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 10, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

5 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
Qilin Ransomware	Bloom Financials
INC Ransomware	ATMS & Co
Insomnia	Park Place Behavioral Health Care
Qilin Ransomware	Akuğur Law Firm
DragonForce Ransomware	One Community Federal Credit Union

DEEP AND DARK WEB INTELLIGENCE

12 findings

CRITICAL FINDINGS

CRITICAL **Alleged Breach of bIgCloud's Data and Downstream Victim Exposure**

On August 8-9, 2026, threat actors "misere" and "ChimeraZ" claimed to have breached alleged CRM data associated with two disctinct entities on the predominantly English-language deep and dark web forum PwnForums.

Source: PwnForums **Actor:** misere, ChimeraZ

CRITICAL **Alleged Comcast-Linked Tradeify[.]co Records Leaked**

On August 10, 2026, untested threat actor "kill" shared a database allegedly containing Comcast-linked Tradeify[.]co records on the predominantly Russian-language deep and dark web forum Exploit.

Source: Exploit **Actor:** kill

CRITICAL **Internal Azure Tenant Data Allegedly Tied to HCLTech and TCS Advertised**

On August 7 and August 10, 2026, untested threat actor "TheHatman" published two separate posts on the predominantly English-language deep and dark web forum PwnForums, advertising internal employee databases allegedly extracted from Azure/Entra ID portals using compromised credentials.

Source: PwnForums/Spear/DarkForums **Actor:** TheHatman

CRITICAL **Data Allegedly Associated with Lucid Motors and eShocan Advertised**

On August 6, 2026, untested threat actor "carport" claiming affiliation with the "SovCali Group" advertised a proprietary engineering database allegedly associated with Lucid Motors and eShocan on the predominantly English-language deep and dark web forum PwnForums.

Source: PwnForums/DarkForums **Actor:** carport

CRITICAL **Data Allegedly Associated with 365.bank Leaked**

On August 7, 2026, untested threat actor "ssyndicate" leaked data allegedly associated with 365.bank on the predominantly English-language deep and dark web forum PwnForums.

Source: PwnForums **Actor:** ssyndicate

CRITICAL **24 New Victims Listed**

On August 07, 2026, ZeroFox observed that The Gentlemen ransomware group listed 24 new victims on their leak site.

Source: The Gentlemen Ransomware

CRITICAL **Data Allegedly Associated with Morgan Stanley Advertised**

On August 8, 2026, threat actor "MDGhost666" advertised a database allegedly associated with Morgan Stanley, a U.S.-based global financial services firm on the predominantly English-language deep and dark web forum DarkForums.

Source: DarkForums **Actor:** MDGhost666

UNAUTHORIZED ACCESS CLAIMS

HIGH **Web Panel Access Allegedly Associated with Supreme Court's Decision Directory Advertised**

On August 7, 2026, untested threat actor "marlanwg" advertised web panel access with administrator rights allegedly associated with the Supreme Court's Decision Directory (Direktori Putusan Mahkamah Agung) on the predominantly English-language deep and dark web forum DarkForums.

Source: DarkForums **Actor:** marlanwg

HIGH **Portal Access Allegedly Associated with Meta's Law Enforcement Online Request System Advertised**

On August 7, 2026, untested threat actor "marlanwg" advertised access allegedly associated with the Meta's Law Enforcement Online Request System (LEORS) portal on the predominantly English-language deep and dark web forum DarkForums.

Source: DarkForums **Actor:** marlanwg

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

On August 7, 2026, well-known threat actor "Big-Bro" advertised RDWeb access with domain user rights allegedly associated with an unnamed U.S.-based consumer services company on the predominantly Russian-language deep and dark web forum Exploit.

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

HIGH **Pulse Secure VPN Access Allegedly Associated with India-Based Financial Services Company Advertised**

On August 6, 2026, untested threat actor "JWKush" advertised Pulse Secure VPN access with local administrator rights allegedly associated with an unnamed India-based financial services company on the predominantly English-language deep and dark web forum PwnForums.

Source: PwnForums **Actor:** JWKush

VULNERABILITY EXPLOITATION

HIGH **Alleged Exploit for CVE-2026-16232 Advertised**

On August 6, 2026, untested threat actor "display107" advertised an alleged fully operational exploit for CVE-2026-16232 on the predominantly Russian-language deep and dark web forum Exploit.

Source: Exploit **Actor:** display107

COLLECTED, PROCESSED DATA BREACHES

2 entries

VICTIM	SOURCE	THREAT ACTOR	PROCESSED RECORDS
Redhat[.]com (Employee Database)	DarkForums	urharrmless	411
efab[.]fr	PwnForums	84City	32.28K

PROCESSED DATA SET STATISTICS

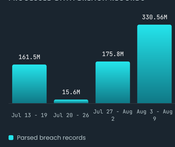
Past 4 Weeks

683.47M CAC RECORDS

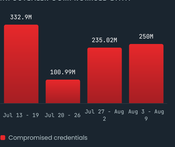
918.91M BOTNET CAC RECORDS

846 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.