

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 24, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

7 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
Shadowbyt3\$ Ransomware	Chevron
Space Bears Ransomware	Tomix
Booba Project Ransomware	Merrimack County
Booba Project Ransomware	Washington County Maine
Anubis Ransomware	Gaedke & Partner
Emperador Ransomware	Receita Federal Do Brasil
Lockbit 5.0 Ransomware	Taspen Life

VULNERABILITY DISCLOSURES

6 disclosures

CVE-2026-87900 Argument Injection Vulnerability in WebPros WP Toolkit for cPanel
CVE-2026-87899 Privilege Escalation Vulnerability in cPanel CalDAV/CardDAV
CVE-2026-94127 Heap-Based Buffer Overflow Vulnerability in F5 BIG-IP Access Policy Manager
CVE-2026-93952 Improper Input Validation Vulnerability in Arista Networks VeloCloud Orchestrator On-Prem
CVE-2026-68490 Incorrect Permission Assignment Vulnerability in cPanel CalDAV/CardDAV
CVE-2026-87902 Unauthenticated Local File Inclusion Vulnerability in WordPress Core

DEEP AND DARK WEB INTELLIGENCE

7 findings

CRITICAL FINDINGS

CRITICAL New Data Leak Site Emerges (EXFS TEAM) On September 24, 2026, ZeroFox observed a new data leak site operating under the name "EXFS TEAM." Source: breached[.]st Actor: EXFS TEAM
HIGH Alleged Uncensored LLM Service "Uncensored.monster" Advertised On September 22, 2026, untested threat actor "cbshy" advertised an alleged uncensored AI models service, under the name "Uncensored.monster," on the predominantly Russian-language DDW forum Exploit. Source: Exploit Actor: cbshy

DATA BREACHES & LEAKS

HIGH Data Allegedly Associated with Horizane Santé Leaked On September 24, 2026, well-reputed threat actor "Jaded" leaked data allegedly associated with Horizane Santé on a predominantly English-language DDW forum PwnForums. Source: PwnForums Actor: Jaded
HIGH Collection of Internal Assets Allegedly Associated with France-Based Company LVMH Advertised On September 22, 2026, untested threat actor "HollowCrimeCorp" advertised collection of internal assets allegedly associated with LVMH, a France-based luxury goods holding, on predominantly English-language DDW forum BreachForums (breached[.]st). Source: Breachforums Actor: hollowcrimecorp

UNAUTHORIZED ACCESS CLAIMS

HIGH Network Access Allegedly Tied to U.S.-Based Government Entity Advertised On September 23, 2026, untested threat actor "sapron777" advertised an auction for FortiClient VPN and FortiGate access with domain administrator rights allegedly associated with an unnamed U.S.-based government entity on Exploit. Source: Exploit Actor: sapron777
HIGH Network Access Allegedly Tied to Germany-Based Hosting Company Advertised On September 22, 2026, untested threat actor "scanner" advertised an auction for network access allegedly associated with an unnamed Germany-based hosting company on Exploit. Source: Exploit Actor: scanner
HIGH Network Access Allegedly Tied to Undisclosed TV Channel Group Advertised On September 22, 2026, untested threat actor "APT73" advertised collection of internal network assets and Active Directory domain access allegedly associated with undisclosed TV Channel Group on BreachForums. Source: Breachforums Actor: apt73

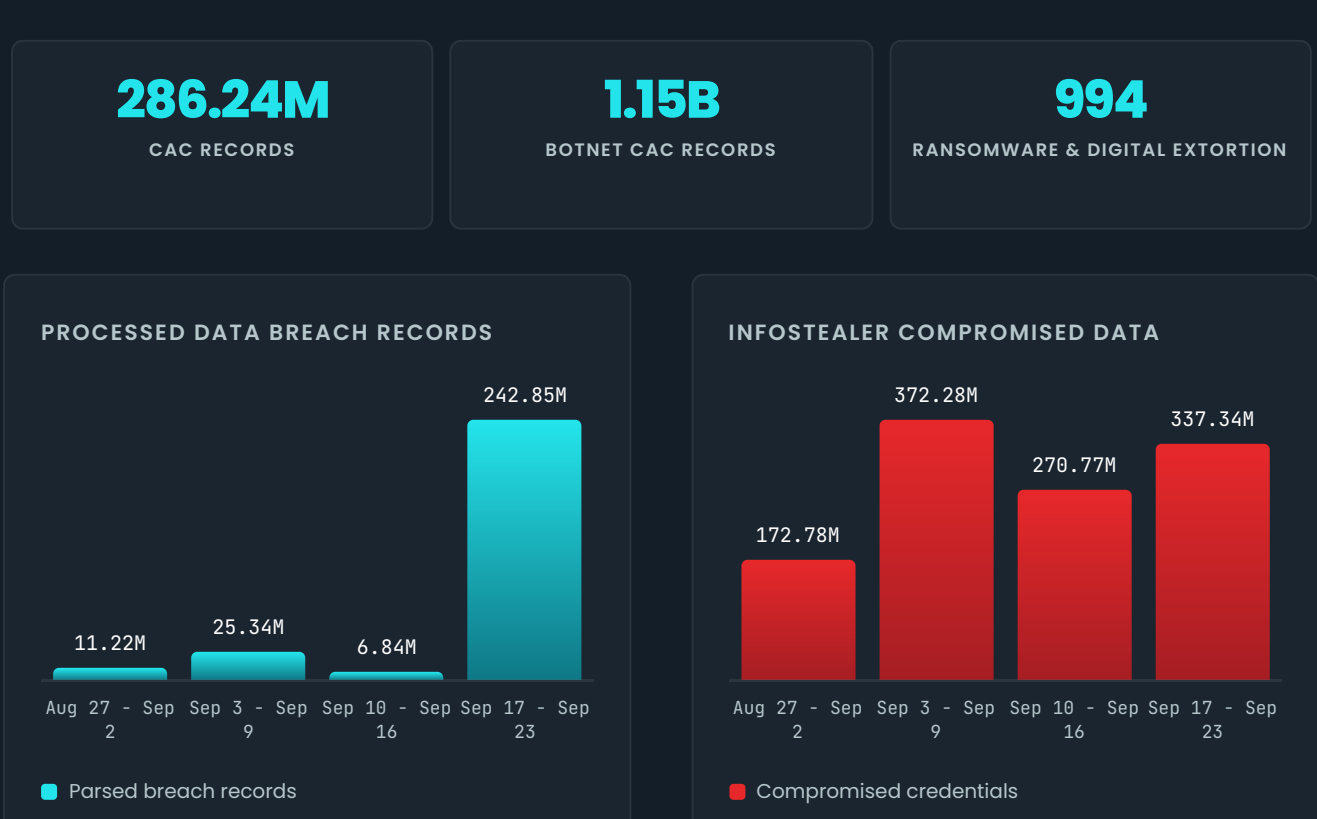
COLLECTED, PROCESSED DATA BREACHES

2 entries

VICTIM	SOURCE	THREAT ACTOR	PROCESSED RECORDS
century21[.]com	PwnForums	peluche911	19.44K
magairports[.]com	FulcrumSec	FulcrumSec	273.55M

PROCESSED DATA SET STATISTICS

Past 4 Weeks



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.