ZEROFOX

Deep and Dark Web Intelligence Reporting

Here is a curated list of critical incidents and compromised data observed on deep and dark web ransomware sites, forums, and marketplaces ingested into the ZeroFox Platform in the past 24 hours.

September 3, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

6 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
MedusaLocker Ransomware	Life Insurance Corporation of India
KRYBIT Ransomware	Arab Maritime Petroleum Transport Company
Dire Wolf Ransomware	Honeycomb Insurance
Akira Ransomware	PennFab
BravoX Ransomware	Schmidt Manufacturing
INC Ransomware	Westfield Public Schools

VULNERABILITY DISCLOSURES

2 disclosures

CVE-2026-9586

Unauthenticated SQL Injection Leading to Remote Code Execution in Sangoma Switchvox

CVE-2026-82329

Authentication Bypass in JFrog Artifactory

DEEP AND DARK WEB INTELLIGENCE

6 findings

CRITICAL FINDINGS

CRITICAL **Data Allegedly Associated with Plataforma Patria Advertised**

On September 3, 2026, a moderately credible threat actor "GordonFreeman" advertised data allegedly associated with Plataforma Patria on the predominantly English-language DDW forum DarkForums.

Source: DarkForums **Actor:** GordonFreeman

CRITICAL **Data Allegedly Associated with Ticketmaster Advertised**

On September 2, 2026, untested threat actor "brokering" advertised a database allegedly associated with Ticketmaster on the predominantly Russian-language DDW forum Exploit.

Source: Exploit **Actor:** brokering

UNAUTHORIZED ACCESS CLAIMS

HIGH **Shipment Database Management Access Allegedly Tied to Aymakan Advertised**

On September 2, 2026, untested threat actor "Keishell" advertised shipment database management access allegedly associated with Aymakan on DarkForums.

Source: DarkForums **Actor:** Keishell

HIGH **Network Access Allegedly Tied to U.S.-Based Accounting Firm Advertised**

On September 2, 2026, untested threat actor "larrypat09" advertised an auction for Dropbox access allegedly associated with U.S.-based accounting firm on Exploit.

Source: Exploit **Actor:** larrypat09

VULNERABILITY EXPLOITATION

MEDIUM **Alleged "FortiVPN" Zero-Day Vulnerability Advertised**

On September 2, 2026, untested threat actor "Dppray" advertised an alleged "FortiVPN" zero-day vulnerability on Exploit.

Source: Exploit **Actor:** Dppray

NEW LEAKSITES, MARKETPLACES, FORUMS

CRITICAL **New Ransomware Leak Site Emerges**

On September 3, 2026, ZeroFox observed a new leak site claiming to be a ransomware group, operating under the name "Vexy". As of this report, the leak site list one entity as victim and is accessible via the following dark web address:hXXp://vexytsr3chimdz6siwaqi2lvxxwfkxvffkpwyanr2llequ2hkm56jvqd[.]onion/blog

Source: Leak Site **Actor:** Vexy

COLLECTED, PROCESSED DATA BREACHES

1 entries

VICTIM	SOURCE	THREAT ACTOR	PROCESSED RECORDS
alcon[.]com	ShinyHunters	ShinyHunters	209.79K

PROCESSED DATA SET STATISTICS

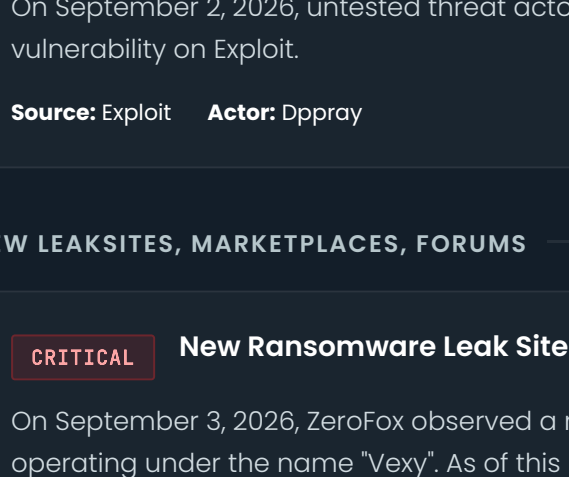
Past 4 Weeks

1.19B CAC RECORDS

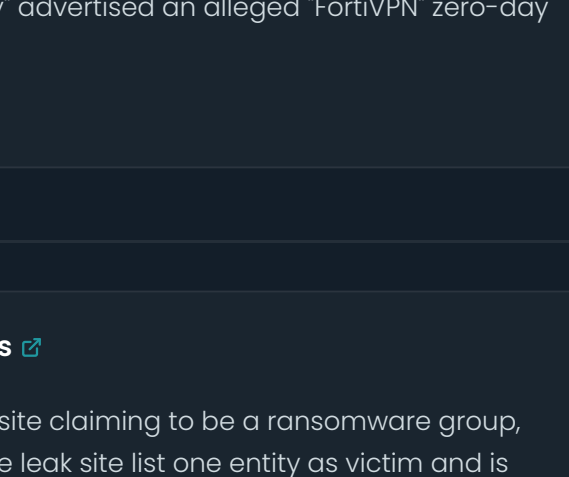
1.05B BOTNET CAC RECORDS

1.08K 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.