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.

September 25, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

7 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
INC Ransomware	UK Brazilian Jiu Jitsu Association
INC Ransomware	Welgen One
Qilin Ransomware	All Tech Machine & Engineering
The Gentlemen Ransomware	Grupo Ligue-se
Rhysida Ransomware	Legis
LockBit 5.0 Ransomware	Anery Home Care
INC Ransomware	Grupo Caberj

VULNERABILITY DISCLOSURES

1 disclosure

CVE-2026-48842

SQL Injection Vulnerability in Roundcube Webmail

DEEP AND DARK WEB INTELLIGENCE

8 findings

CRITICAL FINDINGS

CRITICAL **New Data Leak Site Emerges**

On September 25, 2026, ZeroFox observed a new data leak site operating under the name "ULOSE."

Source: Leak site **Actor:** ulose

CRITICAL **New Data Leak Site Emerges**

On September 25, 2026, ZeroFox observed a new data leak site operating under the name "ImNotAVillain."

Source: Leak Site **Actor:** ImNotAVillain

CRITICAL **New Data Leak Site Emerges**

On September 25, 2026, ZeroFox observed a new data leak site operating under the name "NoTrace Group."

Source: Leak site **Actor:** notrace group

DATA BREACHES & LEAKS

HIGH **PMS Access and Data Allegedly Associated with Multiple Hotels in South Korea Advertised**

On September 25, 2026, moderately credible threat actor "DDEEAALLEERR" advertised alleged access to data and PMS (Property Management System) belonging to hotels in South Korea on a predominantly Russian-language DDW forum Exploit.

Source: Exploit **Actor:** DDEEAALLEERR

UNAUTHORIZED ACCESS CLAIMS

HIGH **GitHub Access Allegedly Tied to U.S.-Based Company Pfizer Advertised**

On September 23, 2026, untested threat actor "HollowCrimeCorp" advertised full GitHub access and organization control allegedly associated with Pfizer on the predominantly English-language DDW forum BreachForums (breached[.]st).

Source: Breachforums **Actor:** hollowcrimecorp

HIGH **RDWeb Access Allegedly Tied to Canada-Based Accounting Company Advertised**

On September 23, 2026, untested threat actor "MrRDWeb" advertised an auction for RDWeb access with domain user rights allegedly associated with an unnamed Canada-based accounting company for legal practices on Exploit.

Source: Exploit **Actor:** mrrdweb

HIGH **Network Access Allegedly Tied to Italy-Based Industrial Machinery & Equipment Company Advertised**

On September 24, 2026, untested threat actor "aloev" advertised an auction for network access with domain administrator rights allegedly associated with an unnamed Italy-based industrial machinery and equipment company on Exploit.

Source: Exploit **Actor:** aloev

VULNERABILITY EXPLOITATION

HIGH **Alleged One-Day VMware vCenter Exploit Advertised**

On September 24, 2026, untested threat actor "Matilda" advertised an alleged one-day exploit for VMware vCenter on the predominantly Russian-language DDW forum Exploit. Notably, the same was posted on predominantly English-language DDW forum RehubCom.

Source: Exploit/rehubcom **Actor:** matilda, lalo

COLLECTED, PROCESSED DATA BREACHES

3 entries

VICTIM	SOURCE	THREAT ACTOR	PROCESSED RECORDS
alert360[.]com	ShinyHunters	ShinyHunters	385.04K
sushietcie[.]fr	PwnForums	4me1	6.8K
zara[.]com	ShinyHunters	ShinyHunters	256.43K

PROCESSED DATA SET STATISTICS

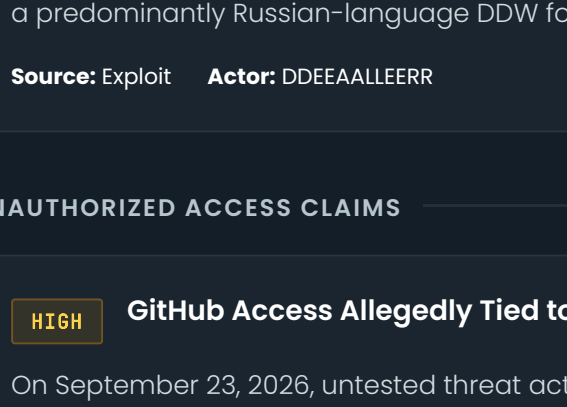
Past 4 Weeks

326.83M CAC RECORDS

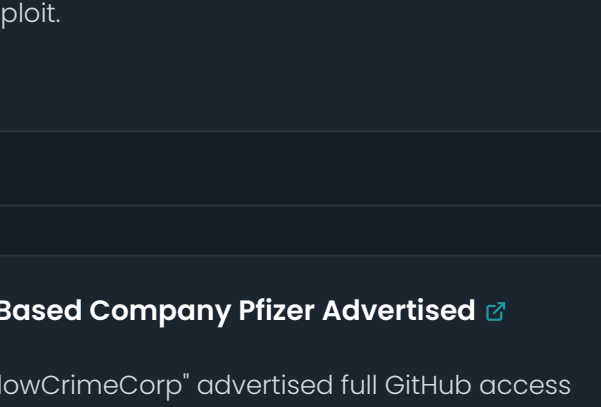
1.07B BOTNET CAC RECORDS

962 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.