

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 16, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

5 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
Akira Ransomware	Southern California Telephone Company
ShadowByt3\$ Ransomware	HandyTrac
Dire Wolf Ransomware	Hazel Health
CHAOS Ransomware	Glasfloss Industries
SafePay Ransomware	Centro Hospitalario La Concepción

VULNERABILITY DISCLOSURES

4 disclosures

CVE-2026-87886

Local Privilege Escalation Vulnerability in Acronis Backup Plugin for cPanel and WHM and Plesk

CVE-2026-39364

Server File Restriction Bypass Vulnerability in Vite Development Server

CVE-2026-27540

Unrestricted File Upload Vulnerability in Rymera Web Co WooCommerce Wholesale Lead Capture

CVE-2026-76461

SQL Injection Vulnerability in Cisco AsyncOS Software for Cisco Secure Email Gateway

DEEP AND DARK WEB INTELLIGENCE

10 findings

CRITICAL FINDINGS

CRITICAL

32 New Victims Listed

On September 15, 2026, ZeroFox observed that The Gentlemen ransomware group listed 32 new victims on their leak site.

Source: The Gentlemen Ransomware

CRITICAL

Data Allegedly Associated with UAE-Based Company Oil & Gas International FZC Advertised

On September 11, 2026, moderately credible threat actor "HelluvaHack" advertised data allegedly associated with Oil & Gas International FZC, a UAE-based major supplier and solutions provider to the oil & gas industry on the predominantly Russian-language DDW forum Exploit.

Source: Exploit **Actor:** HelluvaHack

CRITICAL

Data Allegedly Associated with Castleton Commodities Japan Advertised

On September 15, 2026, moderately credible threat actor "zestix" advertised data associated with Castleton Commodities Japan on Exploit.

Source: Exploit **Actor:** zestix

CRITICAL

Actor Issues Warning Targeting U.S. Water Facilities

On September 11, 2026, a threat actor "Golden Falcon" claimed, via its Telegram channel, to have issued a warning against the United States, stating that its water facilities are under the group's supervision and monitoring.

Source: Telegram **Actor:** Golden Falcon

HIGH

Actor Claims DDoS Attack Targeting General Directorate of Civil Defense

On September 16, 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 General Directorate of Civil Defense, Saudi Arabia.

Source: Telegram **Actor:** 313 Team

HIGH

Dark Project RaaS Affiliate Program Advertised

On September 9, 2026, untested threat actor "dark_project" advertised a Ransomware-as-a-Service (RaaS) affiliate program called "Dark Project" on the predominantly Russian-language DDW forum DUTY-FREE.

Source: DUTY-FREE **Actor:** dark_project

VULNERABILITY EXPLOITATION

CRITICAL

Alleged iOS Exploit Kits and Attack Chains Advertised

On September 13 and 14, 2026, untested threat actor "lucy" advertised several exploit kits and attack chains allegedly tied to iOS on the predominantly English-language DDW forum DarkForums.

Source: DarkForums **Actor:** lucy

CRITICAL

Alleged One-Day RCE Exploit Targeting Fortinet Advertised

On September 16, 2026, moderately credible threat actor "Spaniard" advertised an alleged one-day exploit targeting Fortinet FortiWeb instances on the predominantly English-language DDW forum PwnForums.

Source: PwnForums **Actor:** Spaniard

UNAUTHORIZED ACCESS CLAIMS

HIGH

Network Access Allegedly Tied to Saudi Arabia-Based Engineering Company Advertised

On September 15, 2026, untested threat actor "HVNC-HVNC" advertised an auction for network access with domain user rights allegedly associated with an unnamed Saudi Arabia-based engineering company on Exploit.

Source: Exploit **Actor:** HVNC-HVNC

HIGH

Bot Access Allegedly Tied to U.S.-Based Systems Integrator Advertised

On September 14, 2026, moderately credible threat actor "Magic_Man" advertised an auction for malware bot access with domain user rights allegedly associated with an unnamed U.S.-based legal services company on Exploit.

Source: Exploit **Actor:** Magic_Man

COLLECTED, PROCESSED DATA BREACHES

1 entries

VICTIM	SOURCE	THREAT ACTOR	PROCESSED RECORDS
leroch-distribution[.]fr	PwnForums	ChimeraZ	1.44K

PROCESSED DATA SET STATISTICS

Past 4 Weeks

91.6M

CAC RECORDS

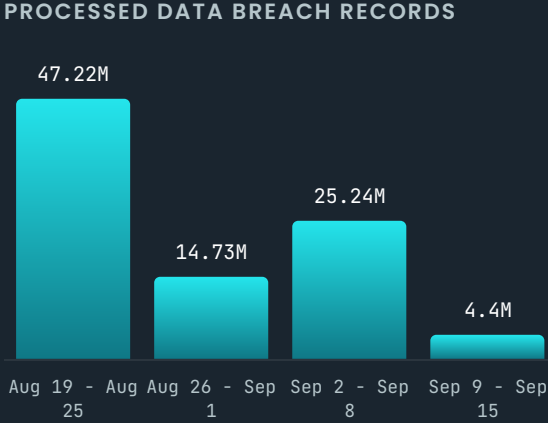
1.17B

BOTNET CAC RECORDS

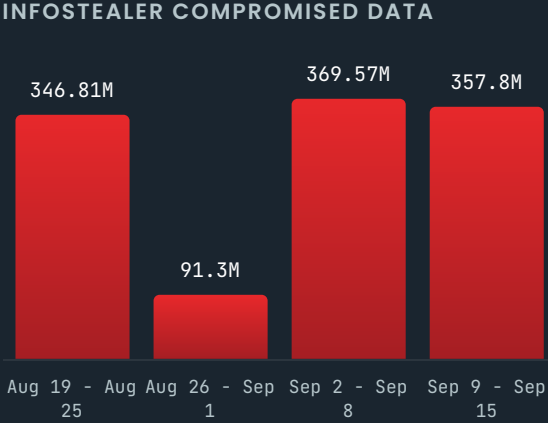
975

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.