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 15, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

6 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
D1R	Bosch
DragonForce Ransomware	Asian Marine Services
DragonForce Ransomware	Momenta
Payouts King Ransomware	Casta Diva Group
SafePay Ransomware	Shuttle Meadow Country Club
ShinyHunters	Exact Sciences Corporation

VULNERABILITY DISCLOSURES

4 disclosures

CVE-2026-56155
Elevation of Privilege in Microsoft Active Directory Federation Services

CVE-2026-56164
Elevation of Privilege in Microsoft SharePoint Server

CVE-2026-15409
Server-Side Request Forgery in SonicWall SMA1000

CVE-2026-44747
Memory Corruption in SAP NetWeaver Application Server ABAP

DEEP AND DARK WEB INTELLIGENCE

6 findings

CRITICAL FINDINGS

CRITICAL **Alleged Access to Compromised Spain-Based PC Associated with CaixaBank Account Advertised**

On July 15, 2026, an untested threat actor "Johnney2024" advertised to sell alleged remote access to a compromised personal computer located in Spain, specifically targeting the Spain-based financial institution CaixaBank with an account balance of more than EUR 165,000, on a predominantly English-language dark web forum Darkforums.

Source: DarkForums **Actor:** Johnney2024

CRITICAL **Alleged Data Associated with U.S. Government Agencies Advertised**

On July 14, 2026, an untested threat actor "thesinon" advertised a dataset associated with multiple U.S. government agencies, on a predominantly English language deep and dark web forum BreachForums(breached[.]su).

Source: BreachForums **Actor:** thesinon

CRITICAL **Alleged Data Associated with Conasems Leaked**

On July 14, 2026, a well reputed threat actor "888" leaked data allegedly associated with Conasems, on a predominantly deep and dark web forum PwnForums.

Source: PwnForums **Actor:** 888

UNAUTHORIZED ACCESS CLAIMS

HIGH **Alleged RDP and Shell Access to Germany-Based Electronics Manufacturing Company Advertised**

On July 14, 2026, a well-regarded threat actor "Saturned33" advertised an auction for RDP and shell access with domain administrator, local administrator and SYSTEM rights to an unnamed Germany-based electronics manufacturing company, on a predominantly Russian language deep and dark web forum Exploit.

Source: Exploit **Actor:** Saturned33

HIGH **Alleged Network Access to Hong Kong-based VoIP MSP Company Advertised**

On July 13, 2026, an untested threat actor "endtoast" advertised VNC, SSH and web panel access with root and administrator rights to an unnamed Hong Kong-based VoIP MSP company, on a predominantly English language deep and dark web forum DarkForums.

Source: DarkForums **Actor:** endtoast

HIGH **Alleged Initial Access Associated with Three Distinct Companies Advertised**

On July 15, 2026, an untested threat actor "xpl0itrs" advertised to sell Initial Access (IA) allegedly associated with three distinct companies, on a predominantly English language dark web forum Spear. Notably, the same post was also made in the deep and dark web form PwnForums by the same threat actor.

Source: PwnForums/Spear **Actor:** xpl0itrs

COLLECTED, PROCESSED DATA BREACHES

3 entries

VICTIM	SOURCE	THREAT ACTOR	PROCESSED RECORDS
Municipality of León (leon[.]gob[.]mx)	DarkForums	cenfecracked	4.08K
700M_4	Telegram	Satanic Cloud	71.8M
2.3KK_MIX_Mailpass_395	XSS	STRADU_DB	2.38M

PROCESSED DATASET STATISTICS

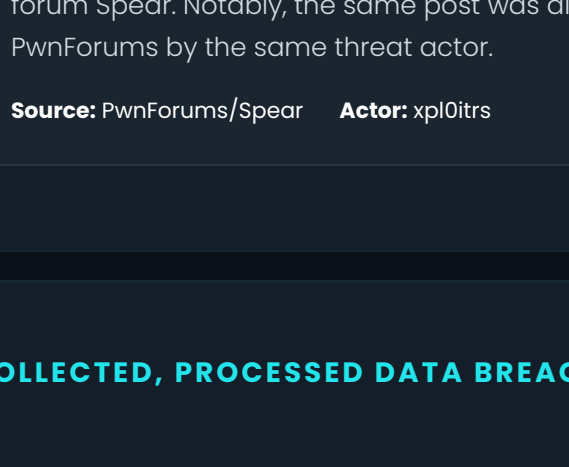
Past 4 Weeks

693.89M CAC RECORDS

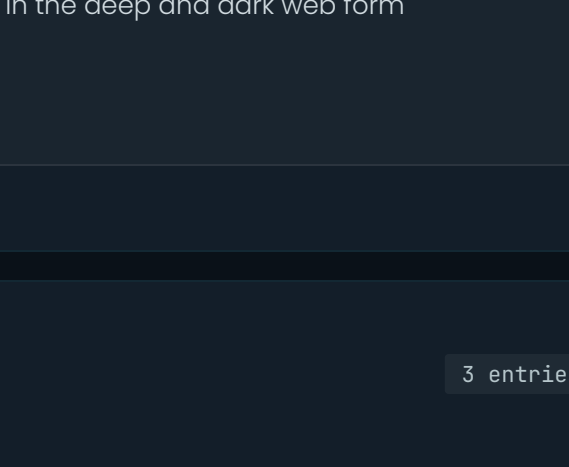
1.12B BOTNET CAC RECORDS

805 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.