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.

August 13, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

6 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
SETTRA Ransomware	Flowco
SETTRA Ransomware	Advanced Tax Solutions
Storm Ransomware	Indiana University Health
Storm Ransomware	Liberty Health
Dark Project	Labpharma
Dark Project	Mile Bluff Medical Center

VULNERABILITY DISCLOSURES

3 disclosures

CVE-2026-55040
Authentication Bypass Vulnerability in Microsoft SharePoint Server

CVE-2026-58231
Improper Authorization Vulnerability in SAP Commerce Cloud (Data Hub Adapter)

CVE-2026-59310
Directory Traversal Vulnerability in VMware vCenter Server

DEEP AND DARK WEB INTELLIGENCE

9 findings

CRITICAL FINDINGS

CRITICAL **42 Previously Redacted Entities Disclosed, Alongside 2 New Entities**

On August 13, 2026, ZeroFox observed that the Clop ransomware group disclosed the 42 previously redacted victims (listed on August 5, 2026), alongside two newly added victims, bringing the total number of newly disclosed victims to 44.

Source: Leak Site **Actor:** Clop Ransomware

CRITICAL **Threat Actor Claims Unauthorized Access to Ukraine-Based Water Treatment Facility SCADA System (NoName057(16))**

On August 12, 2026, a pro-Russian threat group "NoName057(16)" claimed to have gained unauthorized access to an unnamed industrial control system (ICS/SCADA) of a water treatment facility in Ukraine.

Source: Telegram

NEW LEAKSITES, MARKETPLACES, FORUMS

CRITICAL **New Data Leak Site Emerges**

On August 12, 2026, ZeroFox observed a new data leak site named "Ethics." As of this report, the site lists three entities and a redacted entity as its victims, and is accessible via the following Tor hidden address: hxxp://ethics67vxjomvlcugjovv4fc3g6ru5tpwotg533d4j3uf2btmnndead.onion

Source: Leak Site **Actor:** Ethics

CRITICAL **New Ransomware Leak Site Emerges**

On August 13, 2026, ZeroFox observed a new ransomware leak site operating under the name "MAJINAHANASHI". As of this report, the site lists fifteen entities, and is accessible via the following Tor hidden address: hxxp://ithicpjqc7gkn5eq3epxndc2uig3yngvcbdya4u3m3byjod5ikm4yuwqd[.]onion/#blog

Source: Leak Site **Actor:** MAJINAHANASHI

HIGH **New Ransomware Leak Site Emerges**

On August 13, 2026, ZeroFox observed a new ransomware leak site operating under the name "EMPERADOR." As of this report, the leak site lists one entity and is accessible via the following Tor hidden address:hXXp://emprdr4p7iwlhpky33tswt3k2qdeljyjcdpoysabudmmrz4z32laexad[.]onion

Source: Leak Site **Actor:** EMPERADOR

HIGH **New Ransomware Leak Site Emerges**

On August 13, 2026, ZeroFox observed a new ransomware leak site operating under the name "Eclipse." As of this report, the site does not list any entities as targets and is accessible via the following Tor hidden address:hxxp://eclipse4g5kxfwsvpu4qx5sdcnrjii6gxl5gt67bucjlgt35g7akvjoid.onion

Source: Leak Site **Actor:** Eclipse

UNAUTHORIZED ACCESS CLAIMS

HIGH **VPN Access Allegedly Tied to U.S.-Based Energy, Utilities and Waste Company Advertised**

On August 12, 2026, moderately credible threat actor "blink" advertised an auction for VPN access with domain user rights allegedly tied to an unnamed U.S.-based energy, utilities and waste company on the predominantly Russian-language DDW forum Exploit.

Source: Exploit **Actor:** blink

HIGH **RDWeb Access Allegedly Tied to U.S.-Based Law Firm Advertised**

On August 12, 2026, well-known threat actor "Big-Bro" advertised an auction for RDWeb access with domain user rights allegedly tied to an unnamed U.S.-based law firm on Exploit.

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

HIGH **AnyDesk Access Allegedly Tied to State Psychiatric Hospital Based in Latin America Advertised**

On August 12, 2026, moderately credible threat actor "crypmans" advertised an auction for AnyDesk access with domain administrator rights allegedly tied to an unnamed state psychiatric hospital based in Latin America on Exploit.

Source: Exploit **Actor:** crypmans

COLLECTED, PROCESSED DATA BREACHES

4 entries

VICTIM	SOURCE	THREAT ACTOR	PROCESSED RECORDS
playground.wellbees[.]com	PwnForums	nest0r	18.58K
ffft[.]com	PwnForums	efraim	8.28K
Hellfest	PwnForums	Saturne	1.04K
Quality Woven Labels	PwnForums	nest0r	10.55K

PROCESSED DATA SET STATISTICS

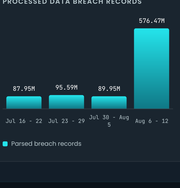
Past 4 Weeks

849.96M CAC RECORDS

846.97M BOTNET CAC RECORDS

934 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.