ZEROFOX

Deep and Dark Web Intelligence Reporting

Here is a curated list of critical incidents and compromised data observed in deep and dark web ransomware sites, forums, and marketplaces ingested into the ZeroFox Platform in the past 72 hours.

July 13, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

5 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
M3RX Ransomware	Eclective
Everest Ransomware	Rodschinson Investment
Anubis Ransomware	Community Advocates
Everest Ransomware	NIMR Oil
CRPx0 Ransomware	SF Smile Doctor

VULNERABILITY DISCLOSURES

2 disclosures

CVE-2026-20896

Authentication Bypass in Gitea Docker Image

CVE-2026-3844

Unauthenticated Arbitrary File Upload in Cloudways Breeze Cache (WordPress Plugin); Reported Exploitation Identified

DEEP AND DARK WEB INTELLIGENCE

3 findings

CRITICAL FINDINGS

CRITICAL **Alleged Data Associated with Mobilemed Adertised**

On July 10, 2026, a credible threat actor "Kazu" advertised data allegedly associated with Mobilemed, on a predominantly English-language deep and dark web forum PwnForums. Notably, the actor also shared the post on their data leak site (DLS).

Source: LeakSite/PwnForums **Actor:** Kazu

HACKTIVISM

HIGH **Alleged DDoS Attack on New York City Police Department Website**

On July 12, 2026, pro-Palestinian hacktivist group Dark Storm Team announced via its official Telegram channel that it had conducted a distributed denial-of-service (DDoS) attack against the "nypdonline.org" web endpoint. This url is the official transparency and public accountability portal of the New York City Police Department (NYPD).

Source: Telegram **Actor:** Dark Storm Team

NEW LEAKSITES, MARKETPLACES, FORUMS

HIGH **New Data Leak Site Emerges**

On July 13, 2026, ZeroFox observed a new data leak site called "D1R." As of this report, the leak site lists three victims and is accessible via the following dark web address: hXXp://dirone3rl3vvq64ckcnrvhe2ogrhjrwu5u7hqzrlotu3rfvmqmmbsuqd[.]onion/

Source: Leak Site **Actor:** D1R

COLLECTED, PROCESSED DATA BREACHES

4 entries

VICTIM	SOURCE	THREAT ACTOR	PROCESSED RECORDS
100K LINES - GERMANY MAILPASS 2026	Cracked	UniqueCombo	106.1K
replicawatchessales (replicawatchessales[.]com)	DarkForums	Sophia01	140.3K
Soundbanks (soundbanks[.]io)	DarkForums	Sophia01	6.2K
879K Social Network Target Mailpass #397	XSS	STRADU_DB	879.1K

PROCESSED DATASET STATISTICS

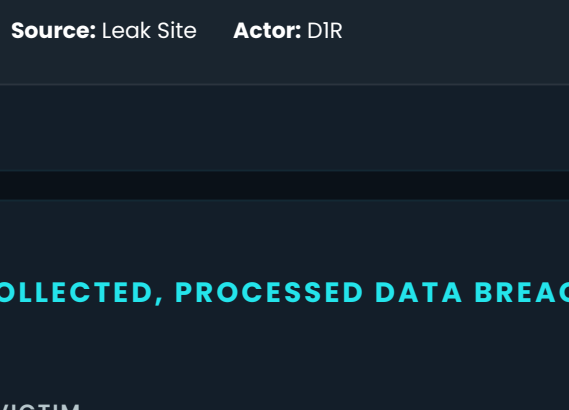
Past 4 Weeks

647.1M CAC RECORDS

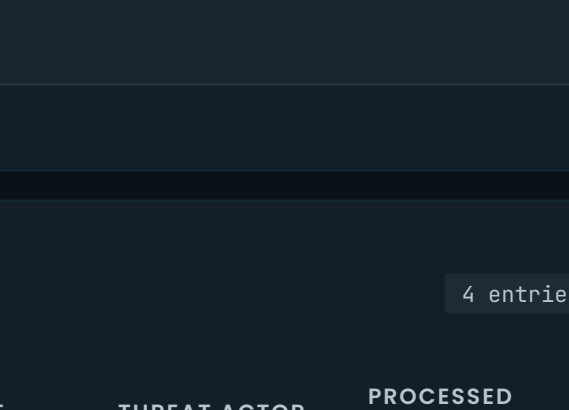
1.1B BOTNET CAC RECORDS

732 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, bizarre tactics, and significant operational spikes that deviate from the baseline threat landscape.