: PwnForums **Actor:** AckLine

HIGH **Data Allegedly Associated with U.S.-Based Software Engineering Leads Advertised**

On November 2, 2026, well-reputed threat actor "betway" advertised a data set allegedly containing over 800,000 software engineering leads located in the United States at a price of USD 500 on a predominantly Russian-language DDW forum Exploit.

Source: Exploit **Actor:** betway

MEDIUM **Data Allegedly Associated with TopDevz Advertised**

On November 2, 2026, untested threat actor "Marx1337" advertised data set allegedly associated with the U.S.-based company TopDevz on a predominantly Russian-language DDW forum XSS.

Source: XSS **Actor:** Marx1337

UNAUTHORIZED ACCESS CLAIMS

HIGH **SSL-VPN Access Allegedly Tied to Two Distinct U.S.-based Healthcare and Energy Companies Advertised**

On November 2, 2026, untested threat actor "divisibly" advertised SSL-VPN access allegedly associated with two unnamed distinct U.S.-based healthcare and energy companies on PwnForums.

Source: PwnForums **Actor:** divisibly

HIGH **Network Access Allegedly Tied to Indonesia-Based Hotel Chain Advertised**

On November 3, 2026, untested threat actor "conductor001" advertised an auction for network access allegedly associated with an unnamed Indonesia-based hotel chain on Exploit.

Source: Exploit **Actor:** conductor001

HIGH **Network Access Allegedly Tied to Spain-Based Hotel Chain Advertised**

On November 3, 2026, untested threat actor "conductor001" advertised an auction for network access allegedly associated with an unnamed Spain-based hotel chain on Exploit.

Source: Exploit **Actor:** conductor001

HIGH **Hotel Property Management System Access Allegedly Associated with Latin American Hotels Advertised**

On November 4, 2026, untested threat actor “sora” advertised access to hotel property management system (PMS) dashboards allegedly associated with hotels in Latin America on Exploit.

Source: Exploit **Actor:** sora

VULNERABILITY EXPLOITATION

HIGH **Alleged Turborepo Zero-Day Exploit Advertised**

On November 3, 2026, untested threat actor “EVIDENCE” advertised an alleged zero-day exploit affecting Turborepo on a predominantly English-language DDW forum BreachForums (breached[.]st).

Source: BreachForums **Actor:** EVIDENCE

NEW LEAKSITES, MARKETPLACES, FORUMS

CRITICAL **New Ransomware Leak Site Emerges**

On November 4, 2026, ZeroFox observed a new data leak site named "DESTELLO."

Source: Leak Site **Actor:** DESTELLO

CRITICAL **New Data Leak Site Emerges**

On November 4, 2026, ZeroFox observed a new data leak site named "AOQIN LEAKS."

Source: Leak Site **Actor:** AOQIN LEAKS

CRITICAL **New Data Leak Site Emerges**

On November 4, 2026, ZeroFox observed a new data leak site named "OBSOFT."

Source: Leak Site **Actor:** OBSOFT

COLLECTED, PROCESSED DATA BREACHES

1 entries

VICTIM	SOURCE	THREAT ACTOR	PROCESSED RECORDS
jamundi[.]gov[.]co	DarkForums	Azelmodsx677	14.86K

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.