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 5, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

6 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
Everest Ransomware	Keysight Technologies
The Gentlemen Ransomware	Câmara Municipal da Serra
KRYBIT Ransomware	Country Motors
Anubis Ransomware	Cameron Regional Medical Center
Aur0ra Ransomware	US Installation Group
SafePay Ransomware	CPU Softwarehouse

VULNERABILITY DISCLOSURES

1 disclosure

CVE-2026-9198

Critical Code Injection Vulnerability in IBM Langflow OSS

DEEP AND DARK WEB INTELLIGENCE

9 findings

CRITICAL FINDINGS

CRITICAL **Sophos VPN Access Allegedly Associated with Abu Dhabi National Energy Company Advertised**

On August 5, 2026, untested threat actor "impotent4000" advertised an auction for VPN access allegedly associated with Abu Dhabi National Energy Company, United Arab Emirates on the predominantly Russian-language deep and dark web (DDW) forum Exploit.

Source: Exploit **Actor:** impotent4000

CRITICAL **Data Allegedly Associated with Intermarché Advertised**

On August 5, 2026, moderately credible threat actor advertised data allegedly exfiltrated from Intermarché, a France-based supermarket chain on the predominantly English-language DDW forum PwnForums.

Source: PwnForums **Actor:** ZeroBytes

CRITICAL **Domain Admin Access Allegedly Associated with U.S.-Based Pharmaceutical Company Advertised**

On August 5, 2026, untested threat actor "Dummy" advertised an auction for network access with domain administrator rights allegedly associated with an unnamed U.S.-based pharmaceutical company on Exploit.

Source: Exploit **Actor:** Dummy

CRITICAL **Leak Site Lists 42 New Unidentified Victims**

On August 5, 2026, ZeroFox observed that the Clop ransomware group listed 42 new victims, with their names redacted, on its leak site over the past 24 hours.

Source: Clop Ransomware

UNAUTHORIZED ACCESS CLAIMS

HIGH **FortiGate and SSH Access Allegedly Associated with UAE-Based Motor Vehicle Manufacturing Company Advertised**

On August 4, 2026, untested threat actor "SCP-2013" advertised FortiGate and SSH access allegedly associated with an unnamed UAE-based motor vehicle manufacturing company on Exploit.

Source: Exploit **Actor:** SCP-2013

HIGH **FortiGate and SSH Access Allegedly Associated with Turkey-Based Retail Company Advertised**

On August 4, 2026, untested threat actor "SCP-2013" advertised FortiGate and SSH access with Super_Admin rights allegedly associated with an unnamed Turkey-based retail company on Exploit.

Source: Exploit **Actor:** SCP-2013

HIGH **Fortinet SSL VPN Access Allegedly Associated with Germany-Based Municipality Advertised**

On August 3, 2026, moderately credible threat actor "barak" advertised Fortinet SSL VPN access with domain administrator rights allegedly associated with an unnamed Germany-based municipality on the predominantly Russian-language deep web forum DUTY-FREE.

Source: DUTY-FREE **Actor:** barak

HIGH **Fortinet VPN Access Allegedly Associated with Argentina-Based Government Entity Advertised**

On August 3, 2026, untested threat actor "casanova" advertised Fortinet VPN access allegedly associated with an unnamed Argentina-based government entity on the predominantly English-language DDW forum BreachForums (breached[.]su).

Source: BreachForums **Actor:** casanova

NEW LEAKSITES, MARKETPLACES, FORUMS

HIGH **New Ransomware Leak Site Emerges**

On August 4, 2026, ZeroFox observed a new ransomware leak site named "OROVA". As of this report, the leak site lists 24 victims and is accessible via the following onion address: hxxp://mll5ddmdzgiq2siv3qnocmmqyiigfpajtc663xtf32qtp6weycyx2hyd[.]onion/

Source: Leak Site **Actor:** OROVA

PROCESSED DATA SET STATISTICS

Past 4 Weeks

364.2M	859.19M	867
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.