ZEROFOX

Deep and Dark Web Intelligence Reporting

Here is a curated list of critical incidents and compromised data observed in deep and dark web ransomware sites, forums, and marketplaces ingested into the ZeroFox Platform since our last reporting.

July 7, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

5 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
The Gentlemen Ransomware	Mibet Energy
Wallstreet	Baraga County Memorial Hospital
The Gentlemen Ransomware	Arabia Falcon Insurance
Play Ransomware	Silvestri & Associates Insurance
GENESIS Ransomware	Dunagan Associates

DEEP AND DARK WEB INTELLIGENCE

10 findings

CRITICAL FINDINGS

CRITICAL **PwnForums: Alleged Breach of Accenture's Source Code Data (888)**

On July 6, 2026, a well reputed threat actor and forum moderator "888" advertised data associated with Accenture, an Ireland-based professional services and management consulting company, on predominantly English-language deep and dark web forum PwnForums.

PwnForums

CRITICAL **DarkForums: Alleged Data of Community Development Authority (CDA) Advertised (neonlite)**

On July 7, 2026, an untested threat actor "neonlite" advertised a dataset allegedly associated with Community Development Authority (CDA) in Dubai, United Arab Emirates, on a predominantly English-language dark web forum DarkForums.

DarkForums

CRITICAL **PwnForums: Alleged Breach of Hellenic Navy Data (lastopsecbroker)**

On July 6, 2026, an untested threat actor "lastopsecbroker" claimed to have leaked data associated with Hellenic Navy, naval force of Greece and a branch of the Hellenic Armed Forces, on predominantly English-language deep and dark web forum PwnForums.

PwnForums

CRITICAL **Breached/DarkForums: Alleged Data Associated with monday.com Advertised (almeria, egomanyak)**

On July 6, 2026, an untested threat actor "almeria" advertised to sell a dataset allegedly associated with monday.com, a global software company, on a predominantly English-language dark web forum Breached.

Breached

CRITICAL **Exploit: Alleged Data of National Aerospace Science and Technology Park of Pakistan Advertised (Cyb3R_Shubh4M)**

On July 6, 2026, an untested threat actor "Cyb3R_Shubh4M" advertised to sell a 20 GB dataset allegedly associated with the National Aerospace Science and Technology Park of Pakistan, on a predominantly Russian-language deep and dark web forum Exploit.

Exploit

CRITICAL **DUTY-FREE: Alleged 1,000 Fortinet VPN Entry Points Advertised (IntegraGT)**

On July 6, 2026, an untested threat actor "IntegraGT" advertised to sell an alleged collection of over 1,000 Fortinet VPN entry points, on a predominantly Russian-language deep web forum DUTY-FREE.

DUTY-FREE

UNAUTHORIZED ACCESS CLAIMS

HIGH **Exploit: Alleged Network Access to U.S.-Based Telecommunications Company Advertised (hubert)**

On July 4, 2026, a moderately credible threat actor "hubert" advertised an auction for network access allegedly associated with an unnamed U.S.-based telecommunications company, on a predominantly Russian-language deep and dark web forum Exploit.

Exploit

HIGH **RehubCom: Alleged Fortinet VPN Access to Two U.S.-Based Legal Services and Business Consulting Companies Advertised (corestrike)**

On July 5, 2026, an untested threat actor "corestrike" advertised to sell Fortinet VPN access allegedly associated with two unnamed U.S.-based legal services and business consulting companies, on a predominantly Russian-language deep and dark web forum RehubCom.

RehubCom

HIGH **Exploit: Alleged Network Access to China-Based AI Platform Advertised (512bit)**

On July 3, 2026, an untested threat actor "512bit" advertised an auction for network access allegedly associated with an unnamed China-based enterprise-level AI platform and computing infrastructure provider, on a predominantly Russian-language deep and dark web forum Exploit.

Exploit

HIGH **Exploit: Alleged RDWeb Access to U.S.-Based Cable Equipment and Solutions Supplying Company Advertised (dogs)**

On July 4, 2026, an untested threat actor "dogs" advertised an auction for RDWeb access with domain user rights allegedly associated with an unnamed U.S.-based cable equipment and solutions supplying company, on a predominantly Russian-language deep and dark web forum Exploit.

Exploit

COLLECTED, PROCESSED DATA BREACHES

5 entries

VICTIM	SOURCE	THREAT ACTOR	PROCESSED RECORDS
utsh[.]edu[.]mx	DarkForums	Krxzy	784
yaeliq[.]com	DarkForums	Richard2002	9.5K
thpp[.]dtam[.]moph[.]go[.]th	DarkForums	Richard2002	923
educacionbogota[.]edu[.]co	DarkForums	DozerMx	15.2K
kawaiianimes[.]app	DarkForums	JustJK	1.2M

PROCESSED DATASET STATISTICS

Past 4 Weeks

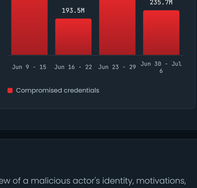
669.7M CAC RECORDS

1.2B BOTNET CAC RECORDS

786 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, bizarre tactics, and significant operational spikes that deviate from the baseline threat landscape.