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.

September 8, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

7 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
ShinyHunters	State of Florida DMV
CHAOS Ransomware	Evergen
Qilin Ransomware	Philippine Ports Authority
The Gentlemen Ransomware	Zdrowit
AurOra Ransomware	Metrea
BLACKLOCKS	Kwang Myung
Dire Wolf Ransomware	Wolfram Research

VULNERABILITY DISCLOSURES

3 disclosures

CVE-2026-86218
Static Code Injection Vulnerability in N-able N-central

CVE-2026-67276
SSH Authentication Bypass Vulnerability in MikroTik RouterOS

CVE-2026-86060
SSH Argument Injection Privilege Escalation Vulnerability in MikroTik RouterOS

DEEP AND DARK WEB INTELLIGENCE

9 findings

CRITICAL FINDINGS

CRITICAL **Actor Claims DDoS Attack Targeting King Abdulaziz International Airport**

On September 8, 2026, a pro-Palestinian threat actor group "313 Team" claimed, via its Telegram channel, to have carried out a Distributed Denial-of-Service (DDoS) attack against King Abdulaziz International Airport.

Source: Telegram **Actor:** 313 Team

CRITICAL **Alleged Magneto 2 RCE Zero-Day Advertised**

On September 8, 2026, well reputed threat actor "TylerDurden" advertised an alleged zero-day exploit associated with Magneto 2, a U.S.-based e-commerce platform, on Exploit.

Source: Exploit **Actor:** TylerDurden

CRITICAL **Data Allegedly Associated with Condé Nast Advertised**

On September 7, 2026, untested threat actor "luv" advertised data allegedly associated with U.S.-based mass media company Condé Nast and its affiliated brands, on Exploit.

Source: Exploit **Actor:** luv

VULNERABILITY EXPLOITATION

HIGH **Alleged Hyper-V VM Escape Zero-Day Advertised**

On September 8, 2026, moderately credible threat actor "btc1837" advertised Hyper-V zero-day exploit on the predominantly Russian-language DDW forum Exploit.

Source: Exploit **Actor:** btc1837

DATA BREACHES & LEAKS

HIGH **Alleged US Life Insurance Portfolio Dataset Associated with Infineo Advertised**

On September 5, 2026, untested threat actor "cyberdluffy" advertised alleged US life insurance portfolio dataset on the predominantly Russian-language DDW forum XSS.

Source: XSS **Actor:** cyberdluffy

HIGH **Data Allegedly Associated with U.S.-Based Company iClaim Advertised**

On September 4, 2026, well-regarded threat actor "betway" advertised data allegedly associated with iClaim, a U.S.-based revenue cycle management company, on Exploit.

Source: Exploit **Actor:** betway

CRITICAL **Data Allegedly Associated with Hospital Alemán and OSDEPYM Leaked**

On September 7, 2026, untested threat actor "NeonBreach" leaked data allegedly associated with Hospital Alemán (an Argentina-based non-profit hospital) and OSDEPYM (an Argentina-based health insurance provider) on PwnForums.

Source: PwnForums **Actor:** NeonBreach

UNAUTHORIZED ACCESS CLAIMS

HIGH **Network Access Allegedly Tied to U.S.-Based Software Company Advertised**

On September 7, 2026, well-regarded threat actor "888" advertised network access allegedly associated with an unnamed U.S.-based software company on the predominantly English-language DDW forum PwnForums.

Source: PwnForums **Actor:** 888

HIGH **Network Access Allegedly Tied to Vienna-Based Government Entity Advertised**

On September 7, 2026, untested threat actor "br3ach3d" advertised network access to internal hosts along Active Directory allegedly associated with an unnamed Vienna-based government entity, on the predominantly English-language DDW forum DarkForums.

Source: DarkForums **Actor:** br3ach3d

COLLECTED, PROCESSED DATA BREACHES

4 entries

VICTIM	SOURCE	THREAT ACTOR	PROCESSED RECORDS
cropwise[.]com	PwnForums	henrymartin	789
purevents[.]fr	PwnForums	Sophia	3.28K
morgansindall[.]com	PwnForums	PersistentMan	9.26K
acopa-immobilier[.]fr	PwnForums	0x5ec	8.43K

PROCESSED DATA SET STATISTICS

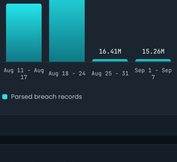
Past 4 Weeks

873.02M
CAC RECORDS

1.17B
BOTNET CAC RECORDS

996
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.