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.

July 22, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

5 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
Akira Ransomware	Finer & Finer
Kairos Ransomware	Collège O'Sullivan de Québec
Akira Ransomware	L&A Transport
CMD Organization	Finance Yorkshire
CoinbaseCartel Ransomware	Caterpillar

VULNERABILITY DISCLOSURES

1 disclosure

CVE-2026-50522

Deserialization Remote Code Execution in Microsoft SharePoint Server

DEEP AND DARK WEB INTELLIGENCE

9 findings

CRITICAL FINDINGS

CRITICAL **BlackRock's Internal Infrastructure Mapping Data Allegedly Leaked**

On July 21, 2026, untested threat actor "urharmless" breached internal infrastructure mapping allegedly associated with BlackRock on the predominantly English-language dark web forum DarkForums.

Source: DarkForums **Actor:** urharmless

CRITICAL **Data Allegedly Associated with RapidFort Advertised**

On July 22, 2026, moderately credible threat actor "xpl0itrs" advertised data allegedly associated with RapidFort, a U.S.-based cybersecurity company, on the predominantly English-language deep and dark web forum Spear.

Source: Spear **Actor:** xpl0itrs

HACKTIVISM

MEDIUM **Hacktivist Group Claims DDoS Attack Targeting OVHcloud Login Portal**

On July 21, 2026, pro-Palestinian hacktivist group "313 Team" claimed on its official Telegram channel to have conducted a DDoS attack on OVHcloud's login portal.

Source: Telegram **Actor:** 313 Team

UNAUTHORIZED ACCESS CLAIMS

HIGH **RDWeb Access Allegedly Tied to U.S.-Based Real Estate Company Advertised**

On July 21, 2026, well-regarded threat actor "doZKey" advertised an auction for RDWeb access with domain user rights allegedly associated with an unnamed U.S.-based real estate company on the predominantly Russian-language deep and dark web forum Exploit.

Source: Exploit **Actor:** doZKey

HIGH **AnyDesk Access Allegedly Tied to U.S.-Based School Advertised**

On July 21, 2026, moderately credible threat actor "Ritsu08" advertised an auction for AnyDesk access with domain administrator rights allegedly associated with an unnamed U.S.-based school on the predominantly Russian-language deep and dark web forum Exploit.

Source: Exploit **Actor:** Ritsu08

HIGH **AnyDesk Access Allegedly Tied to Italy-Based Software Company Advertised**

On July 21, 2026, well-regarded threat actor "Big-Bro" advertised an auction for AnyDesk access with domain administrator rights allegedly associated with an unnamed Italy-based software company on the predominantly Russian-language deep and dark web forum Exploit.

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

HIGH **VNC Access Allegedly Tied to U.S.-Based Financial Technology Company Advertised**

On July 21, 2026, untested threat actor "yurikino" advertised to sell VNC access with administrator rights allegedly associated with an unnamed U.S.-based financial technology company on the predominantly Russian-language deep and dark web forum Exploit.

Source: Exploit **Actor:** yurikino

VULNERABILITY EXPLOITATION

HIGH **Alleged Windows Local Privilege Escalation Zero-Day Exploit Advertised**

On July 20, 2026, well-regarded threat actor "zerodayseller" advertised an alleged new Windows Local Privilege Escalation (LPE) zero-day exploit affecting Windows 11 and Windows Server 2025 on the predominantly Russian-language deep and dark web forum Exploit.

Source: Exploit **Actor:** zerodayseller

DATA BREACHES & LEAKS

HIGH **Data Allegedly Associated with Honduras-Based Individuals Advertised**

On July 20, 2026, well-regarded threat actor "betway" advertised a data set allegedly associated with Honduras-based individuals interested in luxury cars, yachts, golf, restaurants, and hotels on the predominantly Russian-language deep and dark web forum Exploit.

Source: Exploit **Actor:** betway

COLLECTED, PROCESSED DATA BREACHES

1 entries

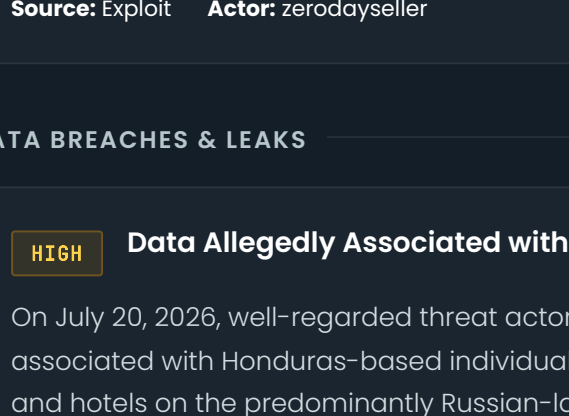
VICTIM	SOURCE	THREAT ACTOR	PROCESSED RECORDS
semitour[.]com	PwnForums	henrymartin	145.71K

PROCESSED DATA SET STATISTICS

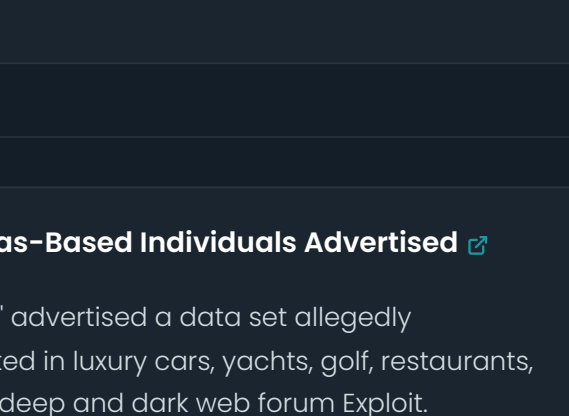
Past 4 Weeks

249.66M	1.14B	819
CAC RECORDS	BOTNET CAC RECORDS	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.