# 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 72 hours.

July 20, 2026

## RANSOMWARE / DIGITAL EXTORTION VICTIMS

5 incidents

| THREAT ACTOR / GROUP | VICTIM ORGANIZATION |
|---|---|
| INTERLOCK Ransomware | District of Columbia Housing Authority |
| BlackNevas Ransomware | L'azurde |
| INC Ransomware | State Bank of Nauvoo |
| UnSafe | CCR Solutions |
| The Gentlemen Ransomware | Gallant |

## VULNERABILITY DISCLOSURES

3 disclosures

CVE-2026-60137
SQL Injection in WordPress WP_Query

CVE-2026-63030
Unauthenticated Remote Code Execution in WordPress Core

CVE-2026-14266
Heap-Based Buffer Overflow in 7-Zip

## DEEP AND DARK WEB INTELLIGENCE

3 findings

### CRITICAL FINDINGS

CRITICAL **Data Allegedly Associated with Al-Nahrain Islamic Bank Leaked**

On July 19, 2026, untested threat actor "Erresira" leaked data allegedly associated with Iraq-based Al-Nahrain Islamic Bank on the predominantly English-language dark web forum DarkForums.

**Source:** DarkForums **Actor:** Erresira

CRITICAL **Data Allegedly Associated with Uber Eats Advertised**

On July 17, 2026, untested threat actor "sheperd_craven" advertised data allegedly associated with Uber Eats on DarkForums.

**Source:** DarkForums **Actor:** sheperd_craven

CRITICAL **Alleged Australian PII and Financial Documents Advertised**

On July 19, 2026, untested threat actor "einein786" advertised a data set allegedly containing Australian PII and financial documents on the predominantly Russian-language deep and dark web forum Exploit.

**Source:** Exploit **Actor:** einein786

## PROCESSED DATASET STATISTICS

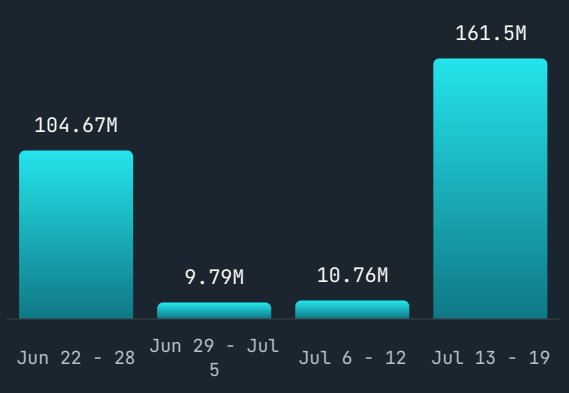
Past 4 Weeks

**286.72M**
CAC RECORDS

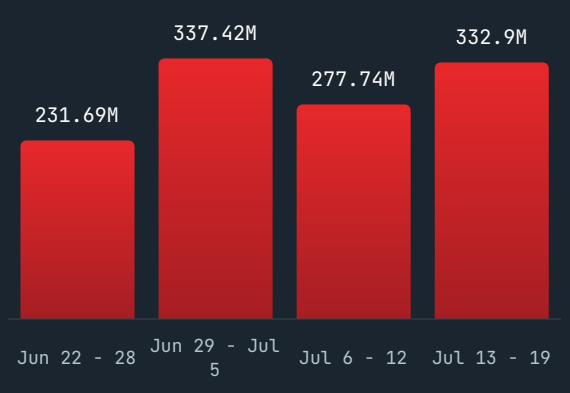
**1.17B**
BOTNET CAC RECORDS

**731**
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.