

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 4, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

6 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
CRPx0 Ransomware	Turkish Airlines
INC Ransomware	Quantinuum
KRYBIT Ransomware	ProHealth Medical Group
Qilin Ransomware	Freedom Claims Management
ShinyHunters	Lumenis
CRPx0 Ransomware	Johnson & Johnson

VULNERABILITY DISCLOSURES

1 disclosure

CVE-2026-18577

Authentication Bypass Vulnerability in N-able N-central

DEEP AND DARK WEB INTELLIGENCE

7 findings

CRITICAL FINDINGS

CRITICAL

Alleged U.S. and U.K. Proxy Lists from NetNut Leaked

On August 4, 2026, untested threat actor "kallm3j" leaked a list of proxies allegedly obtained from NetNut on the predominantly Russian-language deep and dark web (DDW) forum Exploit.

Source: Exploit Actor: kallm3j

CRITICAL

Data Allegedly Associated with U.S.-Based "leads stores" Advertised

On August 4, 2026, well-regarded threat actor "betway" published two posts on Exploit advertising data sets allegedly containing business leads of stores based in the United States.

Source: Exploit Actor: betway

UNAUTHORIZED ACCESS CLAIMS

HIGH

Network Access Allegedly Associated with Middle East-Based Hospital and Patient Portal Advertised

On August 1, 2026, untested threat actor "missiyaprizrak0" advertised network access allegedly associated with an unnamed Middle East-based hospital and patient portal on the predominantly English-language DDW forum PwnForums.

Source: PwnForums Actor: missiyaprizrak0

HIGH

RDWeb Access Allegedly Associated with Spain-Based Manufacturing Company Advertised

On August 2, 2026, well-known threat actor "Big-Bro" advertised an auction for RDWeb access with domain user rights allegedly tied to an unnamed Spain-based manufacturing company on Exploit.

Source: Exploit Actor: Big-Bro

HIGH

S3 Bucket Access Allegedly Associated with U.S.-Based Enterprise AI Platform Advertised

On July 31, 2026, well-regarded threat actor "stuffing" advertised an auction for S3 Bucket access allegedly associated with an unnamed U.S.-based enterprise artificial intelligence (AI) platform on Exploit.

Source: Exploit Actor: stuffing

HIGH

SSL VPN Access Allegedly Associated with Administrative Court of Thailand Advertised

On August 2, 2026, untested threat actor "spark" advertised SSL and VPN access allegedly associated with the Administrative Court of Thailand on the predominantly English-language DDW forum BreachForums (breached[.]su).

Source: BreachForums Actor: spark

VULNERABILITY EXPLOITATION

MEDIUM

Alleged RCE Exploit for CVE-2024-38077 Advertised

On August 2, 2026, untested threat actor "Slepoy_Gamer" advertised an alleged remote code execution (RCE) exploit for CVE-2024-38077 on the Exploit forum.

Source: Exploit Actor: Slepoy_Gamer

PROCESSED DATA SET STATISTICS

Past 4 Weeks

366.08M

CAC RECORDS

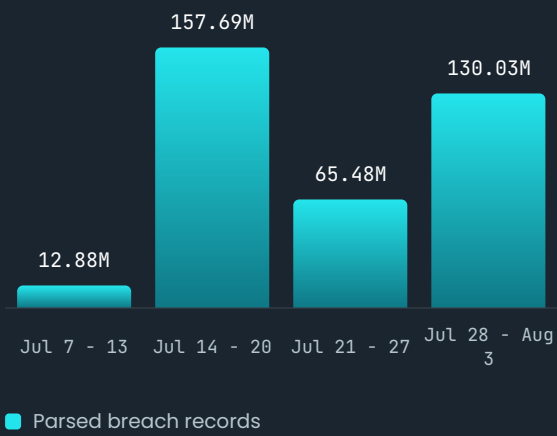
946.01M

BOTNET CAC RECORDS

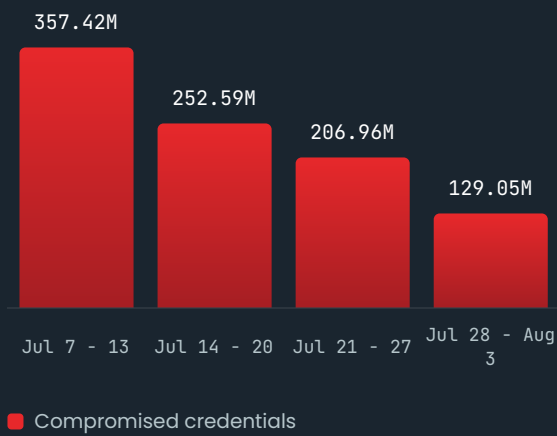
836

RANSOMWARE & DIGITAL EXTORTION

PROCESSED DATA BREACH RECORDS



INFOSTEALER COMPROMISED DATA



Threat Actor Profiles

A threat actor profile is a comprehensive overview of a malicious entity that outlines its motivations, capabilities, and observed attack patterns. These profiles typically include known aliases, targeted sectors, and documented tactics, techniques, and procedures (TTPs), and are used to characterize a wide range of groups operating across the cyber threat landscape, from highly sophisticated actors to those driven by financial or ideological motives.

Monthly Threat Spotlight

The Monthly Threat Spotlight highlights highly unusual threat actor behaviors, bizarre tactics, and significant spikes in specific ransomware or threat operations observed over a recent period. This intelligence focuses on the anomalies and notable shifts that stand out from the baseline threat landscape.