

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 8, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

7 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
LockBit 5.0 Ransomware:	Capital Bank
Lockbit 5.0 Ransomware	Argentina Valores
Qilin Ransomware	Qatar National Import and Export
Inc Ransomware	City of Cloverdale
Inc Ransomware	UAE Pro League
Interlock Ransomware	Riviera Healthcare Center
Vypr	JPS Health Network

VULNERABILITY DISCLOSURES

1 disclosure

[CVE-2026-102255](#)

Pre-Authentication SSRF Vulnerability in SonicWall SMA1000

DEEP AND DARK WEB INTELLIGENCE

9 findings

CRITICAL FINDINGS

CRITICAL

[Alleged Disclosure of U.S.- and Israel-based Government Entities' and Individuals' Data](#)

On October 8, 2026, ZeroFox identified a site claiming to host data allegedly associated with multiple U.S.-based organizations, the Israel Police, and high-profile individuals from the United States and Israel.

Source: Dark Website

CRITICAL

[Alleged Silent Ransom Group Operational Archive Leaked](#)

On October 8, 2026, ZeroFox identified a site claiming to host data allegedly associated with the Silent Ransom Group (SRG).

Source: Dark website

CRITICAL

[New Data Leak Site Emerges \(SCARLETTGROUP\)](#)

On October 8, 2026, ZeroFox observed a new data leak site named "SCARLETTGROUP."

Source: Leak site **Actor:** scarlettgroup

DATA BREACHES & LEAKS

CRITICAL

[Data Allegedly Associated with FDCTech Advertised \(nineteen\)](#)

On October 7, 2026, untested threat actor "nineteen" advertised a data set allegedly associated with the U.S.-based financial technology company FDCTech on a predominantly Russian-language DDW forum Exploit.

Source: Exploit **Actor:** nineteen

CRITICAL

[Data Allegedly Tied to Uganda Airlines Advertised \(SilentHex\)](#)

On October 7, 2026, moderately reputed threat actor "SilentHex" advertised a data set allegedly associated with Uganda Airlines on Exploit.

Source: Exploit **Actor:** silenthex

HIGH

[Data Allegedly Tied to Government of Bahrain Advertised \(Marx1337\)](#)

On October 6, 2026, untested threat actor "Marx1337" advertised a data set associated with the Government of Bahrain on a predominantly Russian-language DDW forum XSS.

Source: Xss **Actor:** marx1337

HIGH

[Data Allegedly Tied to U.S.-Based High-Ranking Business Leads Advertised \(Spectre6272\)](#)

On October 7, 2026, untested threat actor "Spectre6272" advertised a data set of business owner leads, specifically targeting high-ranking positions such as CEO, CFO, Director, and Manager, on Exploit.

Source: Exploit **Actor:** spectre6272

HIGH

[Data Allegedly Tied to U.S.- and Canada-Based Business Owners Advertised \(FBI\)](#)

On October 7, 2026, untested threat actor "FBI" advertised a data set of U.S.- and Canada-based business owners on Exploit.

Source: Exploit **Actor:** fbi

UNAUTHORIZED ACCESS CLAIMS

HIGH

[ERP Access Allegedly Tied to Argentina-Based Retail Company Advertised \(Synoptek\)](#)

On October 7, 2026, untested threat actor "Synoptek" advertised an auction for network access with administrator rights to a ERP system allegedly associated with an unnamed Argentina-based retail company on Exploit.

Source: Exploit **Actor:** synoptek

COLLECTED, PROCESSED DATA BREACHES

2 entries

VICTIM	SOURCE	THREAT ACTOR	PROCESSED RECORDS
pharmaland[.]fr	PwnForums	Alduin	7.32K
openagent[.]sg	PwnForums	jail	25.75K

PROCESSED DATA SET STATISTICS

Past 4 Weeks

436.92M

CAC RECORDS

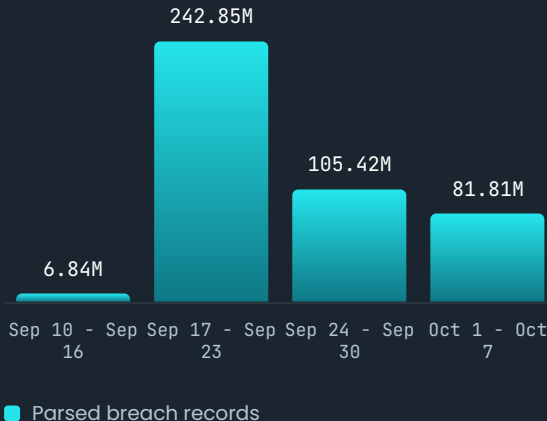
1.18B

BOTNET CAC RECORDS

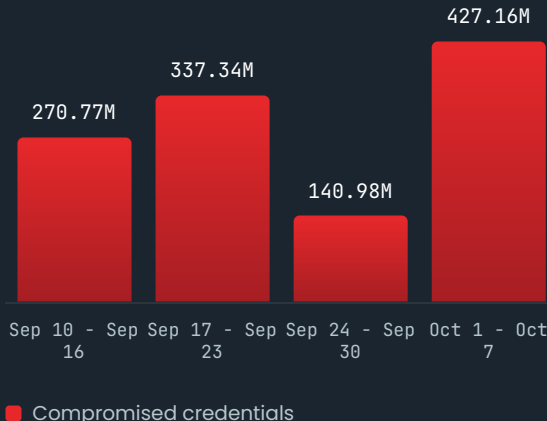
933

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.