

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 72 hours.

October 19, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

5 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
REDACT	ONEOK
INC Ransomware	Verveba Telecom
n0n Ransomware	Polaris Shipping
Qilin Ransomware	Kemlows Diecasting Products
HYFLOCK Ransomware	Nodhom

VULNERABILITY DISCLOSURES

3 disclosures

CVE-2026-106931

OS Command Injection Vulnerability in EG Secure Solutions SiteGuard Server Edition

CVE-2026-103849

Server-Side Template Injection Vulnerability in Adobe Commerce

CVE-2026-102764

Authentication Bypass Vulnerability in BeyondTrust Remote Support

DEEP AND DARK WEB INTELLIGENCE

8 findings

CRITICAL FINDINGS

CRITICAL

Data Allegedly Associated with AstraZeneca Advertised

On October 16, 2026, untested threat actor "TheHatman" advertised data allegedly associated with AstraZeneca on a predominantly English-language DDW forum PwnForums. The actor posted the identical advertisement under the same handle on predominantly English-language DDW forums Spear and DarkForums.

Source: PwnForums **Actor:** TheHatman

CRITICAL

Data Allegedly Associated with Cardinal Health Advertised

On October 16, 2026, untested threat actor "TheHatman" advertised data allegedly associated with Cardinal Health on a predominantly English-language DDW forum PwnForums. The actor posted the identical advertisement under the same handle on Spear and DarkForums.

Source: PwnForums **Actor:** TheHatman

DATA BREACHES & LEAKS

HIGH

Data Allegedly Associated with Wyndham Hotels & Resorts and Dubai Police Advertised

On October 16, 2026, moderately credible threat actor "omerta" advertised a data set allegedly associated with, and likely referencing, the UAE-based operational unit of Wyndham Hotels & Resorts on a predominantly Russian-language DDW forum Exploit.

Source: Exploit **Actor:** omerta

HIGH

Alleged 1.7 Million U.S. Corporate Leads Data set Advertised

On October 15, 2026, a well-regarded threat actor "betway" advertised a data set allegedly containing over 1.7 million corporate leads from the United States on Exploit.

Source: Exploit **Actor:** betway

HIGH

Data Allegedly Associated with U.S. Medical Clinic Advertised

On October 17, 2026, untested threat actor "41stan5th" advertised a data set allegedly associated with a U.S. medical clinic on Spear.

Source: Spear **Actor:** 41stan5th

HIGH

Data Allegedly Associated with Ministry of Health of the Province of Chaco Advertised

On October 17, 2026, moderately credible threat actor "GordonFreeman" advertised data allegedly associated with Ministerio de Salud de la Provincia del Chaco (Ministry of Health of Chaco), Argentina on DarkForums.

Source: DarkForums **Actor:** GordonFreeman

VULNERABILITY EXPLOITATION

HIGH

Alleged Zero-Day Exploit Targeting New Zealand Government Certificates API Advertised

On October 18, 2026, untested threat actor "marlanwg" advertised an alleged zero-day insecure direct object reference (IDOR) vulnerability affecting a New Zealand government certificates API on DarkForums.

Source: DarkForums **Actor:** marlanwg

HIGH

Alleged Google Account Takeover 0-Day Exploit Advertised

On October 18, 2026, untested threat actor "fang" advertised an alleged zero-day account takeover vulnerability affecting Google accounts on Spear.

Source: Spear **Actor:** fang

COLLECTED, PROCESSED DATA BREACHES

1 entries

VICTIM	SOURCE	THREAT ACTOR	PROCESSED RECORDS
pazarama[.]com	DarkForums	emretix	401

PROCESSED DATA SET STATISTICS

Past 4 Weeks

529.03M

CAC RECORDS

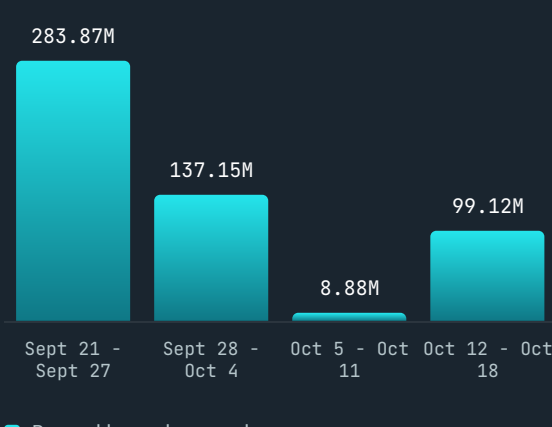
1.08B

BOTNET CAC RECORDS

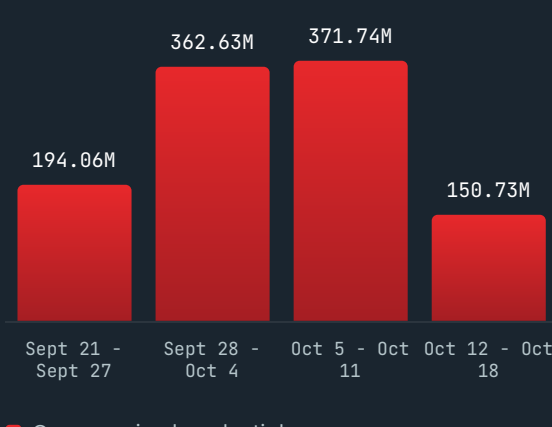
938

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.