

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 21, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

6 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
Nitrogen Ransomware	Walbro
Qilin Ransomware	Grupo Crónica
LeakedData	Latham & Watkins
REDACT	Parker Hannifin
n0n Ransomware	Kingwood Endoscopy
SCARLETTGROUP	NBCUniversal

VULNERABILITY DISCLOSURES

1 disclosure

CVE-2026-110936

DLL Side-Loading Vulnerability in Siemens Software Center

DEEP AND DARK WEB INTELLIGENCE

9 findings

THREAT ACTOR PROFILE

MEDIUM

Threat Actor Profile: NightSpire Raas

NightSpire is a financially motivated ransomware operation that emerged in early 2025 and launched its Tor-based leak site in March 2025. It runs a double-extortion model—stealing data before encrypting it with a custom Go encryptor that appends the .nspire extension—and has claimed more than 240 victims across five global regions.

CRITICAL FINDINGS

CRITICAL

New Data Leak Site Emerges

On October 21, 2026, ZeroFox observed a new data leak site named "WHITEARMOR."

Source: Leak Site **Actor:** WHITEARMOR

HIGH

Cryptographic Keys Allegedly Associated with eMudhra Leaked

On October 21, 2026, untested threat actor "kedrlog" leaked cryptographic keys allegedly associated with eight eMudhra intermediate certificate authorities (CAs) on a predominantly Russian-language DDW forum Exploit.

Source: Exploit **Actor:** kedrlog

DATA BREACHES & LEAKS

HIGH

Data Allegedly Associated with State Bank of India Leaked

On October 16, 2026, untested threat actor "Siriusim" leaked customer data associated with State Bank of India (SBI) on a predominantly English-language DDW forum BreachForums (bf[.]st).

Source: BreachForums **Actor:** Siriusim

HIGH

PII Data Allegedly Tied to U.S.-Based Transportation Company Advertised

On October 20, 2026, untested threat actor "Barb" advertised an auction for a data set allegedly associated with an unnamed U.S.-based transportation company using HubSpot CRM, on Exploit.

Source: Exploit **Actor:** Barb

HIGH

Data Allegedly Tied to UNINTER Advertised

On October 20, 2026, untested threat actor "Kazu" advertised a data set allegedly associated with the Brazil-based distance learning education platform UNINTER on Exploit.

Source: Exploit **Actor:** Kazu

UNAUTHORIZED ACCESS CLAIMS

HIGH

Fortinet Access Allegedly Tied to Argentina-Based Business Services Company Advertised

On October 19, 2026, well reputed threat actor "Big-Bro" advertised an auction for Fortinet access with domain administrator rights allegedly associated with an unnamed Argentina-based business services company on Exploit.

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

HIGH

Network Access Allegedly Tied to U.S.-Based B2B Digital Agency Advertised

On October 19, 2026, untested threat actor "Barb" advertised an auction for full chain hosting access to a U.S.-based B2B digital agency, including Cloudways account keys, GitHub Personal Access Tokens (PATs), and access to over 20 WordPress sites and 183 repositories on Exploit.

Source: Exploit **Actor:** Barb

VULNERABILITY EXPLOITATION

HIGH

Alleged BYOVD Driver Exploit Kit with Source Code Advertised

On October 21, 2026, moderately credible threat actor "Cruciferra" advertised a kit of Bring Your Own Vulnerable Driver (BYOVD) drivers with proof-of-concept source code on Exploit.

Source: Exploit **Actor:** Cruciferra

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.