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 24, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

5 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
KRYBIT Ransomware	Delhi Heart and Lung Institute
Qilin Ransomware	Sunway Group
Play Ransomware	Tax-MT
Qilin Ransomware	Salida Union School District
Chaos Ransomware	Infosync Services

VULNERABILITY DISCLOSURES

2 disclosures

CVE-2026-64680
Local Privilege Escalation Vulnerability via Race Condition in Linux Kernel XFS Filesystem

CVE-2026-16232
Authentication Bypass Vulnerability in Check Point Security Management SmartConsole

DEEP AND DARK WEB INTELLIGENCE

13 findings

CRITICAL FINDINGS

CRITICAL **Disney Family**

On July 23, 2026, ZeroFox observed an update on The Gentlemen ransomware leak site targeting Disney Family, likely referring to the family descended from brothers Walt Disney and Roy O. Disney who co-founded The Walt Disney Company.

Source: The Gentlemen Ransomware

CRITICAL **Data Allegedly Tied to Saudi General Intelligence Presidency Advertised**

On July 22, 2026, threat actors (moderator of the forum) "0cx00iq" and (owner of the forum) "Resolute" independently published posts advertising data allegedly associated with the Saudi General Intelligence Presidency (GIP) on the predominantly English-language deep and dark web forum BreachForums (breached[.]su).

Source: BreachForums **Actor:** 0cx00iq, Resolute

CRITICAL **Data Allegedly Tied to Instituto Estatal Electoral y de Participación Ciudadana de Oaxaca Leaked**

On July 22, 2026, untested threat actor "Arcepah" claimed to have breached data associated with Instituto Estatal Electoral y de Participación Ciudadana de Oaxaca on the predominantly English-language deep and dark web forum BreachForums(breached[.]su.)

Source: BreachForums **Actor:** Arcepah

CRITICAL **30 New Victims Listed**

On July 23, 2026, ZeroFox observed that The Gentlemen ransomware group listed 30 new victims on their leak site.

Source: The Gentlemen Ransomware

UNAUTHORIZED ACCESS CLAIMS

HIGH **Network Access Allegedly Tied to Global Legal Services Company Advertised**

On July 22, 2026, untested threat actor "shrouded_fang" advertised network access with domain administrator rights allegedly associated with an unnamed global legal services company on the predominantly Russian-language deep and dark web forum Exploit.

Source: Exploit **Actor:** shrouded_fang

HIGH **RDP Access Allegedly Tied to Argentina-Based Real Estate Company Advertised**

On July 23, 2026, well-regarded threat actor "BURBERRY" advertised an auction for RDP access with domain administrator rights on the predominantly Russian-language deep and dark web forum Exploit.

Source: Exploit **Actor:** BURBERRY

HIGH **VNC/HVNC Access Allegedly Tied to U.S.-Based Public School District Advertised**

On July 23, 2026, untested threat actor "techno" advertised remote access to an unnamed U.S.-based public school district, on the predominantly Russian-language deep and dark web forum RehubCom.

Source: RehubCom **Actor:** techno

DATA BREACHES & LEAKS

HIGH **Data Allegedly Tied to ModelsLab Advertised**

On July 22, 2026, well-regarded threat actor "betway" advertised a dataset allegedly associated with a U.S.-based LLM API development company ModelsLab on the predominantly Russian-language deep and dark web forum Exploit.

Source: Exploit **Actor:** betway

HIGH **Data Allegedly Associated with South Korea-Based Financial Services Company Advertised**

On July 22, 2026, well-regarded threat actor "Vlkln9" advertised a dataset allegedly associated with an unnamed South Korea-based financial services company on the predominantly Russian-language deep and dark web forum Exploit.

Source: Exploit **Actor:** Vlkln9

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

On July 22, 2026, moderately credible threat actor "Galaher" advertised a dataset allegedly associated with Netherlands-based individuals on the predominantly Russian-language deep and dark web forum XSS.

Source: XSS **Actor:** Galaher

HIGH **Actor Claims Breach of PokemonGym User Data**

On July 23, 2026, well-reputed threat actor "888" alleged leaking data associated with PokemonGym, a Pokémon-themed online Role-Playing Game (RPG) platform operating from the Netherlands on the predominantly English-language deep and dark web forum PwnForums.

Source: PwnForums **Actor:** 888

HACKTIVISM

HIGH **Actor Claims DDoS Attack Targeting Microsoft 365 Services**

On July 23, 2026, a pro-Palestinian threat actor group "313 Team" claimed to have conducted DDoS attack targeting Microsoft 365, alleging that the operation resulted in worldwide service outages affecting Microsoft Azure, Microsoft SharePoint and other products.

Source: Telegram **Actor:** 313 Team

NEW LEAKSITES, MARKETPLACES, FORUMS

HIGH **New Ransomware Leak Site Emerges**

On July 24, 2026, ZeroFox observed a new ransomware leak site named "DarkMatter." As of this report, the site lists no victims and is accessible via a Tor hidden service address and 15 mirror links.

Source: Leak Site **Actor:** DarkMatter

COLLECTED, PROCESSED DATA BREACHES

4 entries

VICTIM	SOURCE	THREAT ACTOR	PROCESSED RECORDS
barqun[.]com	BreachForums	Tanaka	4.1K
france-terrain[.]com	PwnForums	ChimeraZ	2.94K
96k User Pass "leakbase.io"	--	--	96.18K
Broker Forex Breach Exposure Of 1,003 Data Entries	LeakBase	stride	982

PROCESSED DATA SET STATISTICS

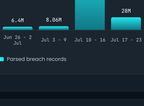
Past 4 Weeks

192.34M CAC RECORDS

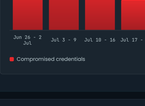
1.04B BOTNET CAC RECORDS

708 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.