

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 16, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

5 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
Akira Ransomware	Videk
n0n Ransomware	Interior Technologies
The Gentlemen Ransomware	MoneyGram
n0n Ransomware	Hunter Neurology
Wallstreet Ransomware	Green Clinic Health System

VULNERABILITY DISCLOSURES

3 disclosures

CVE-2026-108097

Remote Code Execution Vulnerability in Drupal Core

CVE-2026-110447

OS Command Injection Vulnerability in Collabora Online Built-in CODE Server

CVE-2026-99999

Memory Corruption Vulnerability in Linux Kernel

DEEP AND DARK WEB INTELLIGENCE

10 findings

CRITICAL FINDINGS

CRITICAL

Data Breach Allegedly Associated with H&M Advertised; Suspected ShinyHunters Impersonation

On October 8, 2026, a Telegram channel operated by untested threat actor "ShinyHunters," accessible via t[.]me/UNC6040prt2 claims to have breached H&M and leaked sample data allegedly associated with the company on the channel.

Source: Telegram **Actor:** ShinyHunters

DATA BREACHES & LEAKS

HIGH

Data Allegedly Associated with Betashares Advertised

On October 16, 2026, untested threat actor "nineteen" advertised data allegedly associated with Betashares on a predominantly English-language DDW forum PwnForums.

Source: PwnForums **Actor:** nineteen

HIGH

Data Allegedly Tied to Qatar-Based E-Commerce Company Garey Trading Advertised

On October 15, 2026, untested threat actor "Marx1337" advertised a data set allegedly associated with Garey Trading on a predominantly Russian-language DDW forum XSS.

Source: XSS **Actor:** Marx1337

HIGH

Data Allegedly Tied to UAE-Based EV Charging Solution Company 4EVo Advertised

On October 15, 2026, untested threat actor "Marx1337" advertised a data set allegedly associated with 4EVo on XSS.

Source: XSS **Actor:** Marx1337

HIGH

Data Allegedly Tied to Kuwait-Based Online Food Ordering Company Talabat Advertised

On October 15, 2026, untested threat actor "Marx1337" advertised a data set allegedly associated with Talabat on XSS.

Source: XSS **Actor:** Marx1337

HIGH

Data Allegedly Tied to Canada-Based Real Estate Platform ViewPoint Advertised

On October 15, 2026, untested threat actor "nineteen" advertised a data set allegedly associated with ViewPoint on a predominantly Russian-language DDW forum Exploit.

Source: Exploit **Actor:** nineteen

HIGH

Alleged PII Data from U.S.-Based Credit Bureau Advertised

On October 14, 2026, untested threat actor "blacklotus71" advertised an auction for a data set allegedly obtained from an unnamed U.S.-based credit bureau on Exploit.

Source: Exploit **Actor:** blacklotus71

UNAUTHORIZED ACCESS CLAIMS

HIGH

Bot Access Allegedly Tied to Undisclosed U.S.-Based Company Advertised

On October 14, 2026, well-reputed threat actor "Big-Bro" advertised an auction for Bot access with domain user rights allegedly associated with an undisclosed U.S.-based company on Exploit.

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

HIGH

Network Access Allegedly Tied to Bahrain-Based Mining Company Advertised

On October 14, 2026, untested threat actor "mochachosman" advertised an auction for proxy or Remote Desktop Protocol (RDP) access with domain administrator rights allegedly associated with an unnamed Bahrain-based mining company on Exploit.

Source: Exploit **Actor:** mochachosman

NEW LEAKSITES, MARKETPLACES, FORUMS

HIGH

New Data Leak Site Emerges

On October 16, 2026, ZeroFox observed a new data leak site named "THE SEVEN DEADLY SINS".

Source: Leak Site **Actor:** THE SEVEN DEADLY SINS

PROCESSED DATA SET STATISTICS

Past 4 Weeks

510.19M

CAC RECORDS

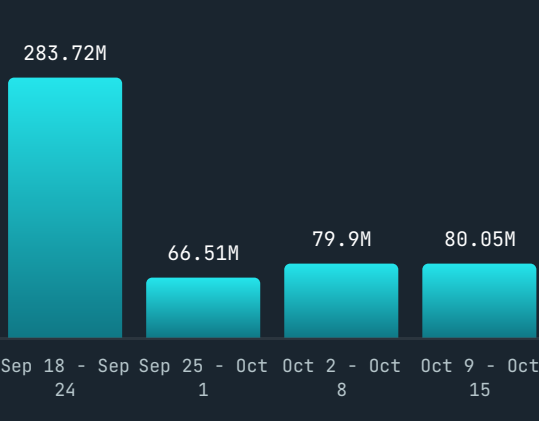
1.14B

BOTNET CAC RECORDS

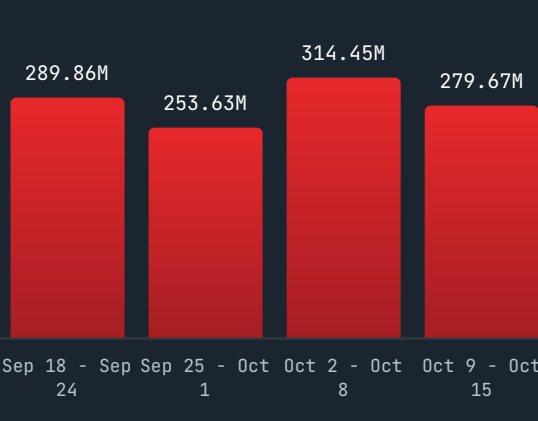
990

RANSOMWARE & DIGITAL EXTORTION

PROCESSED DATA BREACH RECORDS



INFESTEALER 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.