ZEROFOX

Deep and Dark Web Intelligence Reporting

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

July 9, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

5 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
Akira Ransomware	Wade's Dairy
CMD Organization	Mount Royal University Library
INC Ransomware	Aesthetic Surgical Images
BravoX Ransomware	PB Fiduciaire
Everest Ransomware	Oasis Legal Group

VULNERABILITY DISCLOSURES

2 disclosures

CVE-2026-54402

Command Injection via Improper Input Validation in Ubiquiti UniFi OS

CVE-2026-50746

Improper Access Control Leading to Command Injection in Ubiquiti UniFi Connect Application

DEEP AND DARK WEB INTELLIGENCE

8 findings

CRITICAL FINDINGS

CRITICAL **Alleged Breach of Nike And Alcon's Data**

On July 8, 2026, untested threat actor group "Nocturne" claimed to have leaked data associated with Nike and Alcon, on a predominantly English-language dark web forum DarkForums.

Source: DarkForums **Actor:** Nocturne

CRITICAL **Alleged Data Associated with Directorate-General for Scientific Research and Technological Development Advertised**

On July 8, 2026, an untested threat actor "anisanas2" advertised data allegedly associated with Directorate-General for Scientific Research and Technological Development (DGRSDT), on a predominantly English-language dark web forum DarkForums.

Source: DarkForums **Actor:** anisanas2

CRITICAL **Alleged GitHub Credentials Associated with Deloitte Leaked**

On July 8, 2026, untested threat actor "grave" leaked data allegedly associated with Deloitte, a UK-based company that provides auditing, consulting, risk and financial advisory, tax, and legal services, on a predominantly English language dark web forum Spear.

Source: Spear **Actor:** grave

UNAUTHORIZED ACCESS CLAIMS

HIGH **Alleged SSH Access Tied to U.S.-Based Healthcare Insurance Company Advertised**

On July 8, 2026, an untested threat actor "vegitaxi" advertised to sell SSH access with root rights allegedly associated with an unnamed U.S.-based healthcare insurance company, on a predominantly English-language dark web forum DarkForums.

Source: DarkForums **Actor:** vegitaxi

HIGH **Alleged SSL VPN Access Associated with Undisclosed U.S. and Japan-based Entities Advertised**

On July 7, 2026, an untested threat actor "maximalism" advertised to sell VPN access allegedly associated with two undisclosed companies, on a predominantly Russian-language deep and forum DUTY-FREE.

Source: DUTY-FREE **Actor:** maximalism

HIGH **Alleged VPN Access Bundle Associated with 500 Undisclosed Companies Advertised**

On July 7, 2026, an untested threat actor "sql" advertised an auction for VPN access bundle allegedly associated with 500 undisclosed companies, on a predominantly Russian-language deep and dark web forum Exploit.

Source: Exploit **Actor:** sql

DATA BREACHES & LEAKS

HIGH **Alleged Data Associated with MilleEtUneListes Leaked**

On July 7, 2026, an untested threat actor "84City" breached data allegedly associated with MilleEtUneListes, on a predominantly English-language deep and dark web forum PwnForums.

Source: PwnForums **Actor:** 84City

HIGH **Alleged Data Associated with Heavy Industries Taxila Advertised**

On July 8, 2026, an untested threat actor "Cyb3R_Shubh4M" advertised to sell a 50 GB dataset allegedly associated with Heavy Industries Taxila, a Pakistan-based primary state-owned defense manufacturing and heavy engineering organization, on a predominantly Russian-language deep and dark web forum Exploit.

Source: Exploit **Actor:** Cyb3R_Shubh4M

COLLECTED, PROCESSED DATA BREACHES

3 entries

VICTIM	SOURCE	THREAT ACTOR	PROCESSED RECORDS
cossmil[.]mil[.]bo	DarkForums	konata_izumi_shell	49.8K
[CH[HR Onboarding Database FREE!!!	DarkForums	chechnyafsbc	123
france-services[.]gouv[.]fr	PwnForums	misere	12.8K

PROCESSED DATASET STATISTICS

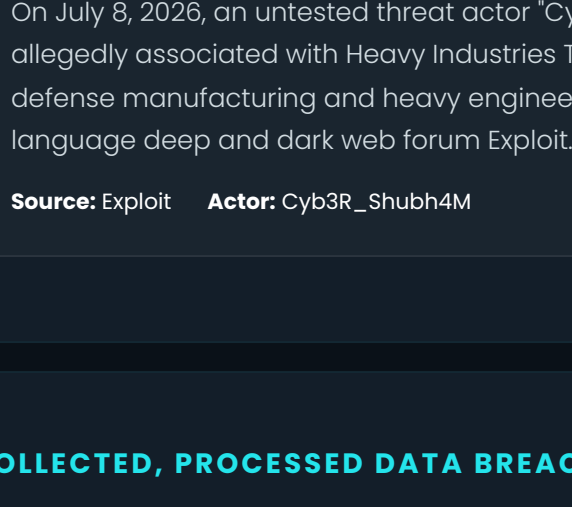
Past 4 Weeks

671.5M CAC RECORDS

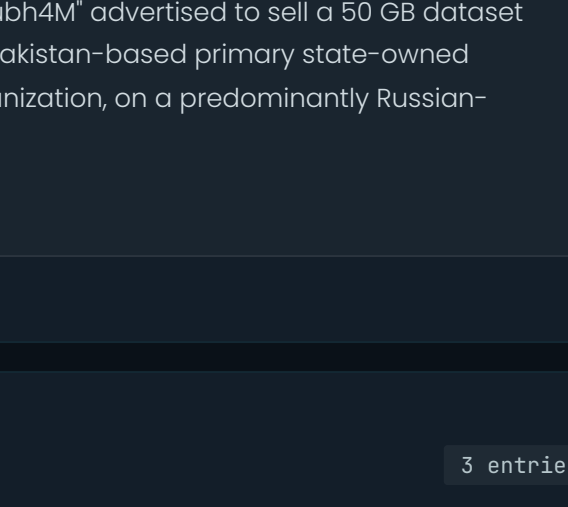
1.1B BOTNET CAC RECORDS

821 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, bizarre tactics, and significant operational spikes that deviate from the baseline threat landscape.