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 14, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

5 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
DragonForce Ransomware	Al Saidi Group
TITAN Ransomware	Eureka Construction
DOOMMAGEDDON Ransomware	Hospital Di Camp
CMD Organization	Golden Star Resources
INTERLOCK Ransomware	Borger Independent School District

VULNERABILITY DISCLOSURES

2 disclosures

CVE-2026-56291
Unrestricted File Upload in Balbooa Forms for Joomla

CVE-2026-48939
Unauthenticated Arbitrary File Upload leading to Remote Code Execution in JoomliC iCagenda

DEEP AND DARK WEB INTELLIGENCE

7 findings

CRITICAL FINDINGS

CRITICAL **Alleged Data Associated with Demander Justice Leaked**

On July 13, 2026, a credible threat actor "misere" leaked data allegedly associated with Demander Justice, on a predominantly English-language deep and dark web forum PwnForums.

Source: PwnForums **Actor:** misere

CRITICAL **Alleged Data Associated with Accounting and Adviser Services Advertised**

On July 14, 2026, a moderately credible threat actor "2019" advertised data allegedly associated with Accounting and Adviser Services, on a predominantly English-language deep and dark web forum PwnForums.

Source: PwnForums **Actor:** 2019

UNAUTHORIZED ACCESS CLAIMS

HIGH **Alleged Web Panel Access to France-Based Assurance Company Advertised**

On July 11, 2026, an untested threat actor "brokers" advertised a web panel access with administrator rights to an unnamed France-based assurance company, on a predominantly English language deep and dark web forum DarkForums.

Source: DarkForums **Actor:** brokers

HIGH **Alleged SQL Injection Access to U.S.-Based File Hosting Advertised**

On July 10, 2026, an untested threat actor "Deadsilence" advertised an auction for SQL Injection access to an unnamed U.S.-based file hosting, on a predominantly Russian language deep and dark web forum Exploit.

Source: Exploit **Actor:** Deadsilence

VULNERABILITY EXPLOITATION

HIGH **Zero-Day Castles VEGA 3000 POS Exploit Advertised**

On July 12, 2026, an untested threat actor "platovoplomo" advertised a zero-day exploit affecting Castles VEGA 3000 Point-of-Sale (POS) terminals, on a predominantly Russian language deep and dark web forum Exploit.

Source: Exploit **Actor:** platovoplomo

DATA BREACHES & LEAKS

CRITICAL **Alleged Data of Hastings & Hastings Advertised**

On July 12, 2026, a moderately credible threat actor "Citrix_one_love" advertised an auction for a dataset associated with the U.S.-based law firm Hastings & Hastings, on a predominantly Russian language deep and dark web forum Exploit.

Source: Exploit **Actor:** Citrix_one_love

CRITICAL **Alleged Data Associated with Pakistan Army and Air Force Advertised for Sale**

On July 13, 2026, an untested threat actor "Cyb3R_Shubh4M" advertised to sell the 1.2 GB dataset associated with Pakistan Army and Air Force, on a predominantly Russian language deep and dark web forum Exploit.

Source: Exploit **Actor:** Cyb3R_Shubh4M

COLLECTED, PROCESSED DATA BREACHES

2 entries

VICTIM	SOURCE	THREAT ACTOR	PROCESSED RECORDS
5.1KK_MUSIC_TARGET_Mailpass_396	XSS	STRADU_DB	5.12M
3.1KK France FR Mailpass #398	XSS	STRADU_DB	3.13M

PROCESSED DATASET STATISTICS

Past 4 Weeks

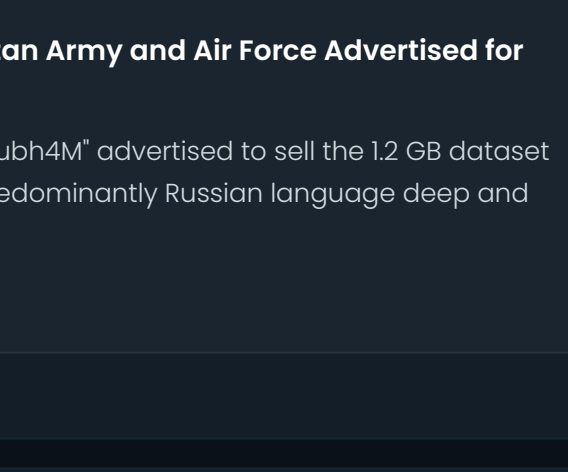
651.19M CAC RECORDS

1.12B BOTNET CAC RECORDS

764 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.