

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 9, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

5 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
LeakedData	Baker McKenzie
LeakedData	O'Hagan Meyer
Nightspire Ransomware	Instituto Nacional de Infectologia Evandro Chagas
UMBRA Ransomware	Raqib Vision
Sovcali	Hollywood Hair

VULNERABILITY DISCLOSURES

6 disclosures

CVE-2026-76485

Stack-Based Buffer Overflow Vulnerability in Cisco NX-OS Software

CVE-2026-76471

Heap-Based Buffer Overflow Vulnerability in Cisco NX-OS Software NX-API

CVE-2026-47483

Uncontrolled Resource Consumption in NVIDIA DCGM Exporter

CVE-2026-76581

Stack-Based Buffer Overflow Vulnerability in Cisco NX-OS Software (NGOAM SRv6 OAM)

CVE-2026-76465

Free of Memory Not on the Heap (MPLS OAM Remote Code Execution) in Cisco NX-OS Software

CVE-2026-76486

Stack-Based Buffer Overflow Vulnerability in Cisco NX-OS Software

DEEP AND DARK WEB INTELLIGENCE

10 findings

THREAT ACTOR PROFILE

CRITICAL

Threat Actor Profile: VECT RaaS

The VECT ransomware operation, tracked in its more recent iteration as VECT 2.0, is a Ransomware-as-a-Service (RaaS) offering that first appeared in late December 2025. The operation emerged from Russian-language cybercrime forums. VECT operates a double-extortion model, encrypting corporate networks while systematically exfiltrating sensitive enterprise data.

CRITICAL FINDINGS

CRITICAL

New Ransomware Leak Site Emerges

On October 9, 2026, ZeroFox observed a new ransomware leak site named "NetRunner".

Source: Leak site **Actor:** NetRunner

CRITICAL

RaaS Program Dubbed "FLOCKER" Advertised

On October 7, 2026, untested threat actor "pwntoearn" advertised an affiliate program for a ransomware-as-a-service (RaaS) operation on a predominantly English-language deep and dark web forum PwnForums.

Source: PwnForums **Actor:** pwntoearn

HIGH

PMS Access and Data Allegedly Associated with 14 Luxury Hotels in USA Advertised

On October 9, 2026, moderately reputed threat actor "DDEEAALLEERR" advertised access to a management panel and data associated with 14 Luxury Hotels in the United States on a predominantly Russian-language DDW forum Exploit.

Source: Exploit **Actor:** DDEEAALLEERR

DATA BREACHES & LEAKS

HIGH

Data Allegedly Associated with Apple Advertised

On October 8, 2026, untested threat actor "Marx1337" advertised a data set allegedly associated with the U.S.-based company Apple on a predominantly Russian-language DDW forum XSS.

Source: Xss **Actor:** Marx1337

HIGH

Data Allegedly Tied to Betashares Advertised

On October 8, 2026, untested threat actor "nineteen" advertised a data set allegedly tied to an Australia-based investment management company Betashares on Exploit.

Source: Exploit **Actor:** nineteen

HIGH

Data Allegedly Tied to Jubelio Advertised

On October 7, 2026, untested threat actor "Snow_Bunnies" advertised 17 GB of freshly dumped data and 6 GB of source code belonging to Jubelio, a major Indonesian cloud-based eCommerce solution, on Exploit.

Source: Exploit **Actor:** Snow_Bunnies

UNAUTHORIZED ACCESS CLAIMS

HIGH

AnyDesk Access Allegedly Tied to U.S.-Based Legal Services Company Advertised

On October 6, 2026, untested threat actor "AFKForever" advertised AnyDesk access with local administrator rights allegedly associated with an unnamed U.S.-based legal services company on a predominantly English-language DDW forum BreachForums (breached[.]st).

Source: Breachforums **Actor:** AFKForever

HIGH

SOCKS Access Allegedly Tied to U.S.-Based Automotive Parts Manufacturing Company Advertised

On October 7, 2026, well-known threat actor "Big-Bro" advertised an auction for Socks proxy access with Domain Administrator rights allegedly associated with an unnamed U.S.-based automotive parts manufacturing company on Exploit.

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

VULNERABILITY EXPLOITATION

HIGH

Alleged VMware vCenter Server RCE Exploit Advertised

On October 9, 2026, well-reputed threat actor "SebastianPereiro" advertised an alleged remote code execution (RCE) exploit targeting VMware vSphere Server's vCenter component on Exploit.

Source: Exploit **Actor:** SebastianPereiro

COLLECTED, PROCESSED DATA BREACHES

5 entries

VICTIM	SOURCE	THREAT ACTOR	PROCESSED RECORDS
Hungary[.]hu	DarkForums	404muse	4.11K
R��������[.]fr	PwnForums	Alduin	44.74K
geonature[.]arb-����[.]fr	PwnForums	Alduin	3.4K
diagnozis[.]hu	PwnForums	Sophia	14.97K
������[.]fr	PwnForums	Sophia	176

PROCESSED DATA SET STATISTICS

Past 4 Weeks

436.99M

CAC RECORDS

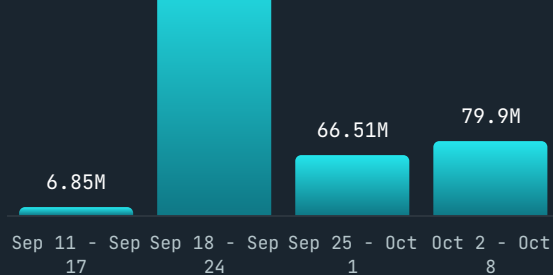
1.18B

BOTNET CAC RECORDS

920

RANSOMWARE & DIGITAL EXTORTION

PROCESSED DATA BREACH RECORDS



INFOTEALER 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