

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 17, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

4 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
The Gentlemen Ransomware	Hattiesburg Eye Clinic
The Gentlemen Ransomware	Peachtree Group
Qilin Ransomware	Resolve Law Group
Insomnia	Wiggins, Childs, Pantazis, Fisher & Goldfarb

VULNERABILITY DISCLOSURES

3 disclosures

CVE-2026-89026

Use of Hard-coded Cryptographic Key in Issabel Foundation Issabel Framework

CVE-2026-90894

Argument Injection and Local Privilege Escalation Vulnerability in Parallels Desktop for Mac

CVE-2026-58704

Elevation of Privilege Vulernability in Google Android Pixel Cellular Modem

DEEP AND DARK WEB INTELLIGENCE

5 findings

CRITICAL FINDINGS

CRITICAL

Exploit: Alleged Mastercard Gift Card Advertised (CallSpooF)

On September 17, 2026, untested threat actor "CallSpooF" advertised alleged Mastercard Gift cards on the predominantly Russian-language DDW forum Exploit.

CRITICAL

PwnForums: Data Allegedly Associated with TASPEN Advertised (10811118101)

On September 15, 2026, well-regarded threat actor "10811118101" advertised data allegedly associated with TASPEN on the predominantly English-language DDW forum PwnForums.

CRITICAL

DarkForums: Customer Order Database Allegedly Associated with Trezor and Shipmonk Advertised (HiddenHq)

On September 16, 2026, untested threat actor "HiddenHq" advertised a data set allegedly containing customer order and shipping records associated Trezor and ShipMonk on the predominantly English-language DDW forum DarkForums.

UNAUTHORIZED ACCESS CLAIMS

HIGH

Exploit: Network Access Allegedly Tied to U.S.-Based Freight & Logistics Services, Transportation Company Advertised (test_mobi)

On September 16, 2026, untested threat actor "test_mobi" advertised an auction for network access with local administrator rights allegedly associated with an unnamed U.S.-based freight & logistics services, transportation company on Exploit.

HIGH

Exploit/DarkForums: Web Shell Access Allegedly Tied to U.S.-Based Healthcare Services Company Advertised (grigory, buggsbunny)

On September 15, 2026, untested threat actor "grigory" advertised web shell access allegedly associated with an unnamed U.S.-based healthcare services company on Exploit.

PROCESSED DATA SET STATISTICS

Past 4 Weeks

94.35M

CAC RECORDS

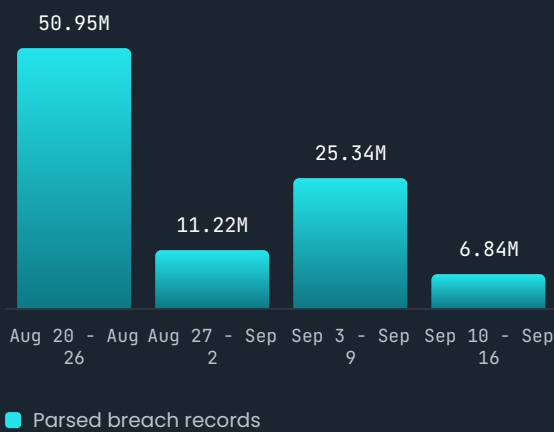
1.08B

BOTNET CAC RECORDS

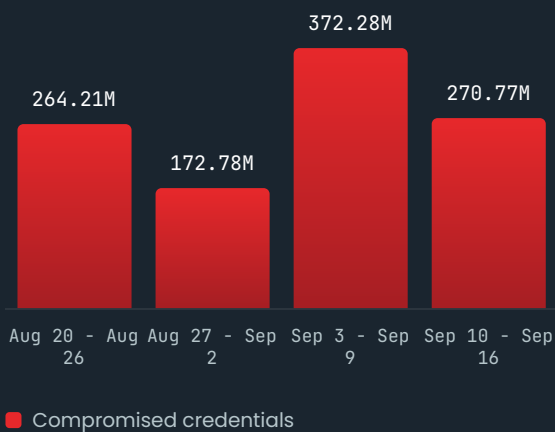
1.02K

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.