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 16, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

6 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
ARCUS MEDIA Ransomware	NowVertical Group
Leaknet	Anglo Belgian Corporation
AiLock	Nihon Kotsu
NightSpire Ransomware	Cedar Crest College
CMD Organization	Target Energy Solutions
Chaos Ransomware	Spectrum Chemical

VULNERABILITY DISCLOSURES

5 disclosures

CVE-2026-53412
Improper Input Validation in Zoom Workplace Desktop Client, VDI Client, and Meeting SDK for Windows

CVE-2026-27690
HTTP Request Smuggling in SAP Approuter

CVE-2026-50661
Security Feature Bypass in Microsoft Windows BitLocker

CVE-2026-15410
Code Injection in SonicWall SMA1000 Appliance Management Console

CVE-2026-44761
Use of Hardcoded Credentials in SAP Commerce Cloud

DEEP AND DARK WEB INTELLIGENCE

6 findings

CRITICAL FINDINGS

CRITICAL **Alleged Document Associated with SpaceX Starshield Architecture Advertised**

On July 14, 2026, an untested threat actor "1XL" advertised internal document allegedly associated with the SpaceX Starshield program, on a predominantly English-language dark web forum DarkForums.

Source: DarkForums **Actor:** 1XL

CRITICAL **Alleged Data Associated with Bendigo Law Courts Leaked**

On July 15, 2026, a moderately credible threat actor "2019" leaked data allegedly associated with Bendigo Law Courts, Australia, on a predominantly English-language deep and dark web forum PwnForums.

Source: PwnForums **Actor:** 2019

CRITICAL **Data Allegedly Tied to Agenția Națională de Cadastru și Publicitate Imobiliară Advertised**

On July 15, 2026, an untested threat actor "bytetobreach33" advertised data allegedly associated with genția Națională de Cadastru și Publicitate Imobiliară (ANCPI), on a predominantly English-language dark web forum BreachForums (Breached[.]su). Notably, the same actor also advertised similar dataset on multiple deep and dark web forums such as PwnForums, Spear, Exploit and DarkForums.

Source: BreachForums **Actor:** bytetobreach33

UNAUTHORIZED ACCESS CLAIMS

HIGH **Alleged FortiGate Access to UAE-Based Retail Company Advertised**

On July 15, 2026, a well-known threat actor "Big-Bro" advertised an auction for FortiGate access with administrator rights to an unnamed UAE-based retail company, on a predominantly Russian language deep and dark web forum Exploit.

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

HIGH **Alleged Network Access to Undisclosed Cloud Storage Service Advertised**

On July 15, 2026, an untested threat actor "Deadsilence" advertised an auction for network access with administrator rights to an undisclosed Cloud Storage service, on a predominantly Russian language deep and dark web forum Exploit.

Source: Exploit **Actor:** Deadsilence

DATA BREACHES & LEAKS

HIGH **Data Allegedly Tied to Monster[.]com Advertised**

On July 15, 2026, an untested threat actor "Domperidone" advertised to sell a dataset associated with Monster[.]com, a Puerto Rico-based global employment website and job search engine, on a predominantly Russian language deep and dark web forum Exploit.

Source: Exploit **Actor:** Domperidone

COLLECTED, PROCESSED DATA BREACHES

3 entries

VICTIM	SOURCE	THREAT ACTOR	PROCESSED RECORDS
Smartbox Group (smartbox[.]com)	PwnForums	misere	46.26K
Association Francophone de Padel (afpadel[.]be)	PwnForums	Lar	9.84K
Taiwan_loan_data	LeakBase	wrreg	22.21K

PROCESSED DATASET STATISTICS

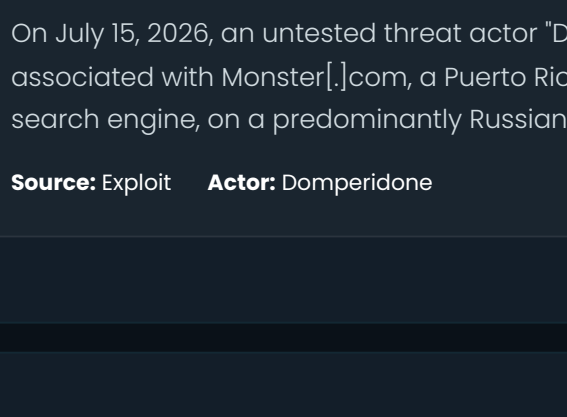
Past 4 Weeks

726.53M CAC RECORDS

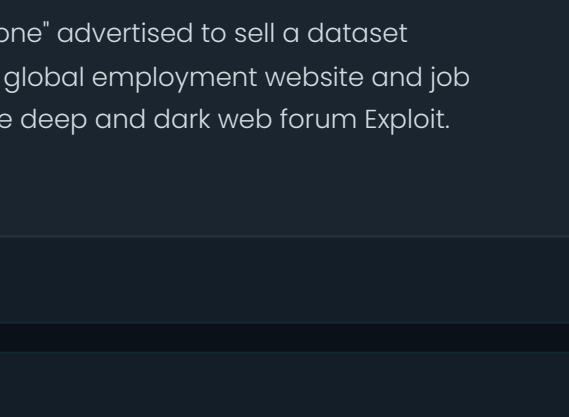
1.12B BOTNET CAC RECORDS

800 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.