

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 2, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

5 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
GENESIS Ransomware	VeroScience
REDACT	Graybar Electric
INC Ransomware	Guardian Pharmacy Services
INC Ransomware	Northern Counties Health Care
n0n Ransomware	Houston Thyroid & Endocrine Specialists

VULNERABILITY DISCLOSURES

2 disclosures

[CVE-2026-104286](#)

Path Traversal in Fortinet FortiMail

[CVE-2026-54154](#)

Code Injection in Kiteworks Email Protection Gateway

DEEP AND DARK WEB INTELLIGENCE

7 findings

CRITICAL FINDINGS

CRITICAL

Law Enforcement Seizes Leak Site and Servers

On September 30, 2026, an international law enforcement operation dubbed "Operation KillSwitch," led by German authorities, reportedly seized the KillSec ransomware group's dark web data leak site and servers.

Source: Kill Security Ransomware

CRITICAL

Data Allegedly Associated with Cisco Systems Advertised

On October 1, 2026, untested threat actor "Mr_Raccoonn" advertised a database allegedly associated with Cisco Systems on a predominantly English-language DDW forum DarkForums.

Source: DarkForums **Actor:** Mr_Raccoonn

CRITICAL

Alleged Google Cloud/Firebase Credentials Advertised

On October 1, 2026, well-reputed threat actor "MrDark" advertised 2,690 JSON credential files, allegedly containing valid Google Cloud and Firebase credentials, on a predominantly Russian-language DDW forum XSS.

Source: XSS **Actor:** MrDark

HIGH

Multi-National Scraped B2B Datasets Allegedly Associated with RevenueBase Advertised

Over four consecutive days, from September 28 to October 1, 2026, untested threat actor "B2BMatrix" advertised four scraped B2B databases totaling over 102 million records, allegedly sourced from RevenueBase, on a predominantly English-language DDW forum PwnForums.

Source: PwnForums **Actor:** B2BMatrix

UNAUTHORIZED ACCESS CLAIMS

HIGH

SSH and FortiGate Access Allegedly Tied to Mexico-Based Telecommunications Company Advertised

On October 1, 2026, untested threat actor "SCP-2013" also known as "ALPHV" and "Dark_Alpha" advertised SSH and FortiGate access with super_admin rights allegedly associated with an unnamed Mexico-based telecommunications company on a predominantly Russian and English-language DDW forums Exploit, RehubCom and DarkForums.

Source: Exploit/RehubCom/DarkForums **Actor:** SCP-2013, ALPHV, Dark_Alpha

HIGH

Web Shell Access Allegedly Tied to Thailand-Based Retail and Hospitality Company Advertised

On September 30, 2026, an untested threat actor "WAMBAM99" advertised web shell (ASPX) and MSSQL sysadmin access with NT AUTHORITY\SYSTEM and "sa" rights allegedly associated with an unnamed Thailand-based retail and hospitality company on DarkForums.

Source: DarkForums **Actor:** WAMBAM99

HIGH

Tailscale Access Allegedly Tied to Aerospace Technology Company in Asia Advertised

On September 28, 2026, untested threat actor "guo_df49" advertised Tailscale access allegedly associated with an unnamed aerospace technology company company in Asia on DarkForums.

Source: DarkForums **Actor:** guo_df49

PROCESSED DATA SET STATISTICS

Past 4 Weeks

382.41M

CAC RECORDS

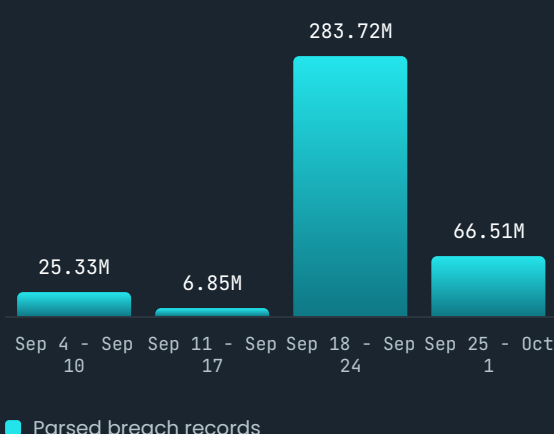
1.18B

BOTNET CAC RECORDS

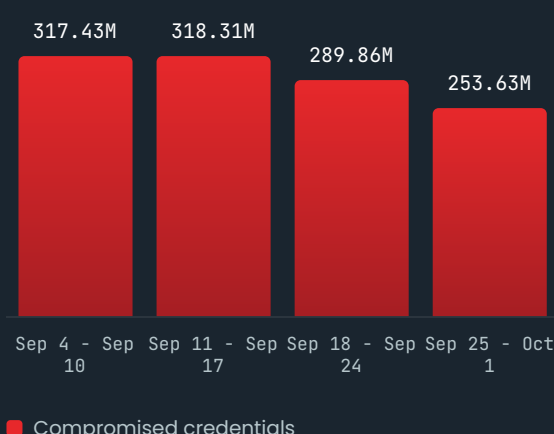
891

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.