

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 28, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

5 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
Metaencryptor Ransomware	GE Vernova
PEAR Ransomware	Indroj Medical Group
DragonForce Ransomware	Arizona Vascular Medical Equipment
Clop Ransomware	Amey
Vexy Ransomware	Majani Insurance Brokers

VULNERABILITY DISCLOSURES

5 disclosures

CVE-2026-5430

Authentication Bypass Vulnerability via JWT Algorithm Confusion in WSO2 API Manager and Related Products

CVE-2026-71362

Incorrect Authorization Vulnerability in Adobe Commerce and Magento Open Source

CVE-2026-67279

SSH Pre-Authentication Rekey State Bypass Vulnerability in MikroTik RouterOS

CVE-2026-88771

Improper Input Validation Vulnerability in Citrix NetScaler ADC and NetScaler Gateway

CVE-2026-88772

Memory Overflow Vulnerability in Citrix NetScaler ADC and NetScaler Gateway

DEEP AND DARK WEB INTELLIGENCE

11 findings

CRITICAL FINDINGS

CRITICAL

RaaS Program Dubbed "KillSec" Advertised

On September 20, 2026, untested threat actor "KillSec" advertised a partner program for a ransomware-as-a-service (RaaS) operation on a predominantly Russian-language DDW forum TlerOne.

Source: TlerOne Actor: KillSec

DATA BREACHES & LEAKS

CRITICAL

Data Allegedly Associated with Sasai Fintech Leaked

On September 25, 2026, well-reputed threat actor "888" leaked data allegedly associated with Sasai Fintech on a predominantly English-language DDW forum PwnForums.

Source: PwnForums Actor: 888

CRITICAL

Data Allegedly Associated with Wealthfront Advertised

On September 27, 2026, moderately credible threat actor "bleedingout" advertised a database allegedly associated with Wealthfront on a predominantly Russian-language DDW forum Exploit.

Source: Exploit Actor: bleedingout

CRITICAL

Data Allegedly Tied to Lucky Shot USA Advertised

On September 24, 2026, moderately credible threat actor "renn" advertised data allegedly associated with Lucky Shot USA on Exploit.

Source: Exploit Actor: renn

CRITICAL

Medicare and Medicaid Patient Data Allegedly Exfiltrated from an Unnamed Kansas Clinic Advertised

On September 28, 2026, untested threat actor "BigCash" advertised data allegedly associated with Medicare and Medicaid patient records on Exploit.

Source: Exploit Actor: BigCash

HIGH

Data Allegedly Tied to UAE-Based Individuals Advertised

On September 24, 2026, moderately credible threat actor "HelluvaHack" advertised data allegedly associated with UAE-based individuals on Exploit.

Source: Exploit Actor: HelluvaHack

UNAUTHORIZED ACCESS CLAIMS

HIGH

Corporate SSO Access to Dynatrace Platform Allegedly Associated with Kyndryl Email Account Advertised

On September 27, 2026, moderately credible threat actor "ShadowByt3S" advertised corporate access to the sso.dynatrace[.]com platform on PwnForums.

Source: PwnForums Actor: ShadowByt3S

HIGH

Network Access Allegedly Tied to GSE Group Advertised

On September 22, 2026, untested threat actor "ShadowByt3\$ 2.0" advertised VPN and RMM access allegedly associated with GSE Group on TlerOne.

Source: TlerOne Actor: ShadowByt3\$ 2.0

VULNERABILITY EXPLOITATION

CRITICAL

Alleged MariaDB Zero-Day Vulnerability and Exploit Advertised

On September 27, 2026, moderately credible threat actor "Spaniard" advertised an alleged zero-day vulnerability and exploit targeting MariaDB on PwnForums.

Source: PwnForums Actor: Spaniard

HIGH

Alleged Unified Hardware Wallet Exploit Panel Targeting Ledger, Trezor, SafePal, and OneKey Advertised

On September 25, 2026, untested threat actor "evil" advertised an alleged unified hardware wallet exploit panel targeting Ledger, Trezor, SafePal, and OneKey devices on Exploit.

Source: Exploit Actor: evil

NEW LEAKSITES, MARKETPLACES, FORUMS

HIGH

New Ransomware-as-a-Service Site Emerges

On September 25, 2026, ZeroFox observed a new dark web site operating under the name "ContFR."

Source: Dark Web Site Actor: ContFR

PROCESSED DATA SET STATISTICS

Past 4 Weeks

322.97M

CAC RECORDS

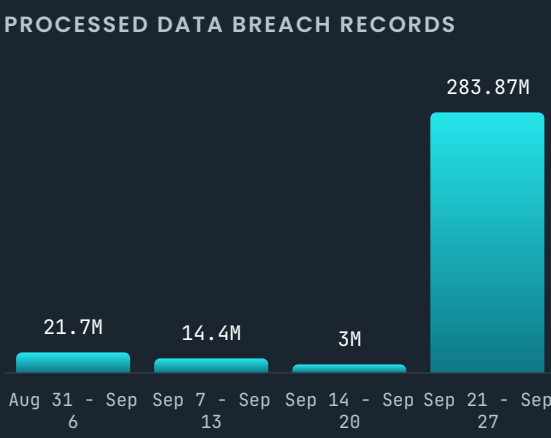
1.07B

BOTNET CAC RECORDS

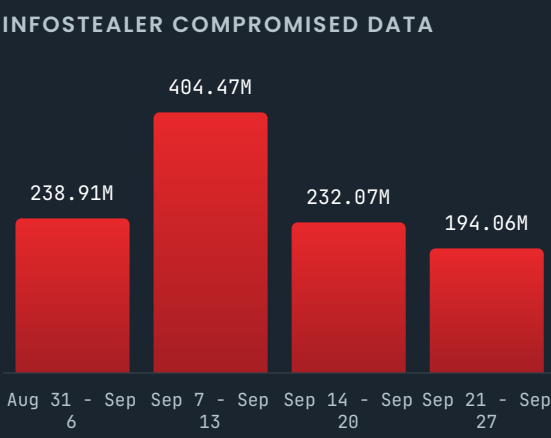
852

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.