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 in the past 24 hours.

July 17, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

5 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
RansomHouse	Fidelity Services Group
PEAR Ransomware	South Plains Rural Health Services
Chaos Ransomware	Aphena Pharma Solutions
The Gentlemen Ransomware	Terry P. Moosmann
INTERLOCK Ransomware	YMCA of Western North Carolina

DEEP AND DARK WEB INTELLIGENCE

11 findings

CRITICAL FINDINGS

CRITICAL **ShadowByt3S Claims Breach of Abbott Laboratories's Data**

On July 15, 2026, a credible threat actor "ShadowByt3S" claimed to have breached data associated with Abbott Laboratories, on a predominant English-language dark web forum DarkForums.

Source: DarkForums

CRITICAL **17 New Victims Listed**

On July 16, 2026, ZeroFox observed that The Gentlemen ransomware group listed 17 new victims on their leak site.

Source: The Gentlemen Ransomware

CRITICAL **Alleged 30,000+ Business-Level API Keys Advertised**

On July 16, 2026, an untested threat actor "chemda5lek3asba" advertised over 30,000 alleged business-level API keys, on a predominantly Russian-language deep and dark web forum Exploit.

Source: Exploit **Actor:** chemda5lek3asba

CRITICAL **Alleged Data Associated with Real Federación Española de Fútbol Leaked**

On July 15, 2026, a moderately credible threat actor "misere" claimed to have breached data associated with the Real Federación Española de Fútbol (RFEF), on a predominantly English-language deep and dark web forum PwnForums.

Source: PwnForums **Actor:** misere

UNAUTHORIZED ACCESS CLAIMS

HIGH **Alleged SSH and FortiGate Access to India-Based Telecommunications Company Advertised**

On July 16, 2026, an untested threat actor "APL-BRK" advertised to sell SSH and FortiGate access allegedly associated with an unnamed India-based telecommunications company, on a predominantly Russian-language deep and dark web forum XSS.

Source: XSS **Actor:** APL-BRK

HIGH **Alleged Data Associated with U.S.-Based Company UpSwell Marketing Advertised**

On July 14, 2026, an untested threat actor "Datavortex_BD" advertised to sell a dataset allegedly associated with UpSwell Marketing, a U.S.-based digital marketing company, on a predominantly English-language dark web forum DarkForums.

Source: DarkForums **Actor:** Datavortex_BD

VULNERABILITY EXPLOITATION

MEDIUM **Alleged TeamViewer SSRF Exploit Advertised**

On July 15, 2026, an untested threat actor "shredder00" advertised to sell alleged TeamViewer SSRF exploit, on a predominantly English-language dark web forum DarkForums.

Source: DarkForums **Actor:** shredder00

HACKTIVISM

MEDIUM **Alleged Cyberattack and Defacement on BSD Group Website**

On July 16, 2026, likely pro-Palestinian hacktivist group "Cyber Islamic Resistance" made a post in there telegram channel in which they claimed to have targeted BSD Group (bsd-group[.]com). Notably, at the time of reporting, the official website of BSD Group (bsd-group[.]com) has been observed to be defaced and displays a banner attributed to the hacktivist group.

Source: Telegram **Actor:** Cyber Islamic Resistance

MEDIUM **Alleged Ongoing DDoS Attack Affecting Saudi Arabia's Ministry Platform Qiwa**

On July 14, 2026, pro-Palestinian threat actor group "313 Team" claimed to have conducted DDoS attacks on Qiwa (qiwa[.]sa) website associated with Saudi Arabia government platform affiliated with the Ministry of Human Resources and Social Development, on their official Telegram channel.

Source: Telegram **Actor:** 313 Team

DATA BREACHES & LEAKS

CRITICAL **Alleged Data Associated with BDL India and MRSAM Program Advertised**

On July 14, 2026, an untested threat actor "slepra" advertised to sell 4.6 GB dataset allegedly associated with the India-based aerospace and defense company BDL India and Medium-Range Surface-to-Air Missile (MRSAM) program, on a predominantly English-language deep and dark web forum BreachForums (breached[.]su).

Source: BreachForums **Actor:** slepra

CRITICAL **Alleged Data of Qatar-Based Company Grand Central Advertised**

On July 15, 2026, an untested threat actor "Anonymous2090" advertised to sell a 44 GB dataset allegedly associated with Grand Central, a Qatar-based food manufacturing and catering company, on a predominantly English-language dark web forum DarkForums.

Source: DarkForums **Actor:** Anonymous2090

COLLECTED, PROCESSED DATA BREACHES

5 entries

VICTIM	SOURCE	THREAT ACTOR	PROCESSED RECORDS
1.8KK Mix Mailpass #399	XSS	STRADU_DB	1.89M
237K Corps MailPass	Exploit	Domainstore	227.5K
97K Mix Mailpass #411	DarkForums	stradu	97.69K
Service de Remplacement France (monservicedereplacement[.]fr)	Exploit	HighRisk	76.2K
MM Mega Market (online[.]mmvietnam[.]com)	Exploit	HighRisk	98.05K

PROCESSED DATASET STATISTICS

Past 4 Weeks

499.29M CAC RECORDS

1.1B BOTNET CAC RECORDS

776 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.