

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.

August 28, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

7 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
INC Ransomware	Benchmark Civil Engineering Services
INC Ransomware	Ruby Seven Studios
EMPERADOR Ransomware	Capitol Mechanics
EMPERADOR Ransomware	Reveal Data
KRYBIT Ransomware	Jindal Life Science
Anubis Ransomware	Caduceus Medical Group
Qilin Ransomware	Kling Automaten

VULNERABILITY DISCLOSURES

1 disclosure

CVE-2026-8452

Heap Buffer Overflow Vulnerability in Citrix NetScaler ADC and NetScaler Gateway

DEEP AND DARK WEB INTELLIGENCE

8 findings

CRITICAL FINDINGS

CRITICAL

New Data Leak Site Emerges

On August 28, 2026, ZeroFox observed a new data leak site operating under the name "Cinder."

Source: Leak Site Actor: Cinder

HIGH

Threat Actor Expresses Intent to Buy AWS Access Keys with Amazon Bedrock Permissions Targeting Claude Models

On August 26, 2026, well regarded threat actor "ShinyHunters" shared a post with an intent to buy AWS access keys (in AKIA:SECRET format) with Amazon Bedrock permissions on the predominantly English-language DDW forum PwnForums.

Source: PwnForums Actor: ShinyHunters

UNAUTHORIZED ACCESS CLAIMS

CRITICAL

Fortinet VPN Access Allegedly Tied to U.S.-Based Finance and Insurance Company Advertised

On August 27, 2026, moderately credible threat actor "molotov477" advertised an auction for Fortinet VPN access with user rights allegedly associated with an unnamed U.S.-based finance and insurance company on the predominantly Russian-language DDW forum Exploit.

Source: Exploit Actor: molotov477

HIGH

Network Access Allegedly Tied to France-Based Manufacturing Company Advertised

On August 26, 2026, untested threat actor "malary" advertised an auction for network access with administrator rights allegedly associated with an unnamed France-based manufacturing company on Exploit.

Source: Exploit Actor: malary

HACKTIVISM

HIGH

Actor Claims DDoS Attack Targeting Proton

On August 27, 2026, a pro-Palestinian threat actor group "313 Team" claimed to have conducted DDoS attack targeting Proton's internal servers.

Source: Telegram Actor: 313 Team

DATA BREACHES & LEAKS

HIGH

Data Allegedly Associated with Scale AI Advertised

On August 27, 2026, untested threat actor "Is1337" advertised an 8 GB dataset allegedly associated with Scale AI on Exploit.

Source: Exploit Actor: Is1337

HIGH

Data Allegedly Associated with Canada-Based Individuals Advertised

On August 27, 2026, moderately credible threat actor "Galahar" advertised data alle associated with Canada-based individuals on the predominantly Russian-language DDW forum XSS.

Source: XSS Actor: Galahar

VULNERABILITY EXPLOITATION

HIGH

Alleged RCE Exploit for CVE-2026-77554 Advertised

On August 27, 2026, untested threat actor "hglzvz" advertised an alleged one-day Remote Code Execution (RCE) exploit for CVE-2026-77554 on the predominantly English-language DDW forum BreachForums (breached[.].st).

Source: BreachForums Actor: hglzvz

COLLECTED, PROCESSED DATA BREACHES

3 entries

VICTIM	SOURCE	THREAT ACTOR	PROCESSED RECORDS
circleone.net[.]id	Pwnforums	metadata	22.73K
allroutetech[.]com	Pwnforums	yuki404	220
cosmundi[.]de	DarkForums	Sophia01	1.33K

PROCESSED DATA SET STATISTICS

Past 4 Weeks

1.21B

CAC RECORDS

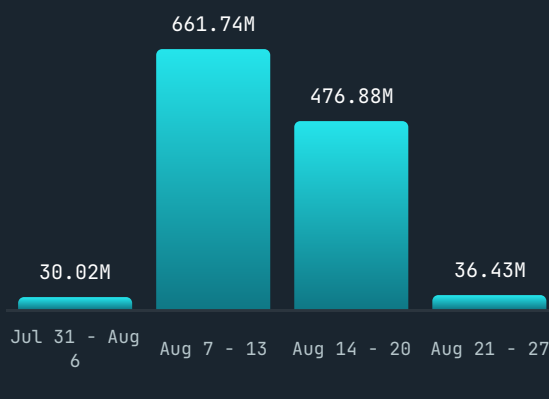
1.09B

BOTNET CAC RECORDS

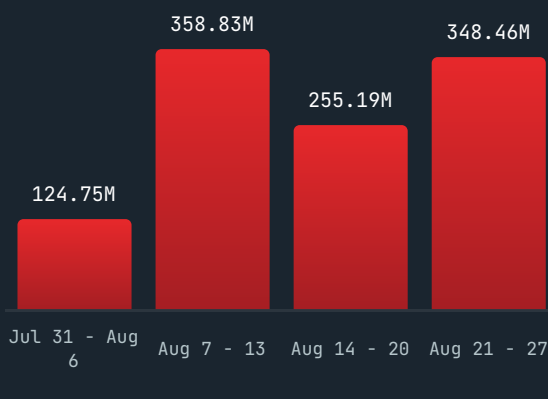
1.1K

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.