

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 23, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

7 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
Settra Ransomware	Quantum Marketing Group
Titan Ransomware	Grupo Hospifar
Storm Ransomware	Manroc Developments
Storm Ransomware	Truecore Behavioral Solutions
Metaencryptor Ransomware	Flex
Anubis Ransomware	Summa Gold
The gentlemen Ransomware	D.W. McMillan Memorial Hospital

VULNERABILITY DISCLOSURES

6 disclosures

CVE-2026-86296
Stack-Based Buffer Overflow Vulnerability in D-Link DIR-822A
CVE-2026-93616
Path Traversal and Arbitrary Script Execution Vulnerability
CVE-2026-7273
Stack-Based Buffer Overflow Vulnerability in Zyxel GS1900 Series Switches
CVE-2026-93485
Unauthenticated Stored Cross-Site Scripting Vulnerability in Automattic WordPress
CVE-2026-89775
Guest-to-Host VM Escape Vulnerability in Linux Kernel KVM (arm64)
CVE-2026-65660
Code Injection Vulnerability in Microsoft SharePoint Server

DEEP AND DARK WEB INTELLIGENCE

8 findings

CRITICAL FINDINGS

CRITICAL

Retaliation and Extortion Threat Targeting Federal Bureau of Investigation

[Link](#)

On September 23, 2026, ZeroFox observed an update on the ShinyHunters leak site targeting the Federal Bureau of Investigation (FBI), United States.

Source: Leak Site

DATA BREACHES & LEAKS

HIGH

Data Allegedly Associated with OnTheHouse Advertised (bleedingout)

[Link](#)

On September 22, 2026, moderately credible threat actor "bleedingout" advertised data allegedly associated with OnTheHouse, on the predominantly Russian-language DDW forum Exploit.

Source: Exploit **Actor:** bleedingout

HIGH

Data Allegedly Associated with France-Based Company Réso Advertised (caustic)

[Link](#)

On September 21, 2026, well-regarded threat actor "caustic" advertised an auction for a 675 GB dataset containing sensitive information allegedly associated with Réso a France-based construction management company on Exploit.

Source: Exploit **Actor:** caustic

VULNERABILITY EXPLOITATION

HIGH

Alleged Windows Privilege Escalation Exploit Advertised (QatarRat)

[Link](#)

On September 23, 2026, moderately credible threat actor "QatarRat" advertised an alleged Windows privilege escalation exploit for CVE-2026-85880, an Advanced Local Procedure Call (ALPC) buffer overflow vulnerability, on Exploit.

Source: Exploit **Actor:** qatarrat

HIGH

Alleged PrestaShop 1.7.x – 8.x Critical Admin Access Bypass Zero-Day Advertised (Snownine)

[Link](#)

On September 22, 2026, negative reputation threat actor "Snownine" advertised an auction for an alleged critical zero-day vulnerability affecting PrestaShop versions 1.7.x through 8.x on Exploit.

Source: Exploit **Actor:** snownine

UNAUTHORIZED ACCESS CLAIMS

HIGH

SSH Access Allegedly Tied to India-Based Energy Company Advertised (Executive)

[Link](#)

On September 20, 2026, untested threat actor "Executive" advertised SSH access allegedly associated with an unnamed India-based energy company on the predominantly Russian-language dark web forum RehubCom.

Source: Rehubcom **Actor:** executive

HIGH

Fortinet Access Allegedly Tied to Philippines-Based Energy Company Advertised (Ritsu08)

[Link](#)

On September 21, 2026, well-regarded threat actor "Ritsu08" advertised an auction for Fortinet access with domain user rights allegedly associated with an unnamed Philippines-based energy company on Exploit.

Source: Exploit **Actor:** ritsu08

THREAT ACTOR PROFILE

CRITICAL

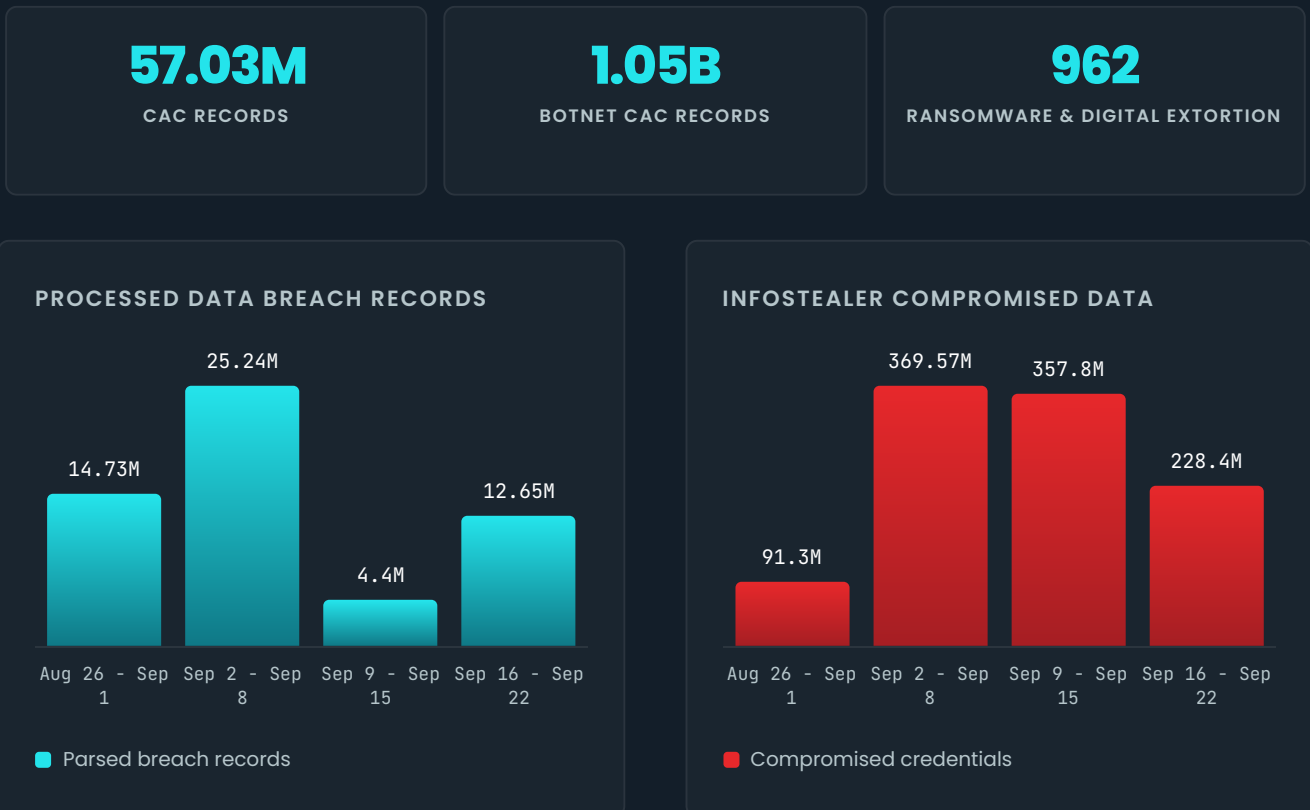
APT28 (Fancy Bear)

[Link](#)

APT28 is a Russian military intelligence operation run by GRU Unit 26165, and one of the longest-running state intrusion sets on record. Confirmed activity spans more than two decades and continues today. Its mission is strategic collection and influence, not profit: credential theft, exfiltration of sensitive communications, and hack-and-leak operations that serve Russian foreign policy objectives.

PROCESSED DATA SET STATISTICS

Past 4 Weeks



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.