

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.

October 6, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

7 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
Insomnia	Praxis EMR
Aur0ra Ransomware	Retriever Danmark
INTERLOCK Ransomware	O2 Dental Group
LeakedData	Nelson Mullins Riley & Scarborough
ENDZONE	Philander Smith University
NightSpire Ransomware	Forma Therapeutics
SETTRA Ransomware	Translarity

VULNERABILITY DISCLOSURES

2 disclosures

CVE-2026-86360

Path Traversal Vulnerability in Dell System Update (DSU)

CVE-2026-21589

Arbitrary File Access Vulnerability in Atlassian Data Center and Server Products

DEEP AND DARK WEB INTELLIGENCE

10 findings

DATA BREACHES & LEAKS

CRITICAL

Data Allegedly Associated with HSBC Bank Advertised (Marx)

On October 5, 2026, moderately credible threat actor “Marx” advertised data allegedly associated with HSBC Bank on the predominantly English-language DDW forum DarkForums.

Source: Darkforums Actor: marx

HIGH

Data Allegedly Associated with Lopay Advertised (DaOnlySpark)

On September 5, 2026, well-reputed threat actor “DaOnlySpark” advertised data allegedly associated with Lopay on a predominantly English-language DDW forum PwnForums.

Source: Pwnforums Actor: daonlyspark

HIGH

Access and Data Allegedly Tied to UK-Based Health Booking Portal Company Advertised (DDEEAALLEERR)

On October 4, 2026, untested threat actor “DDEEAALLEERR” advertised access and a data dump from a UK-based health booking portal on a predominantly Russian-language DDW forum Exploit.

Source: Exploit Actor: ddeeaalleerr

HIGH

Data Allegedly Tied to Marcas Latam Advertised (renn)

On October 4, 2026, moderately credible threat actor “renn” advertised a data set allegedly associated with Marcas Latam, a U.S.-based online marketplace for Latin American fashion designers and brands, on Exploit.

Source: Exploit Actor: renn

HIGH

Data Allegedly Tied to KOHO Advertised (bleedingout)

On October 4, 2026, moderately credible threat actor “bleedingout” advertised data set allegedly associated with KOHO, a Canada-based fintech company providing digital banking, prepaid cards, savings, and credit-building services on Exploit.

Source: Exploit Actor: bleedingout

UNAUTHORIZED ACCESS CLAIMS

CRITICAL

SSH Access Allegedly Tied to Undisclosed Bank Advertised (williamblack)

On October 3, 2026, untested threat actor “williamblack” advertised SSH access allegedly associated with an undisclosed bank on Exploit.

Source: Exploit Actor: williamblack

CRITICAL

Network Access Allegedly Tied to U.S.-Based Hospital Advertised (bianlianbo)

On October 4, 2026, untested threat actor “bianlianbo” advertised network access allegedly associated with an unnamed U.S.-based hospital on PwnForums.

Source: Pwnforums Actor: bianlianbo

HIGH

Alleged Fortinet SSL VPN Access Credentials Advertised (rootkaliwhoami)

On October 4, 2026, untested threat actor “rootkaliwhoami” posted a list of Fortinet SSL VPN access credentials on a predominantly English-language DDW forum BreachForums (breached[.]st).

Source: Breachforums Actor: rootkaliwhoami

VULNERABILITY EXPLOITATION

HIGH

AI-Powered Agent for Malware Developing and Penetration Testing Advertised (NexusCode)

On October 4, 2026, untested threat actor “NexusCode” advertised an AI-powered agent for malware developing and penetration testing on Exploit.

Source: Exploit Actor: nexuscode

HIGH

One-Day Exploit for Undisclosed Open-Source Web Technology Advertised (CodeStudio)

On October 4, 2026, well-reputed threat actor “CodeStudio” advertised a one-day exploit for a popular open-source web technology on Exploit.

Source: Exploit Actor: codestudio

PROCESSED DATA SET STATISTICS

Past 4 Weeks

438.41M

CAC RECORDS

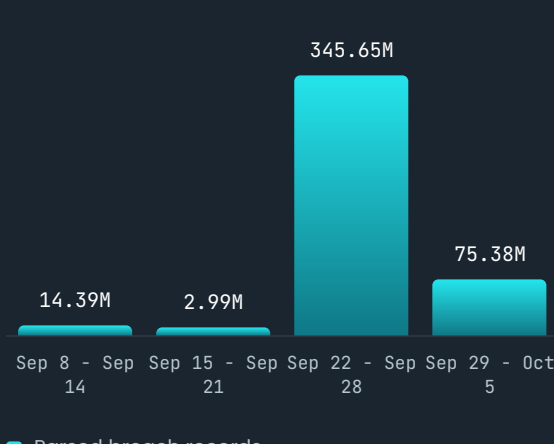
1.06B

BOTNET CAC RECORDS

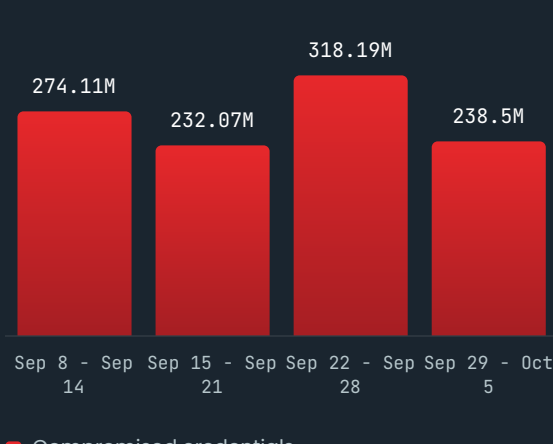
899

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.