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 11, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

5 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
Helix	Uber Freight
Play Ransomware	MIE Solutions
LeakedData	Mayer Brown
Helix	Highwoods Properties
The Gentlemen Ransomware	Applied Business Investments

DEEP AND DARK WEB INTELLIGENCE

9 findings

CRITICAL FINDINGS

CRITICAL **Alleged Fortigate 8.0.0 vm64 Pre-Authentication SSRF Zero-Day Exploit Advertised**

On August 10, 2026, moderately credible threat actor "btc1837" advertised an alleged pre-authentication Server-Side Request Forgery (SSRF) zero-day exploit and scanner targeting FortiGate 8.0.0 vm64 on the predominantly Russian-language deep and dark web forum Exploit.

Source: Exploit **Actor:** btc1837

CRITICAL **Alleged Phishing Tool Called "Phishium" Advertised**

On August 9, 2026, untested threat actor "Phishout" advertised for rent an alleged phishing and stealing tool named "Phishium" on the predominantly Russian-language deep and dark web forum Exploit.

Source: Exploit **Actor:** Phishout

CRITICAL **Data Allegedly Associated with FPFX Tech Advertised**

On August 11, 2026, untested threat actor, "KyokoIT," advertised a database allegedly associated with FPFX Tech on the deep and dark web forum PwnForums.

Source: PwnForums **Actor:** KyokoIT

CRITICAL **Data Allegedly Associated with Ministry of Defence of the Republic of Bulgaria Advertised**

On August 10, 2026, moderately credible threat actor, "ByteToBreach," advertised data allegedly associated with the Ministry of Defence of the Republic of Bulgaria on the predominantly English-language deep and dark web forum DarkForums.

Source: DarkForums/Exploit **Actor:** ByteToBreach

CRITICAL **Data Allegedly Associated with Population and Immigration Authority of Israel Advertised**

On August 8, 2026, threat actor "GordonFreeman" advertised a database allegedly exfiltrated from the Population and Immigration Authority of Israel on the predominantly English-language deep and dark web forum DarkForums.

Source: DarkForums **Actor:** GordonFreeman

UNAUTHORIZED ACCESS CLAIMS

HIGH **Network Access Allegedly Tied to Asia-Based Telecommunications Company Advertised**

On August 9, 2026, untested threat actor "missiyaprizrak0" advertised SSH and VPN access allegedly associated with an unnamed Asia-based "Top 10" telecommunications company on the predominantly English-language deep and dark web forum PwnForums.

Source: PwnForums **Actor:** missiyaprizrak0

HIGH **RDWeb Access Allegedly Tied to Canada-Based Non-Profit Organization Advertised**

On August 9, 2026, untested threat actor "impotent4000" advertised an auction for RDWeb access with domain user rights allegedly tied to an unnamed Canada-based non-profit organization on the predominantly Russian-language deep and dark web forum Exploit.

Source: Exploit **Actor:** impotent4000

HIGH **Fortinet VPN Access Bundle Allegedly Tied to Six U.S. and Turkey-Based Companies Advertised**

On August 8, 2026, untested threat actor "_H_T_P_0101" advertised an auction for Fortinet VPN access bundle with user and administrator rights allegedly tied to three undisclosed U.S.-based companies and three undisclosed Turkey-based companies on the predominantly Russian-language deep and dark web forum Exploit.

Source: Exploit **Actor:** _H_T_P_0101

HIGH **Alleged DoorDash and T-Mobile Insider Service Advertised**

On August 9, 2026, untested threat actor "naloxone" advertised alleged DoorDash and T-Mobile Insider service on the predominantly English-language deep and dark web forum DarkForums.

Source: DarkForums **Actor:** naloxone

COLLECTED, PROCESSED DATA BREACHES

3 entries

VICTIM	SOURCE	THREAT ACTOR	PROCESSED RECORDS
HelloAsso	PwnForums	floflfo9459	158.4K
Koohdar Beekeeping	DarkForums	MXDIV	317
LG Metrologia	PwnForums	Tanaka	11.48K

PROCESSED DATA SET STATISTICS

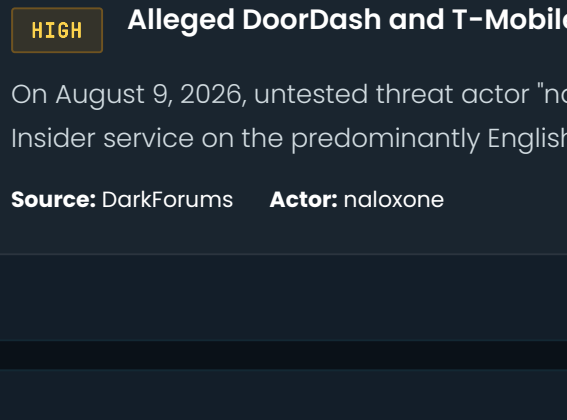
Past 4 Weeks

822.89M CAC RECORDS

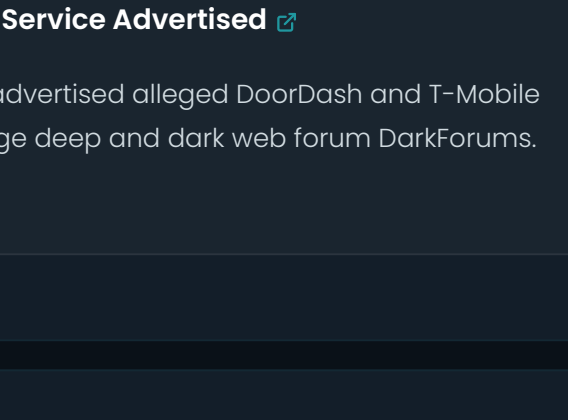
697.11M BOTNET CAC RECORDS

838 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.