

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 18, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

6 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
Brain Cipher Ransomware	AECOM
Brain Cipher Ransomware	Xpera
The Gentlemen Ransomware	Safeware
BlackNevas Ransomware	Optimum First Mortgage
Akira Ransomware	Practice Management
Storm Ransomware	First Secure State Banks

VULNERABILITY DISCLOSURES

1 disclosure

CVE-2026-76460

Authentication Bypass Vulnerability in Cisco Identity Services Engine

DEEP AND DARK WEB INTELLIGENCE

7 findings

CRITICAL FINDINGS

CRITICAL

Exploit: Alleged Google Mailer Plugin Advertised (Krause9)

On September 18, 2026, moderately credible threat actor "Krause9" advertised "GOOGLE MAILER Plugin" on the predominantly Russian-language DDW forum Exploit.

Source: Exploit **Actor:** Krause9

NEW LEAKSITES, MARKETPLACES, FORUMS

CRITICAL

Leak Site: New Data Leak Site Emerges (SPIRALS)

On September 18, 2026, ZeroFox observed a new data leak site operating under the name "SPIRALS."

Actor: SPIRALS

CRITICAL

Leak Site: New Data Leak Site Emerges (ENDZONE)

On September 18, 2026, ZeroFox observed a new data leak site operating under the name "ENDZONE."

Actor: ENDZONE

DATA BREACHES & LEAKS

CRITICAL

Exploit: Data Allegedly Associated with MT Global Advertised (Vespiary)

On September 17, 2026, moderately credible threat actor "Vespiary" advertised an alleged database belonging to MT Global, a UK-based company specializing in international money transfers, on Exploit.

Source: Exploit **Actor:** Vespiary

HIGH

Exploit: Alleged 3.1M+ Saudi Arabia PII Database Advertised (betway)

On September 18, 2026, well-regarded threat actor "betway" advertised a database containing more than 3.1 million records allegedly belonging to individuals in Saudi Arabia on Exploit.

Source: Exploit **Actor:** betway

UNAUTHORIZED ACCESS CLAIMS

HIGH

Exploit: Web Shell Access Allegedly Tied to Undisclosed U.S.-Based Company Advertised (grigory)

On September 17, 2026, untested threat actor "grigory" advertised web shell access allegedly associated with an undisclosed U.S.-based company on Exploit.

Source: Exploit **Actor:** grigory

HIGH

PwnForums: Network Access Allegedly Tied to 11 Distinct Companies Worldwide Advertised (stalled)

On September 16, 2026, untested threat actor "stalled" advertised network access allegedly associated with 11 unnamed distinct companies worldwide on the predominantly English-language DDW forum PwnForums.

Source: PwnForums **Actor:** stalled

COLLECTED, PROCESSED DATA BREACHES

4 entries

VICTIM	SOURCE	THREAT ACTOR	PROCESSED RECORDS
kemper[.]com	ShinyHunters	ShinyHunters	234.34K
treethink[.]kr	PwnForums	AshleyWood2022	5.47K
gazzettadasti[.]it	DarkForums	Sophia01	1.49K
wharton.upenn[.]edu	DarkForums	GhostLeakers	419

PROCESSED DATA SET STATISTICS

Past 4 Weeks

79.53M

CAC RECORDS

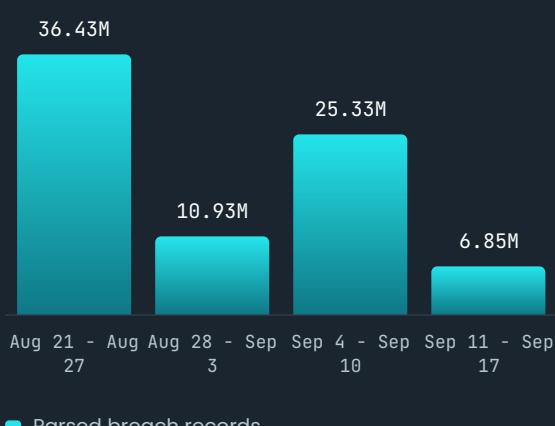
1.13B

BOTNET CAC RECORDS

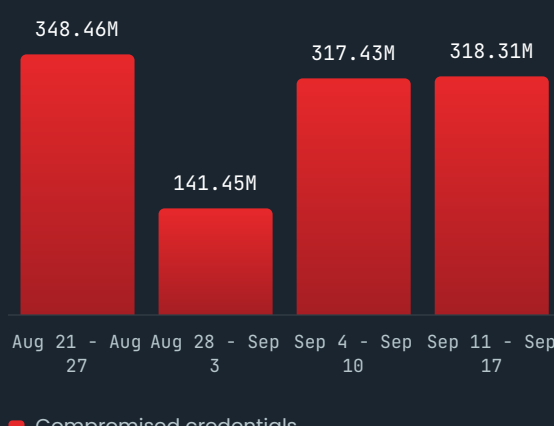
1.03K

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.