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.

July 21, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

5 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
Qilin Ransomware	City Ambulance Service
SafePay Ransomware	Cenesco
0day Syndicate Ransomware	Braincell
Qilin Ransomware	Droguería Martorani
Anubis Ransomware	Fairlife

VULNERABILITY DISCLOSURES

1 disclosure

CVE-2026-6875

Sandbox Escape and Remote Code Execution in ServiceNow AI Platform

DEEP AND DARK WEB INTELLIGENCE

8 findings

CRITICAL FINDINGS

CRITICAL **Alleged Data Associated with PappyJoe Enterprise Advertised**

On July 18, 2026, moderately credible threat actor "Kazu" advertised data allegedly associated with PappyJoe Enterprise on the predominantly English-language dark web forum DarkForums.

Source: DarkForums **Actor:** Kazu

CRITICAL **Alleged Data Associated with Just Eat Advertised**

On July 19, 2026, an untested threat actor "chuttyice" advertised data allegedly associated with Just Eat, on a predominantly English-language dark web forum DarkForums.

Source: DarkForums **Actor:** chuttyice

CRITICAL **Alleged Breach of Courts of Georgia's Data**

On July 20, 2026, moderately credible threat actor "bytestobreach" (a.k.a. bytetobreach33, bytetobreach) breached data allegedly associated with Courts of Georgia, the judicial system of the Country Georgia, on a predominantly Russian-language deep and dark web forum Exploit.

Source: Exploit **Actor:** bytestobreach

HACKTIVISM

MEDIUM **Actor Claims DDoS Attacks Targeting Airbnb**

On July 20, 2026, a pro-Palestinian threat actor group "313 Team" claimed to have conducted DDoS attacks on domain airbnb[.]com associated with Airbnb, a U.S.-based online marketplace for short-term lodging, experiences, and travel services, on their official Telegram channel.

Source: Telegram **Actor:** 313 Team

UNAUTHORIZED ACCESS CLAIMS

HIGH **Alleged VNC Access Tied to Argentina-Based Government-Owned Financial Services Company Advertised**

On July 19, 2026, an untested threat actor "yurikino" advertised to sell VNC access with administrator rights allegedly associated with an unnamed Argentina-Based government-owned financial services company, on a predominantly Russian-language deep and dark web forum Exploit.

Source: Exploit **Actor:** yurikino

HIGH **Alleged Network Access Associated with Five Distinct Companies Based in Europe and Iran Advertised**

On July 20, 2026, a moderately credible threat actor "personX" advertised to sell network access with domain administrator rights allegedly associated with five undisclosed distinct companies based in Europe and Iran, on a predominantly Russian-language deep and dark web forum Exploit.

Source: Exploit **Actor:** personX

HIGH **Alleged Network Access to Indonesian National Police Cyber Division Advertised**

On July 18, 2026, an untested threat actor "missiyaprizrak0" advertised to sell network access allegedly associated with Cyber Division of the Indonesian National Police, on a predominantly English-language deep and dark web forum PwnForums.

Source: PwnForums **Actor:** missiyaprizrak0

HIGH **Alleged VPN Access to Lifetime Brands Advertised**

On July 21, 2026, untested threat actor "Roiese" advertised VPN access allegedly associated with Lifetime Brands, on the predominantly English-language dark web forum DarkForums.

Source: DarkForums **Actor:** Roiese

MONTHLY THREAT SPOTLIGHT

June 2026 Threat Spotlight: Trends in Ransomware Operations, Zero Day Exploits, and Supply Chain Disruptions

June 2026 recorded a wide range of notable cyber activity, including ransomware, data breaches, supply chain compromises intended for mass credential harvesting, and rapid exploitation of newly disclosed vulnerabilities. Alongside steady extortion volumes, concurrent campaigns targeted open-source repositories, network edge devices, and prominent global events, pointing to a broad and active operational landscape.

COLLECTED, PROCESSED DATA BREACHES

4 entries

VICTIM	SOURCE	THREAT ACTOR	PROCESSED RECORDS
incor-med[.]ru	DarkForums	DataLeak_Archive	521
msgsports[.]com	ShinyHunters	ShinyHunters	9.8M
ouestfrance-immo[.]pro	PwnForums	ChimeraZ	6.32K
homepad[.]com	PwnForums	ChimeraZ	305.3K

PROCESSED DATASET STATISTICS

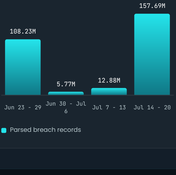
Past 4 Weeks

284.57M CAC RECORDS

1.17B BOTNET CAC RECORDS

791 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.