ZEROFOX

# 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 20, 2026

## RANSOMWARE / DIGITAL EXTORTION VICTIMS

5 incidents

| THREAT ACTOR / GROUP | VICTIM ORGANIZATION |
|---|---|
| xpl0itrs | Target |
| Everest Ransomware | Kingston Technology |
| Everest Ransomware | Capgemini |
| LeakedData | Troutman Pepper Locke |
| Akira Ransomware | Borchert & LaSpina |

## VULNERABILITY DISCLOSURES

1 disclosure

CVE-2026-33824

Double Free Remote Code Execution Vulnerability in Microsoft Windows IKE Extension

## DEEP AND DARK WEB INTELLIGENCE

9 findings

### CRITICAL FINDINGS

CRITICAL **New RaaS Affiliate Program Dubbed 'Moondancer Ransomware' Advertised**

On August 19, 2026, untested threat actor "Straightonumberone" advertised a new Ransomware-as-a-Service (RaaS) affiliate program dubbed "Moondancer Ransomware" on the predominantly English-language DDW forums DarkForums.

**Source:** DarkForums **Actor:** Straightonumberone

CRITICAL **Data Allegedly Associated with Avona Health Institute Advertised**

On August 18, 2026, moderately credible threat actor "2019" leaked data allegedly associated with Anova Health Institute, a South Africa-based public health organization on the predominantly English-language DDW forums PwnForums.

**Source:** PwnForums **Actor:** 2019

CRITICAL **Data Allegedly Associated with Alaxione Advertised**

On August 19, 2026, well-regarded threat actor "Angel_Batista" advertised data allegedly associated with Alaxione on PwnForums.

**Source:** PwnForums **Actor:** Angel_Batista

### UNAUTHORIZED ACCESS CLAIMS

HIGH **FortiGate Access Allegedly Tied to Hong Kong-Based Company OP Mall Advertised**

On August 18, 2026, untested threat actor "morganfreeman666" advertised an auction for FortiGate access allegedly associated with the Hong Kong-based company OP Mall on the predominantly Russian-language DDW forum Exploit.

**Source:** Exploit **Actor:** morganfreeman666

CRITICAL **Network Access Allegedly Tied to UK-Based Telecommunications Company Advertised**

On August 18, 2026, moderately credible threat actor "Florence" advertised to sell network access allegedly associated with an unnamed UK-based telecommunications company on PwnForums.

**Source:** PwnForums **Actor:** Florence

HIGH **Network Access Allegedly Tied to Malaysia-Based Investment Holdings Company Advertised**

On August 18, 2026, moderately credible threat actor "Florence" advertised to sell network access allegedly associated with an unnamed Malaysia-based investment holdings company on PwnForums.

**Source:** PwnForums **Actor:** Florence

### DATA BREACHES & LEAKS

HIGH **Data Allegedly Associated with Tribunal Supremo de Elecciones Leaked**

On August 18, 2026, moderately credible threat actor "GordonFreeman," leaked a database allegedly associated with the Tribunal Supremo de Elecciones (TSE), a Costa Rica-based Electoral Tribunal on DarkForums.

**Source:** DarkForums **Actor:** GordonFreeman

HIGH **Data Allegedly Associated with Ministère de l'Éducation Nationale Advertised**

On August 17, 2026, moderately credible threat actor "ZeroBytes" advertised data allegedly associated with Ministère de l'Éducation Nationale (The French Ministry of National Education) on PwnForums.

**Source:** PwnForums **Actor:** ZeroBytes

HIGH **Account Access and Data Allegedly Associated with Secretaría de Hacienda y Crédito Público Leaked**

On August 20, 2026, untested threat actor "Keishell" leaked account credentials allegedly associated with Secretaría de Hacienda y Crédito Público (Ministry of Finance and Public Credit), Mexico on DarkForums.

**Source:** DarkForums **Actor:** Keishell

## COLLECTED, PROCESSED DATA BREACHES

4 entries

| VICTIM | SOURCE | THREAT ACTOR | PROCESSED RECORDS |
|---|---|---|---|
| sora2u[.]com | PwnForums | 888 | 7.33K |
| spytec[.]com | PwnForums | Erich | 131.58K |
| bnine[.]com | PwnForums | riche | 36.57K |
| 91mobiles[.]com | PwnForums | DataDaddy666 | 109.64K |

## PROCESSED DATA SET STATISTICS

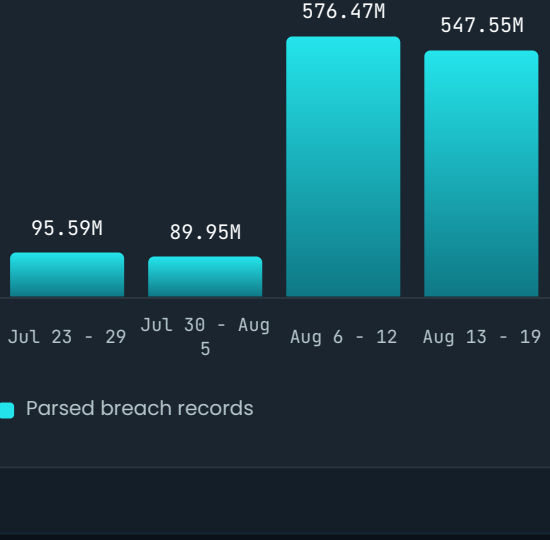
Past 4 Weeks

**1.31B** CAC RECORDS

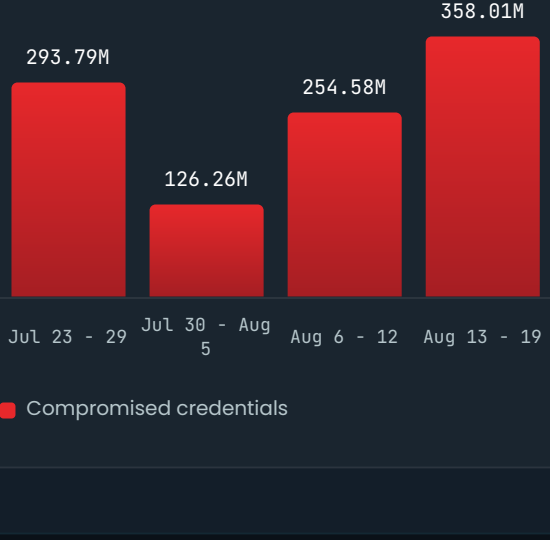
**1.03B** BOTNET CAC RECORDS

**1.03K** 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.