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 21, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

6 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
Dire Wolf Ransomware	PayUp
LockBit 5.0 Ransomware	U.S. Bank
Insomnia	Aurora Health Management
INTERLOCK Ransomware	Southeastern Oklahoma State University
Akira Ransomware	Ericksen Krentel
Qilin Ransomware	Penlink

VULNERABILITY DISCLOSURES

2 disclosures

CVE-2026-73570
OS Command Injection Vulnerability in Zimbra Collaboration Suite

CVE-2026-19490
Authentication Bypass Vulnerability in Citrix NetScaler ADC and NetScaler Gateway

DEEP AND DARK WEB INTELLIGENCE

9 findings

CRITICAL FINDINGS

CRITICAL **Threat Actor Claims Data Breach Associated with Pratt & Whitney**

On August 20, 2026, threat group Infrastructure Destruction Squad (IDS) claimed to have compromised Pratt & Whitney and exfiltrated sensitive data, on their official Telegram channel.

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

CRITICAL **Data Allegedly Associated with Kimber America Advertised**

On August 18, 2026, moderately credible threat actor "iProfessor" advertised a data breach allegedly tied to Kimber America, a U.S-based firearms manufacturer, on the predominantly English-language DDW forum PwnForums.

Source: PwnForums **Actor:** iProfessor

CRITICAL **Data Allegedly Associated with Sports 2000 Leaked**

On August 19, 2026, moderately credible threat actor "ZeroBytes" leaked data allegedly associated with Sport 2000 on PwnForums.

Source: PwnForums **Actor:** ZeroBytes

HIGH **13 New Victims Listed**

On August 21, 2026, ZeroFox observed that the Dire Wolf ransomware group listed 13 new victims on their leak site.

Source: Dire Wolf Ransomware

NEW LEAKSITES, MARKETPLACES, FORUMS

CRITICAL **New Ransomware Leak Site Emerges**

On August 21, 2026, ZeroFox observed a new leak site claiming to be a ransomware group, operating under the name "DYSPHORIA". As of this report, the leak site lists seven entities as victims and is accessible via the following dark web address: hXxp://y3mavelwszbnrzlufbbbenx74cvrdcsf72nxuqxv7ppdmmqzffazid[.]onion/

Source: Leak Site **Actor:** DYSPHORIA

CRITICAL **New Data Leak Site Emerges**

On August 21, 2026, ZeroFox observed a new data leak site operating under the name "Sovcali." As of this report, the leak site listed one entity as a victim, and is accessible via the following dark web address:hxxp://z3mojpjnxt5tgqvu4wgosihl7pxvrcbyjcgquw2bwkyye5gwbhnf4kqd[.]onion/

Source: Leak Site **Actor:** Sovcali

UNAUTHORIZED ACCESS CLAIMS

CRITICAL **Alleged Packagist Developer Account Access Advertised**

On August 20, 2026, moderately credible threat actor "bo4arov" advertised access to undisclosed developer account on Packagist (packagist[.]org) on the predominantly Russian-language DDW forum Exploit.

Source: Exploit **Actor:** bo4arov

HIGH **Network Access Allegedly Tied to France-Based Real Estate Company Advertised**

On August 19, 2026, untested threat actor "_H_T_P_0101" advertised an auction for network access with local administrator rights allegedly tied to an unnamed France-based real estate company on Exploit.

Source: Exploit **Actor:** _H_T_P_0101

HIGH **Web Panel Access Allegedly Tied to Undisclosed Gambling Platform Advertised**

On August 19, 2026, untested threat actor "Capitalist" advertised web panel access with administrator rights allegedly tied to an undisclosed gambling platform on Exploit.

Source: Exploit **Actor:** Capitalist

COLLECTED, PROCESSED DATA BREACHES

5 entries

VICTIM	SOURCE	THREAT ACTOR	PROCESSED RECORDS
allstate[.]com	ExfilSquad	ExfilSquad	647.68K
gamification.prestashop[.]com	DarkForums	Sophia01	565
resaclick[.]net	PwnForums	weykofa	10.13K
learningcrypto[.]com	PwnForums	seraphims	8.29K
interieur.gouv[.]fr	PwnForums	misere	111.51K

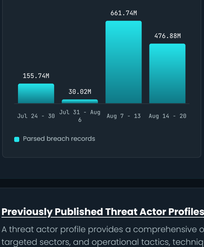
PROCESSED DATA SET STATISTICS

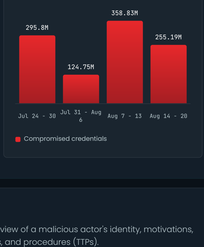
Past 4 Weeks

1.32B CAC RECORDS

1.03B BOTNET CAC RECORDS

1.01K RANSOMWARE & DIGITAL EXTORTION





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.