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 72 hours.

August 3, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

6 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
PEAR Ransomware	Sonitor Technologies
FALCON	DNOW
Clop Ransomware	Blue Vista Capital Management
CoinbaseCartel Ransomware	MIM Fertility
Orion Leaks Ransomware	Nitrex Chemicals India
Qilin Ransomware	The Saturday Evening Post

VULNERABILITY DISCLOSURES

1 disclosure

CVE-2026-48449
Incorrect Authorization Vulnerability in Adobe Campaign Classic

DEEP AND DARK WEB INTELLIGENCE

9 findings

CRITICAL FINDINGS

CRITICAL **Data Allegedly Associated with Bank of America Leaked**

On July 31, 2026, untested threat actor "immanuel_Kant" leaked data allegedly associated with Bank of America on the predominantly Russian-language DDW forum XSS.

Source: XSS **Actor:** Immanuel_Kant

CRITICAL **Data Allegedly Associated with "Citigroup Securities" Leaked**

On August 1, 2026, untested threat actor "Data7785" leaked data allegedly associated with "Citigroup Securities" on the predominantly English-language DDW forum DarkForums

Source: DarkForums **Actor:** Data7785

CRITICAL **27 New Victims Listed**

On July 31, 2026, ZeroFox observed that The Gentlemen ransomware group listed 27 new victims on its leak site.

Source: The Gentlemen Ransomware

UNAUTHORIZED ACCESS CLAIMS

HIGH **Alleged Web Panel Access Tied to South Asia-Based Travel Agency Advertised**

On July 31, 2026, well-regarded threat actor "Trim" advertised an auction for web panel access with administrator rights allegedly tied to an unnamed South Asia-based travel agency on the predominantly Russian-language DDW forum Exploit.

Source: Exploit **Actor:** Trim

HIGH **Alleged RDWeb Access Tied to South Africa-Based Software Company Advertised**

On July 31, 2026, well-known threat actor "Big-Bro" advertised an auction for RDWeb access with domain user rights allegedly tied to an unnamed South Africa-based software company on the predominantly Russian-language DDW forum Exploit.

Source: Exploit **Actor:** Big-Bro

NEW LEAKSITES, MARKETPLACES, FORUMS

HIGH **New Data Leak Site Emerges**

On July 31, 2026, ZeroFox observed a new dark web leak site named "FALCON." As of reporting, one victim has been listed on the leak site. The site remains accessible via hXXp://i7loab6thv24lb7jdr3qoeumbvilwhbgnwsctnlfmvsv7gls3vsiw6yd[.]onion/

Source: Leak Site **Actor:** FALCON

DATA BREACHES & LEAKS

CRITICAL **Data Allegedly Associated with Cyprus WhatsApp Users Advertised**

On August 1, 2026, moderately credible threat actor "IMAN" advertised access allegedly tied to Cyprus WhatsApp users on the predominantly English-language DDW forum PwnForums.

Source: PwnForums **Actor:** IMAN

CRITICAL **Data Allegedly Associated with South Africa Reserve Bank Leaked**

On August 1, 2026, untested threat actor "NullSecNg" advertised employee data records allegedly associated with South Africa Reserve Bank on the predominantly English-language DDW forum DarkForums.

Source: DarkForums **Actor:** NullSecNg

CRITICAL **Data Allegedly Associated with Qi Card Leaked**

On August 3, 2026, an untested threat actor "GoreTurbine" advertised customer data allegedly associated with Qi Card on the predominantly English-language DDW forum PwnForums.

Source: PwnForums **Actor:** GoreTurbine

COLLECTED, PROCESSED DATA BREACHES

7 entries

VICTIM	SOURCE	THREAT ACTOR	PROCESSED RECORDS
homers[.]fr	PwnForums	ChimeraZ	35.85K
Municipal Government of Villahermosa	DarkForums	cenfecracked	120.77K
Keepcool	PwnForums	84City	166.45K
Zhejiang Benyi New Energy	PwnForums	888	16.04K
DruBlox	Exploit	HighRisk	2.9K
BLACKSEXFINDER	Exploit	HighRisk	179.92K
Alfobe Brands Online Shopping	PwnForums	chinabase	29.97K

PROCESSED DATA SET STATISTICS

Past 4 Weeks

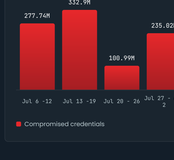
363.66M CAC RECORDS

946.65M BOTNET CAC RECORDS

794 RANSOMWARE & DIGITAL EXTORTION

PROCESSED DATA BREACH RECORDS

INFOSTEALER COMPROMISED DATA



Threat Actor Profiles

A threat actor profile is a comprehensive overview of a malicious entity that outlines its motivations, capabilities, and observed attack patterns. These profiles typically include known aliases, targeted sectors, and documented tactics, techniques, and procedures (TTPs), and are used to characterize a wide range of groups operating across the cyber threat landscape, from highly sophisticated actors to those driven by financial or ideological motives.

Monthly Threat Spotlight

The Monthly Threat Spotlight highlights highly unusual threat actor behaviors, bizarre tactics, and significant spikes in specific ransomware or threat operations observed over a recent period. This intelligence focuses on the anomalies and notable shifts that stand out from the baseline threat landscape.