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 6, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

6 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
Panzer Ransomware	Universitas Surakarta
OROVA Ransomware	Texas Medical Screening
Play Ransomware	First Tek
Gunra Ransomware	All Cosmos Bio-Tech
Qilin Ransomware	Service Electric Cablevision
Chaos Ransomware	Healthcare Highways

VULNERABILITY DISCLOSURES

1 disclosure

CVE-2026-59774
Critical Unauthenticated Arbitrary File Read Vulnerability in Gitea

DEEP AND DARK WEB INTELLIGENCE

10 findings

CRITICAL FINDINGS

CRITICAL **Data Allegedly Associated with SS&C Black Diamond Wealth Solutions Advertised**

On August 6, 2026, untested threat actor "renn" advertised data allegedly associated with SS&C Black Diamond Wealth Solutions on the predominantly Russian-language deep and dark web (DDW) forum Exploit.

Source: Exploit **Actor:** renn

CRITICAL **Data Allegedly Associated with CARMA Advertised**

On August 6, 2026, moderately credible threat actor "2019" advertised data allegedly associated with CARMA on the predominantly English-language DDW forum PwnForums.

Source: PwnForums **Actor:** 2019

VULNERABILITY EXPLOITATION

CRITICAL **Alleged Zero-Day Vulnerability Affecting FortiManager Advertised**

On August 4, 2026, untested threat actor "hello_enenen" advertised an alleged zero-day vulnerability affecting FortiManager on Exploit.

Source: Exploit **Actor:** hello_enenen

CRITICAL **Two Alleged Unauthenticated SQL Injection Zero-Day Vulnerabilities Affecting myBB Plugins Advertised**

On August 3, 2026, threat actor "diencracked" advertised two alleged unauthenticated SQL injection (SQLi) zero-day vulnerabilities affecting commonly used myBB plugins, on the predominantly English-language DDW forum BreachForums (breached[.]su).

Source: BreachForums **Actor:** diencracked

UNAUTHORIZED ACCESS CLAIMS

HIGH **VPN Access Allegedly Associated with UK-Based Cloud-Based Provider Advertised**

On August 5, 2026, moderately credible threat actor "Florence" advertised VPN access allegedly associated with an unnamed UK-based Cloud service provider on PwnForums.

Source: PwnForums **Actor:** Florence

HIGH **Network Access Allegedly Associated with Multiple Thailand-Based Government Entities Advertised**

On August 5, 2026, untested threat actor "impotent4000" advertised an auction for network access allegedly associated with multiple unnamed Thailand-based government entities on Exploit.

Source: Exploit **Actor:** impotent4000

HACKTIVISM

HIGH **Actor Claims DDoS Attack Targeting Narayana Health and India Healthcare Tourism**

On August 5, 2026, threat group Infrastructure Destruction Squad (IDS) claimed to have conducted DDoS attacks on domains associated with Narayana Health and India Healthcare Tourism, on their official Telegram channel.

Source: Telegram **Actor:** Infrastructure Destruction Squad

HIGH **Alleged Automated Breach Tool "BLACKNET-CORPORATE-BREACH-HUNTER" Advertised**

On 5 August 2026, a threat group known as 'Infrastructure Destruction Squad' (IDS) advertised an automated exploitation and data exfiltration tool named 'BLACKNET-CORPORATE-BREACH-HUNTER' on their official Telegram channel.

Source: Telegram **Actor:** Infrastructure Destruction Squad

NEW LEAKSITES, MARKETPLACES, FORUMS

CRITICAL **New Ransomware Leak Site Emerges**

On August 6, 2026, ZeroFox observed a new leak site named "Panzer". As of this report, the site lists two victims and is accessible via the following Tor hidden service address: pnzruro7syvvvehx5mpo2fhzi4jftgquynsqf3vy5x3no57yp2iz4nyad[.]onion.

Source: Leak Site **Actor:** Panzer

CRITICAL **New Data Leak Site Emerges**

On August 6, 2026, ZeroFox observed a new data leak site named "Dark Project". As of this report, the site lists 19 victims all of which operate in different sectors based out of United States, Mexico and Canada. The leak site is accessible through the following Tor hidden service address: darkpm3d3udnhpuxknsrhft3371ilrz5tenhgkrxge5hxqe46pkbrwid[.]onion.

Source: Leak Site **Actor:** Dark Project

COLLECTED, PROCESSED DATA BREACHES

10 entries

VICTIM	SOURCE	THREAT ACTOR	PROCESSED RECORDS
evo[.]gg	PwnForums	ZeroBytes	70.69K
puppyfinder[.]com	PwnForums	herefortheoofs	154.97K
rangee[.]com	PwnForums	Sophia	3.38K
mcs[.]tech-in-order[.]com	PwnForums	MirrorShell	1.44K
xpayrience[.]com	PwnForums	ChimeraZ	465.88K
rezofed[.]centres-sociaux[.]fr	PwnForums	misere	5.87K
motoport-haendler[.]de	PwnForums	Sophia	876
kosc-telecom[.]fr	PwnForums	ChimeraZ	638
humanizerpro[.]ai	PwnForums	Emzywemzy	65.08K
bservice[.]de	PwnForums	Sophia	2.81K

PROCESSED DATA SET STATISTICS

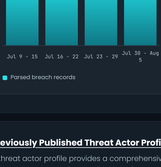
Past 4 Weeks

364.15M CAC RECORDS

943.45M BOTNET CAC RECORDS

902 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.