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 from July 3 to July 6, 2026.

July 6, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

5 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
KRYBIT Ransomware	Majuhome Concept
World Leaks	Treet Corporation
BASHE Ransomware	Holiday Palace
The Gentlemen Ransomware	Shamrock Holdings
INC Ransomware	Estrutural Zortea

DEEP AND DARK WEB INTELLIGENCE

10 findings

CRITICAL FINDINGS

CRITICAL **DarkForums: Alleged Data Associated with Aegis Defense Solutions Advertised for Sale (Shadowreaper)**

On July 5, 2026, an untested threat actor "Shadowreaper" advertised to sell data associated with Aegis Defense Solutions, a U.S.-based security consulting and firearms training company, on a predominantly English-language dark web forum DarkForums.

July 5, 2026 DarkForums

CRITICAL **PwnForums: Alleged Data Associated with Teletrac Navman Advertised for Sale (laserscript)**

On July 4, 2026, a moderately-credible threat actor "laserscript" advertised to sell data associated with Teletrac Navman, on a predominantly English-language deep and dark web forum PwnForums.

July 4, 2026 PwnForums

CRITICAL **DarkForums: Alleged Data Associated with Hanjoon NCS Co. Advertised for Sale (Moneyistime)**

On July 4, 2026, an untested threat actor "Moneyistime" advertised to sell data associated with Hanjoong NCS Co., on a predominantly dark web forum DarkForums.

July 4, 2026 DarkForums

HIGH **DarkForums: Alleged Breach of Golden Agri-Resources Data and Repost of Nintendo's Data Advertised (ShadowByt3S)**

On July 3, 2026, untested threat actor "ShadowByt3S" made a post titled "Sinar Mas Agribusiness and Food (Golden Agri-Resources) Breach and nintendo data," on a predominantly English-language deep and dark web forum DarkForums.

July 3, 2026 DarkForums

CRITICAL **DarkForums: Alleged Data Associated with Inland Revenue Board of Malaysia Advertised for Sale (dezetat)**

On July 3, 2026, an untested threat actor "dezetat" advertised to sell data associated with the Inland Revenue Board of Malaysia, on a predominantly English-language deep and dark web forum DarkForums.

July 3, 2026 DarkForums

HIGH **Exploit: Alleged Backend Access and Data Associated with VIPS Corretora de Cambio Advertised for Sale (scriptore)**

On July 3, 2026, an untested threat actor "scriptore" advertised to sell backend access and sensitive records associated with VIPS Corretora de Câmbio, on a predominantly Russian-language dark web forum Exploit.

July 3, 2026 Exploit

CRITICAL **Exploit: Alleged ClickFix panel Advertised for Sale (tfalse)**

On July 2, 2026, an untested threat actor "tfalse" advertised the sale of an alleged malware delivery framework known as a "ClickFix" panel, on a predominantly Russian-language deep and dark web forum Exploit.

July 2, 2026 Exploit

UNAUTHORIZED ACCESS CLAIMS

CRITICAL **Exploit: Alleged 1,200 Fortinet VPN Entry Points Advertised (Big-Bro)**

On July 2, 2026, a well-known threat actor "Big-Bro" advertised an auction for a collection of 1,200 Fortinet VPN entry points, on a predominantly Russian-language deep and dark web forum Exploit.

July 2, 2026 Exploit

CRITICAL **Exploit: Alleged 3,032 Turkey-Based FortiGate Entry Points Advertised (A-B-A)**

On July 2, 2026, an untested threat actor "A-B-A" advertised to sell a collection of 3,032 FortiGate entry points with super_admin rights, allegedly associated with Turkey-based organizations, on a predominantly Russian-language deep and dark web forum Exploit.

July 2, 2026 Exploit

NEW LEAKSITES, MARKETPLACES, FORUMS

HIGH **Leak Site: New Ransomware Leak Site Emerges (DOOMMAGEDDON)**

On July 3, 2026, ZeroFox identified a new ransomware data leak site dubbed "DOOMMAGEDDON." As of this report, the site lists five publicly named victims and one undisclosed entity categorized as "PAID." The leaksite is accessible via the following dark web addresses: hXXp://iac1jvmxjb2ivqlxxzmde4w6g53gn6ym7c3g6mfifveiyhqtp4wrkypyd[.]onion/

July 3, 2026

COLLECTED, PROCESSED DATA BREACHES

5 entries

VICTIM	SOURCE	THREAT ACTOR	PROCESSED RECORDS
3.5KK_Shopping_394_MailPass Combolist	XSS	STRADU_DB	2.8M
Kalkine[.]com	PwnForums	2019	2.2K
973.855 Lines Shopping Target HQ Germany De Combolist	Cracked	HqComboSpace	922.3K
100K STREAMING HIGH QUALITY COMBOLIST EMAILPASS Combolist	Cracked	Bears	9.9K
133.297 Lines Edu education Mixed Target Combolist	Cracked	HqComboSpace	130.8K

PROCESSED DATASET STATISTICS

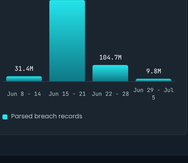
Past 4 Weeks

667.7M CAC RECORDS

1.2B BOTNET CAC RECORDS

732 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.