

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.

October 1, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

4 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
M3RX Ransomware	Chouhan CPA
Brain Cipher Ransomware	Trailer Bridge
Brain Cipher Ransomware	Northeast Rehabilitation Hospital Network
INTERLOCK Ransomware	Blaise C. Bender

VULNERABILITY DISCLOSURES

4 disclosures

[CVE-2026-102490](#)

Local Privilege Escalation Vulnerability in Zammad

[CVE-2026-76504](#)

Authentication Bypass Vulnerability in Cisco Catalyst SD-WAN Manager

[CVE-2026-84411](#)

Integer Underflow Vulnerability in MikroTik RouterOS

[CVE-2026-102489](#)

Session Hijack Vulnerability Leading to Remote Code Execution in Zammad

DEEP AND DARK WEB INTELLIGENCE

9 findings

CRITICAL FINDINGS

CRITICAL

Data Allegedly Tied to SoLo Funds Advertised

On September 30, 2026, untested threat actor "tiger" advertised a data set containing over 1 million records associated with SoLo Funds on a predominantly Russian-language DDW forum Exploit.

Source: Exploit **Actor:** tiger

CRITICAL

CVE-2025-29927 Scan Results Allegedly Targeting New York University Subdomain Advertised

On September 30, 2026, moderately credible threat actor "ShadowByt3S" advertised a vulnerability scan result allegedly targeting a undisclosed New York University (NYU) subdomain on a predominantly English-language DDW forum PwnForums.

Source: PwnForums **Actor:** ShadowByt3S

HIGH

Alleged Sale of 400,000+ UK and Ireland Institutional Email Contacts

On September 30, 2026, untested threat actor "ikki" advertised a data set allegedly containing over 400,000 institutional email contacts from United Kingdom and Ireland-based organizations on Exploit.

Source: Exploit **Actor:** ikki

UNAUTHORIZED ACCESS CLAIMS

HIGH

Citrix Access Allegedly Tied to U.S.-Based Government Entity Advertised

On September 30, 2026, untested threat actor "G0ID3N" advertised Citrix access with domain user rights allegedly associated with an unnamed U.S.-based government entity on a predominantly Russian-language DDW forum TlerOne.

Source: TlerOne **Actor:** G0ID3N

HIGH

SSH Access Allegedly Tied to U.S.-Based Telecommunications Company Advertised

On September 29, 2026, untested threat actor "darex" advertised SSH access allegedly associated with an unnamed U.S.-based telecommunications company on TlerOne.

Source: TlerOne **Actor:** darex

VULNERABILITY EXPLOITATION

MEDIUM

Undisclosed Alleged Zero-Day RCE Advertised

On September 30, 2026, untested threat actor "audi1337" advertised an alleged zero-day remote code execution (RCE) exploit for an unnamed software on Exploit.

Source: Exploit **Actor:** audi1337

MEDIUM

Alleged Zero-Day LPE for Windows Advertised

On September 30, 2026, untested threat actor "Win_Ex" advertised an alleged zero-day Local Privilege Escalation (LPE) exploit targeting a vulnerability in the Windows kernel on Exploit.

Source: Exploit **Actor:** Win_Ex

MEDIUM

Alleged Tripaul RAT Loader Advertised

On September 30, 2026, untested threat actor "tripaul" advertised an alleged "Tripaul RAT Loader" on Exploit.

Source: Exploit **Actor:** tripaul

NEW LEAKSITES, MARKETPLACES, FORUMS

HIGH

New Data Leak Site Emerges

On October 1, 2026, ZeroFox observed a new leak site named "UWAYS QARANI," operated by an untested hacktivist group of the same name.

Source: Leak Site **Actor:** Uways Qarani

COLLECTED, PROCESSED DATA BREACHES

1 entries

VICTIM	SOURCE	THREAT ACTOR	PROCESSED RECORDS
crunchbase[.]com	ShinyHunters	ShinyHunters	559.32K

PROCESSED DATA SET STATISTICS

Past 4 Weeks

380.44M

CAC RECORDS

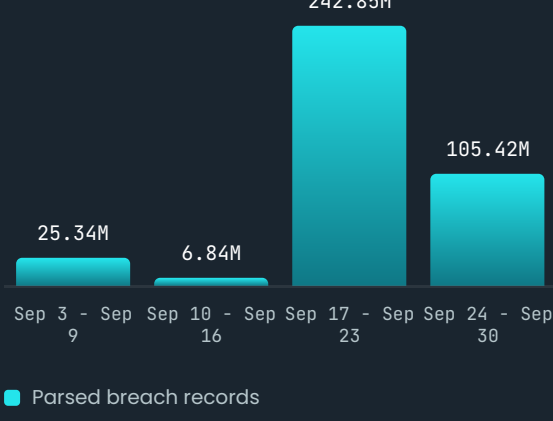
1.12B

BOTNET CAC RECORDS

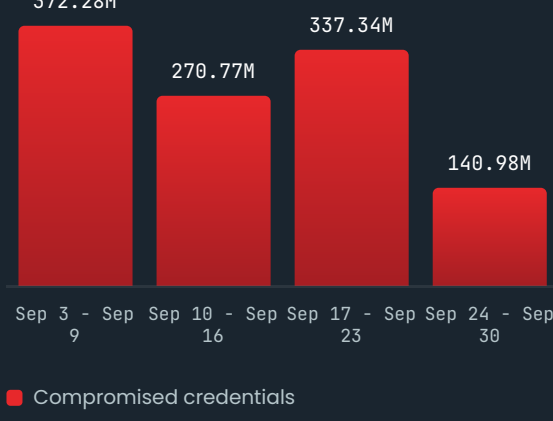
894

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.