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 72 hours.

September 7, 2026

## RANSOMWARE / DIGITAL EXTORTION VICTIMS

7 incidents

| THREAT ACTOR / GROUP | VICTIM ORGANIZATION |
|---|---|
| ShinyHunters | Medela |
| Space Bears Ransomware | Sports Endeavors |
| PEAR Ransomware | Kovo+ Holdings |
| Wallstreet Ransomware | City of Ormond Beach |
| DragonForce Ransomware | Norwood Law Firm |
| Panzer Ransomware | Diskominfo Jawa Tengah |
| Karma Ransomware | Schwartz Giannini Lantsberger & Adamson |

## VULNERABILITY DISCLOSURES

3 disclosures

CVE-2026-85046
Type Confusion Vulnerability in Google Chrome V8

CVE-2026-81578
Improper Access Control Vulnerability in PaperCut NG/MF

CVE-2026-82078
Unsafe Dynamic Class Loading Vulnerability in PaperCut NG/MF

## DEEP AND DARK WEB INTELLIGENCE

6 findings

### CRITICAL FINDINGS

CRITICAL **New Data Leak Site Emerges**

On September 7, 2026, ZeroFox observed a new data leak site operating under the name "BLACKLOCKS."

**Source:** Leak Site **Actor:** BLACKLOCKS

CRITICAL **SMS Gateway Access Allegedly Associated with HSBC Bank Advertised**

On September 7, 2026, untested threat actor “Marx” advertised an alleged real-time SMS traffic monitoring and gateway monitoring solution associated with HSBC Bank on the predominantly English-language DDW forum DarkForums.

**Source:** DarkForums **Actor:** Marx

CRITICAL **Super Administrator Support Portal Access Allegedly Associated with Bitbuy Advertised**

On September 6, 2026, untested threat actor "darkqueenXx" advertised alleged super administrator access to a support portal purportedly associated with Bitbuy, a Canada-based cryptocurrency company, on the predominantly English-language DDW forum Spear.

**Source:** Spear **Actor:** darkqueenXx

### UNAUTHORIZED ACCESS CLAIMS

HIGH **Network Access Allegedly Tied to U.S.-Based Healthcare Services Company Advertised**

On September 4, 2026, well-regarded threat actor "888" advertised network access allegedly associated with an unnamed U.S.-based healthcare services company on the predominantly English-language DDW forum PwnForums.

**Source:** PwnForums **Actor:** 888

HIGH **Network Access Allegedly Tied to Undisclosed Ministry in Central America Advertised**

On September 4, 2026, untested threat actor "WebLoad" advertised VPN access with domain user rights allegedly associated with an undisclosed Ministry of one of top countries in Central America, on the predominantly Russian-language DDW forum DUTY-FREE.

**Source:** DUTY-FREE **Actor:** WebLoad

HIGH **AnyDesk Access Allegedly Tied to Iran-Based Construction Company Advertised**

On September 3, 2026, well-known threat actor "Big-Bro" advertised an auction for AnyDesk access with domain administrator rights allegedly associated with an unnamed Iran-based construction company on the predominantly Russian-language DDW Exploit.

**Source:** Exploit **Actor:** Big-Bro

## COLLECTED, PROCESSED DATA BREACHES

2 entries

| VICTIM | SOURCE | THREAT ACTOR | PROCESSED RECORDS |
|---|---|---|---|
| coincustody[.]io | Exploit | whale_leads42 | 107 |
| earnipay[.]com | Exploit | late | 16.71K |

## PROCESSED DATA SET STATISTICS

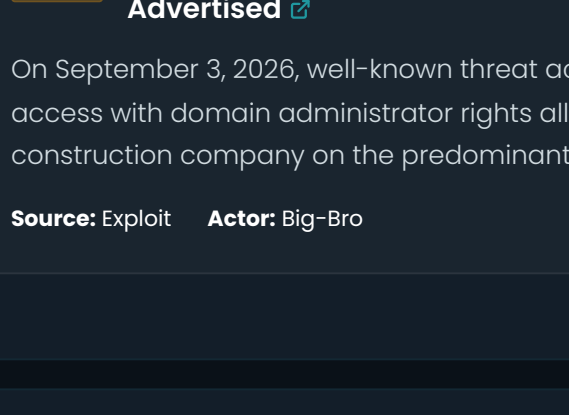
Past 4 Weeks

**875.07M** CAC RECORDS

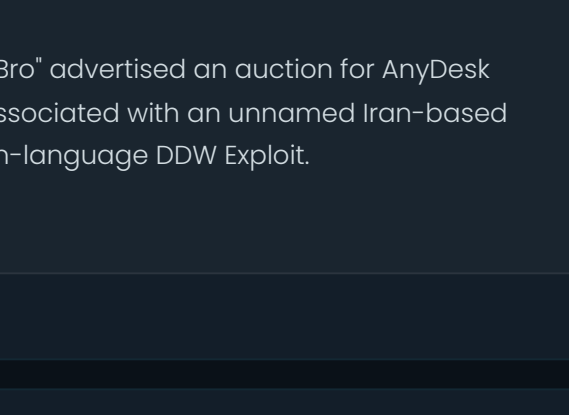
**1.04B** BOTNET CAC RECORDS

**996** 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.