ZEROFOX

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.

August 7, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

4 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
INC Ransomware	Virginia Peninsula Regional Jail
OROVA Ransomware	Ultra Fame
The Gentlemen Ransomware	Bater
Qilin Ransomware	Mera Metal

VULNERABILITY DISCLOSURES

4 disclosures

CVE-2026-15307
Server-Side File Write and SSRF Vulnerability in Django GeoDjango

CVE-2026-16498
Cross-Tenant Credential Reuse in HashiCorp terraform-mcp-server

CVE-2026-58873
Authentication Bypass Vulnerability in Veeam Service Provider Console

CVE-2026-64531
Local Privilege Escalation Vulnerability in Linux Kernel Open vSwitch

DEEP AND DARK WEB INTELLIGENCE

10 findings

CRITICAL FINDINGS

CRITICAL **Data Allegedly Associated with Morgan Sindall Group Leaked**

On August 6, 2026, untested threat actor "Persistent" leaked data allegedly associated with Morgan Sindall Group, a UK-based construction and infrastructure firm on the predominantly English-language deep and dark web (DDW) forum Spear.

Source: Spear/DarkForums **Actor:** Persistent

CRITICAL **Data Allegedly Associated with City24 Advertised**

On August 6, 2026, untested threat actor "vdeployis" advertised data allegedly associated with City24, a Ukraine-based payment company on the predominantly English-language DDW forum DarkForums.

Source: DarkForums **Actor:** vdeployis

CRITICAL **Data Allegedly Associated with DEGIRO Advertised**

On August 7, 2026, untested threat actor "dreamss" advertised data allegedly associated with DEGIRO on DarkForums.

Source: DarkForums **Actor:** dreamss

VULNERABILITY EXPLOITATION

HIGH **Alleged RCE Vulnerability Affecting OpenCart Plugin Advertised**

On August 6, 2026, untested threat actor "grantall" advertised an auction for an alleged remote code execution (RCE) vulnerability affecting an unnamed OpenCart plugin on the predominantly Russian-language DDW forum Exploit.

Source: Exploit **Actor:** grantall

UNAUTHORIZED ACCESS CLAIMS

HIGH **RDWeb Access Allegedly Associated with Undisclosed U.S.-Based Company Advertised**

On August 6, 2026, untested threat actor "Cerebellum" advertised an auction for RDWeb access allegedly associated with an undisclosed U.S.-based company on Exploit.

Source: Exploit **Actor:** Cerebellum

DATA BREACHES & LEAKS

HIGH **PII Data Allegedly Associated with U.S.-Based Individuals Advertised**

On August 5, 2026, well-regarded threat actor "agcash6" advertised an auction for a dataset allegedly associated with U.S.-based individuals on Exploit.

Source: Exploit **Actor:** agcash6

NEW LEAKSITES, MARKETPLACES, FORUMS

CRITICAL **New Data Leak Site Emerges**

On August 7, 2026, ZeroFox observed a new data leak site named "Helix". As of this report, the leak site lists 5 victims and is accessible via the following dark web address: hXXp://heliwr2sncrd3ndsz5oho6mzqw3x5u7mvox5zcsngc5wm7v4l5k7oryd[.]onion

Source: Leak Site **Actor:** Helix

CRITICAL **New Data Leak Site Emerges**

On August 7, 2026, ZeroFox observed a new data leak site named "L Group". As of this report, the leak site lists 26 victims and is accessible via the following dark web address: hXXp://4zrjdyuq4sjogm2epwwoleeqquavhwo3o7fakstnlgox6guqt3qpe4qd.onion

Source: Leak Site **Actor:** L Group

CRITICAL **New Ransomware Leak Site Emerges**

On August 7, 2026, ZeroFox observed a new ransomware leak site named "Storm". As of this report, the leak site lists 6 victims and is accessible via the following dark web address: hXXp://yqhecvqtdvq6p7duqcgw2qca77spbgakxcoibtx6zpvfshltsbbbhfqd[.]onion

Source: Leak Site **Actor:** Storm

CRITICAL **New Data Leak Site Emerges**

On August 7, 2026, ZeroFox observed a new data leak site named "Barracuda". As of this report, the leak site lists 4 victims and is accessible via the following dark web address: hXXp://uvm6hk4wwstfdqja5z5htgtiehmfyflflfjz6iozsuqyacyibzxefkqd[.]onion

Source: Leak Site **Actor:** Barracuda

COLLECTED, PROCESSED DATA BREACHES

2 entries

VICTIM	SOURCE	THREAT ACTOR	PROCESSED RECORDS
erdil[.]fr	DarkForums	Sophia01	310
kaffir[.]fr	DarkForums	Sophia01	476

PROCESSED DATA SET STATISTICS

Past 4 Weeks

303.68M
CAC RECORDS

843.32M
BOTNET CAC RECORDS

874
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.