

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 30, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

5 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
ThreeAM Ransomware	Apexus
Storm Ransomware	Poca Valley Bank
CHAOS Ransomware	Carolina Asthma & Allergy Center
Play Ransomware	EverReady First Aid
Wallstreet Ransomware	Gibson Area Hospital and Health Services

VULNERABILITY DISCLOSURES

1 disclosure

CVE-2026-86950

Out-of-Bounds Write Vulnerability in Apple CoreGraphics

DEEP AND DARK WEB INTELLIGENCE

7 findings

CRITICAL FINDINGS

CRITICAL

Web Defacement of Appeal House and Coordinated Alleged DDoS Attacks Against Israeli Infrastructure

On September 29, 2026, pro-Iran threat actor group "GORZ ROSTAM" published a post in their Telegram channel, claiming responsibility for a web defacement and unauthorized access targeting Appeal House.

Source: Telegram **Actor:** GORZ ROSTAM

CRITICAL

Actor Claims DDoS Attack Targeting Google Design

On September 30, 2026, a pro-Palestinian threat actor group "313 Team" claimed, via its Telegram channel, to have carried out a Distributed Denial-of-Service (DDoS) attack against Google Design, an official editorial platform and digital publication by Google.

Source: Telegram **Actor:** 313 Team

HIGH

Surge in Activity with 26 New Victims Added

On September 30, 2026, ZeroFox observed that The Gentlemen ransomware group listed 26 new victims on their leak site.

Source: The Gentlemen Ransomware **Actor:** The Gentlemen

DATA BREACHES & LEAKS

HIGH

Data Allegedly Tied to Transfast Advertised

On September 29, 2026, untested threat actor "Marx1337" advertised data allegedly associated with Transfast on a predominantly Russian-language DDW forum XSS.

Source: XSS **Actor:** Marx1337

HIGH

Data Allegedly Associated with HUB24 Advertised

On September 29, 2026, moderately credible threat actor "bleedingout" advertised a database allegedly associated with HUB24 on a predominantly Russian-language DDW forum Exploit.

Source: Exploit **Actor:** bleedingout

HIGH

Data Allegedly Tied to Bangladesh Air Force Advertised

On September 29, 2026, untested threat actor "Cyb3R_Shubh4M" advertised a dataset allegedly associated with Bangladesh Air Force on Exploit.

Source: Exploit **Actor:** Cyb3R_Shubh4M

UNAUTHORIZED ACCESS CLAIMS

HIGH

PMS Access Allegedly Tied to Japan-Based Hotel Company Advertised

On September 29, 2026, untested threat actor "DDEEAALLEERR" advertised access to a property management system (PMS) of an unnamed Japan-based hotel company on Exploit.

Source: Exploit **Actor:** DDEEAALLEERR

COLLECTED, PROCESSED DATA BREACHES

2 entries

VICTIM	SOURCE	THREAT ACTOR	PROCESSED RECORDS
coingecko[.]com	Exploit	qlab	1.81M
bcac[.]hu	PwnForums	Sensitive2025	6.76K

PROCESSED DATA SET STATISTICS

Past 4 Weeks

380.11M

CAC RECORDS

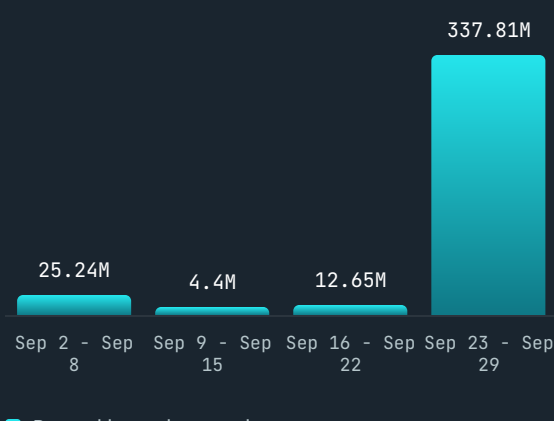
1.21B

BOTNET CAC RECORDS

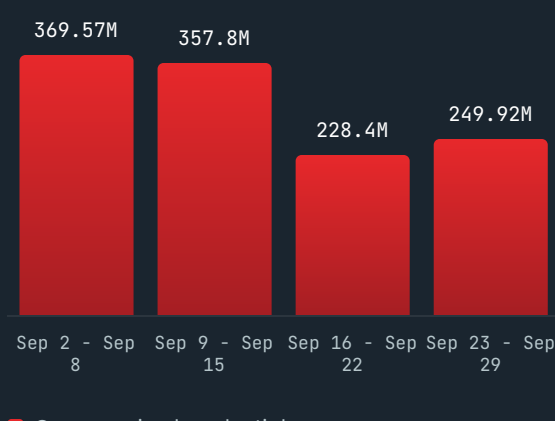
911

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 and TTPs, as well as significant operational spikes that deviate from the baseline threat landscape.