

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 7, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

7 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
Termite Ransomware	Aon
Akira Ransomware	Michael K. Shelby, CPA
SafePay Ransomware	DÚHA
Safepay Ransomware	HAL Service
Safepay Ransomware	ANWO
Everest	flydubai
Qilin Ransomware	J&D Financial

VULNERABILITY DISCLOSURES

3 disclosures

CVE-2026-94504

Stored Cross-Site Scripting Vulnerability in Ninja Forms WordPress Plugin

CVE-2026-63277

Inclusion of Functionality from Untrusted Control Sphere Vulnerability in The Document Foundation LibreOffice

CVE-2026-93836

Unauthenticated Stored Cross-Site Scripting Vulnerability in wpclever WPC Product Bundles for WooCommerce

DEEP AND DARK WEB INTELLIGENCE

9 findings

CRITICAL FINDINGS

CRITICAL

Alleged Customer Data Exfiltration and Snowflake Compromise Claimed Against ASOS

On October 6, 2026, a threat group, "Xuanye Group," claimed via its Telegram channel responsibility for an incident involving ASOS, a UK-based online fast-fashion and cosmetic retailer, asserting they had exfiltrated customer information

Source: Telegram Actor: xuanye group

HIGH

Alleged Multi-Day Internet Outage and Data Exposure Claimed Against Momentum Telecom

On October 7, 2026, ZeroFox observed an update on the ENDZONE leak site claiming responsibility for an alleged multi-day internet outages in Eagle Mountain, Utah.

Source: Leak site Actor: endzone

NEW LEAKSITES, MARKETPLACES, FORUMS

HIGH

New Data Leak Site Emerges

On October 6, 2026, ZeroFox observed a new data leak site named "VYPR."

Source: Leak Site Actor: VYPR

HIGH

New Leak Site Emerges

On October 7, 2026, ZeroFox observed a new leak site named "UMBRA".

Source: Leak Site Actor: umbra

DATA BREACHES & LEAKS

HIGH

Data Allegedly Tied to Personal Banking Services Advertised

On October 6, 2026, an untested threat actor "admin777" advertised a data set allegedly associated with personal banking services on the predominantly Russian-language dark web forum RehubCom

Source: Rehubcom Actor: admin777

HIGH

Data Allegedly Tied to U.S.-Based Accountants Advertised

On October 5, 2026, an untested threat actor, operating under the alias, "FBI" advertised a data set allegedly associated with U.S.-based accountants on the predominantly Russian-language DDW forum Exploit.

Source: Exploit

HIGH

Data Allegedly Tied to Thrive Online Group Advertised (Vespiary)

On October 5, 2026, a moderately reputed threat actor "Vespiary" advertised a data set allegedly associated with the South Africa-based digital marketing company Thrive Online Group on Exploit.

Source: Exploit Actor: vespiary

UNAUTHORIZED ACCESS CLAIMS

HIGH

Citrix Access Allegedly Tied to U.S.-Based Construction Company Advertised

On October 6, 2026, an untested threat actor "vitorwil" advertised an auction for Citrix access with domain user rights allegedly tied to an unnamed U.S.-based construction company on Exploit.

Source: Exploit Actor: vitorwil

HIGH

Fortinet Access Allegedly Tied to Netherlands-Based Waste Management Company Advertised (coco3r3sh)

On October 5, 2026, an untested threat actor "nineteen" advertised a data set allegedly associated with the Germany-based retail company Notino on Exploit.

Source: Exploit Actor: coco3r3sh

COLLECTED, PROCESSED DATA BREACHES

1 entries

VICTIM	SOURCE	THREAT ACTOR	PROCESSED RECORDS
moody[.]edu	ShinyHunters	ShinyHunters	2.31M

PROCESSED DATA SET STATISTICS

Past 4 Weeks

437.2M

CAC RECORDS

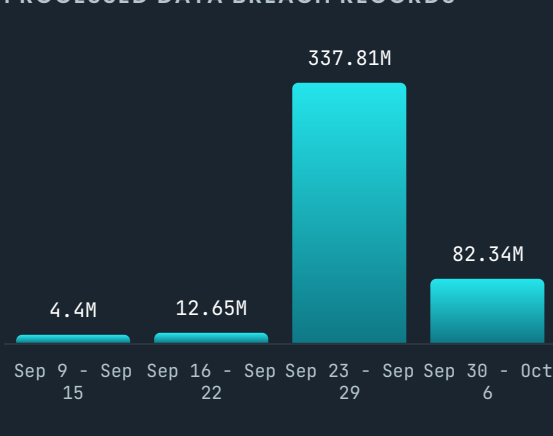
1.17B

BOTNET CAC RECORDS

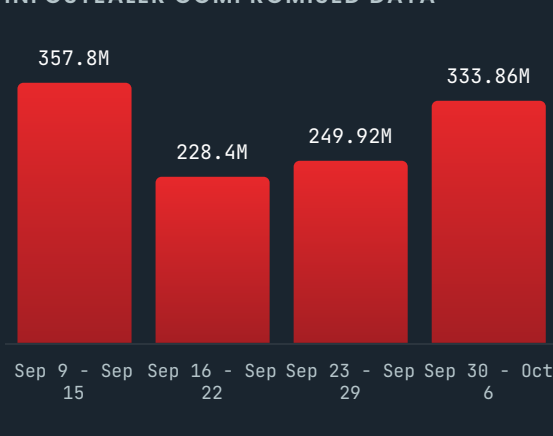
944

RANSOMWARE & DIGITAL EXTORTION

PROCESSED DATA BREACH RECORDS



INFESTEALER 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.