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 10, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

6 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
The Gentlemen Ransomware	Air Canada
Qilin Ransomware	Jet Specialty
Play Ransomware	Red Star Oil
Play Ransomware	GT Distributors
Storm Ransomware	Technology Dynamics
Anubis Ransomware	Gellibrand Support Services

VULNERABILITY DISCLOSURES

3 disclosures

CVE-2026-67401
SQL Injection Vulnerability in WebPros cPanel EmailTrack

CVE-2026-87491
Out-of-Bounds Write Vulnerability in Google Chrome V8

CVE-2026-44756
Memory Corruption Vulnerability in SAP Kernel Extended Passport Processing

DEEP AND DARK WEB INTELLIGENCE

7 findings

CRITICAL FINDINGS

CRITICAL **Alleged Windows Defender Zero-Day Patch Bypass**

On September 8, 2026, GitHub user "Nightmare-Eclipse" publicly released an alleged proof-of-concept (PoC) exploit code for a new Microsoft Defender technique dubbed "ShieldCrash."

Source: ShieldCrash **Actor:** Nightmare-Eclipse

DATA BREACHES & LEAKS

CRITICAL **Data Allegedly Associated with Rezcomm Advertised**

On September 9, 2026, moderately credible threat actor "Vespiary" advertised data allegedly associated with Rezcomm on the predominantly Russian-language DDW forum Exploit.

Source: Exploit **Actor:** Vespiary

HIGH **Data Allegedly Associated with Panama-Based Platforms reposervicespty[.]com, locatorsoft[.]com and pillatupieza[.]com Advertised**

On September 9, 2026, moderately credible threat actor "Vespiary" advertised data allegedly associated with Panama-based platforms reposervicespty[.]com, locatorsoft[.]com and pillatupieza[.]com, on Exploit.

Source: Exploit **Actor:** Vespiary

HIGH **Data Allegedly Associated with India-Based Company SetuBridge Solutions Advertised**

On September 9, 2026, moderately credible threat actor "Vespiary" advertised data allegedly associated with SetuBridge Solutions, an India-based company assisting entrepreneurs, startups, and small and medium-sized businesses with obtaining government subsidies, business development, and other consulting support, on Exploit.

Source: Exploit **Actor:** Vespiary

HIGH **Data Allegedly Associated with France-Based Individuals Advertised**

On September 8, 2026, well-regarded threat actor "betway" advertised data allegedly associated with France-based customers interested in luxury cars, yachts, golf, restaurants, and hotels on Exploit.

Source: Exploit **Actor:** betway

UNAUTHORIZED ACCESS CLAIMS

HIGH **VPN Access Allegedly Tied to India-Based Financial Services Company Advertised**

On September 8, 2026, moderately credible threat actor "Elnoir" advertised an auction for VPN access with domain administrator rights allegedly associated with an unnamed India-based financial services company on Exploit.

Source: Exploit **Actor:** Elnoir

HIGH **Fortinet Access Allegedly Tied to France-Based Car Truck Rental Consumer Services Company Advertised**

On September 8, 2026, well-known threat actor "Big-Bro" advertised an auction for Fortinet access with domain user rights allegedly associated with an unnamed France-based car truck rental consumer services company on Exploit.

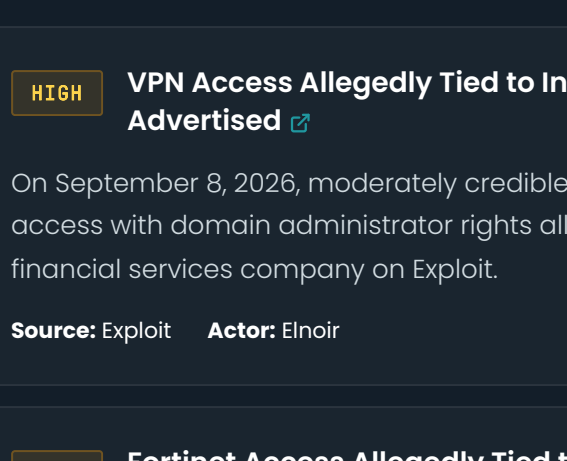
Source: Exploit **Actor:** Big-Bro

PROCESSED DATA SET STATISTICS

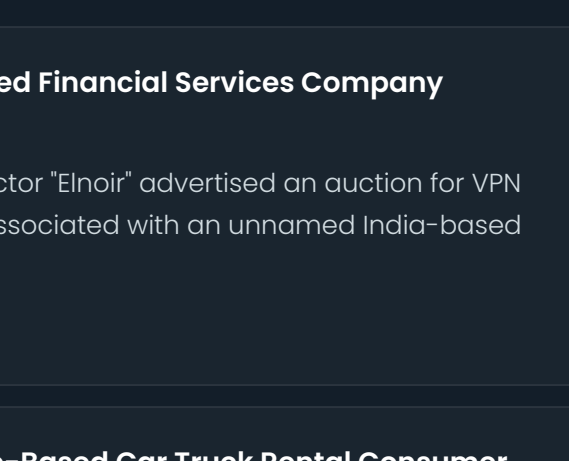
Past 4 Weeks

638.8M	1.31B	1.08K
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.