

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.

October 5, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

7 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
Booba Project Ransomware	Lakewood Medical Centre
ShinyHunters	Dexcom
ShinyHunters	O'Reilly Auto Parts
Akira Ransomware	Pacific Tank Lines
DeadLock Ransomware	Far West Contractors
DeadLock Ransomware	Union Financial Associates
Rhysida Ransomware	Law Office of David Williams

VULNERABILITY DISCLOSURES

3 disclosures

CVE-2026-88779

Memory Overflow Vulnerability in Citrix NetScaler ADC and NetScaler Gateway

CVE-2026-104286

Unauthenticated Path Traversal and Arbitrary File Write Vulnerability in Fortinet FortiMail

CVE-2026-90970

Server-Side Template Injection Vulnerability in GitLab AI Gateway

DEEP AND DARK WEB INTELLIGENCE

11 findings

VULNERABILITY EXPLOITATION

CRITICAL

Alleged OEM-Signed Windows Kernel Driver Vulnerability Advertised (Donrulezz)

On October 4, 2026, well-reputed threat actor "Donrulezz" advertised a zero-day vulnerability in an OEM-signed Windows kernel-mode driver (WDF/KMDF) on a predominantly Russian-language DDW forum Exploit.

Source: Exploit Actor: donrulezz

CRITICAL

Windows Kernel Local Privilege Escalation Zero-Day Exploit Advertised (zeroplayer)

On October 4, 2026, well-reputed threat actor "zeroplayer" advertised a Windows kernel LPE zero-day on Exploit.

Source: Exploit Actor: zeroplayer

CRITICAL

Windows Local Privilege Escalation Zero-Day in Remote Administration Software Advertised (RayBan3000)

On October 3, 2026, well-reputed threat actor "RayBan3000" advertised a zero-day vulnerability targeting commercial remote computer management and administration software on Exploit.

Source: Exploit Actor: rayban3000

DATA BREACHES & LEAKS

HIGH

Data Allegedly Associated with Ministry of Foreign Affairs of Ukraine Leaked (404Crew Cyber Team)

On October 3, 2026, untested threat actor "404Crew Cyber Team" leaked data allegedly associated with the МІНІСТЕРСТВО ЗАКОРДОННИХ СПРАВ УКРАЇНИ (Ministry of Foreign Affairs of Ukraine) on a predominantly English-language deep and dark web forum BreachForums (breached[.]st).

Source: BreachForums Actor: 404Crew Cyber Team

HIGH

Data Allegedly Associated with Elbaite Advertised (KimOCW)

On October 2, 2026, untested threat actor "KimOCW" advertised a data set allegedly associated with Elbaite, an Australia-based cryptocurrency exchange platform on Exploit.

Source: Exploit Actor: kimocw

HIGH

Data Allegedly Associated with Jettly Advertised (hubert)

On October 2, 2026, moderately credible threat actor "hubert" advertised a data set allegedly associated with Jettly, a Canada-based private aviation marketplace and charter platform on Exploit.

Source: Exploit Actor: hubert

HIGH

Data Allegedly Tied to Finfrog Advertised (kfshd)

On October 2, 2026, untested threat actor "kfshd" advertised a data set allegedly associated with the France-based fintech company Finfrag (finfrag[.]fr) on Exploit.

Source: Exploit

HIGH

Data Allegedly Associated with Royal Belgian Football Association Advertised (RedStone)

On October 2, 2026, untested threat actor "RedStone" advertised a database allegedly associated with Royal Belgian Football Association (RBFA) on a predominantly English-language DDW forum PwnForums.

Source: Pwnforums Actor: redstone

UNAUTHORIZED ACCESS CLAIMS

HIGH

Alleged Administrative Access to Indonesian Healthcare Portal Advertised (Keishell)

On October 2, 2026, untested threat actor "Keishell" advertised administrative access allegedly associated with a healthcare center portal in West Java, Indonesia, on a predominantly English-language DDW forum DarkForums.

Source: Darkforums Actor: keishell

HIGH

Citrix Access Allegedly Tied to U.S.-Based Transportation Company Advertised (Big-Bro)

On October 2, 2026, well-known threat actor "Big-Bro" advertised an auction for Citrix access with domain user rights allegedly associated with an unnamed U.S.-based transportation company on Exploit.

Source: Exploit Actor: big-bro

HIGH

VPN Access Allegedly Tied to Eurofarma Group Company Advertised (khosi)

On September 30, 2026, untested threat actor "khosi" advertised VPN access allegedly associated with the Eurofarma Group company on PwnForums.

Source: Pwnforums Actor: khosi

COLLECTED, PROCESSED DATA BREACHES

1 entries

VICTIM	SOURCE	THREAT ACTOR	PROCESSED RECORDS
picup[.]com	PwnForums	jail	14.66K

PROCESSED DATA SET STATISTICS

Past 4 Weeks

438.42M

CAC RECORDS

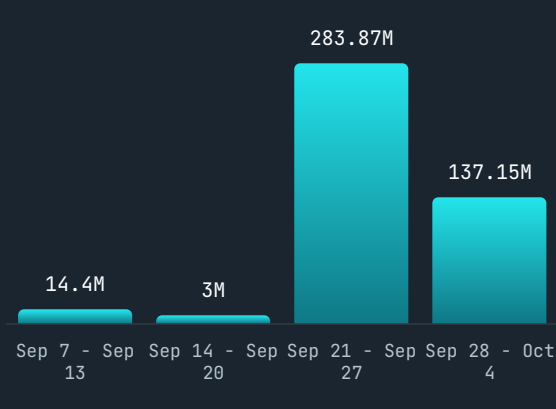
1.19B

BOTNET CAC RECORDS

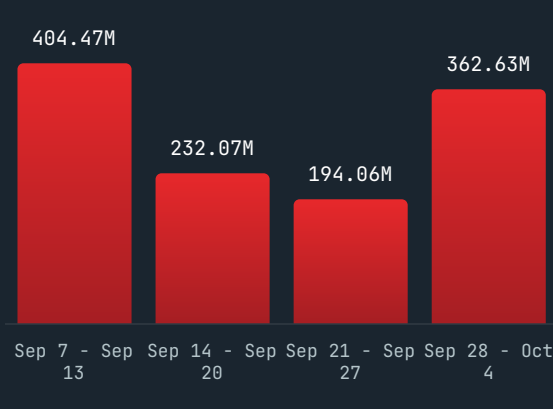
842

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.