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 72 hours.

September 14, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

5 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
Wallstreet Ransomware	New Covenant Believers' Church
RansomHouse	California School Employees Association
Wallstreet Ransomware	Goldston Oil
Rhysida Ransomware	General Santos Doctors Hospital
CHAOS Ransomware	Mankato Clinic

VULNERABILITY DISCLOSURES

4 disclosures

CVE-2026-85103
Heap-Based Buffer Overflow Vulnerability in Check Point Quantum Security Gateway and Quantum Security Management

CVE-2026-85102
Improper Certificate Validation Vulnerability in Check Point Quantum Security Gateway

CVE-2026-85706
Unauthenticated Path Traversal Vulnerability in GitLab CE/EE

CVE-2026-84869
Improper Privilege Management and Missing Authorization Vulnerability in ConnectWise ScreenConnect

DEEP AND DARK WEB INTELLIGENCE

3 findings

CRITICAL FINDINGS

CRITICAL **Exploit: Data Allegedly Associated with Leben Salud, AFC Holdings, Autoplanet, Quick Silver, and Unnamed UK Retailer Advertised**

On September 11 and 13, 2026, well-regarded threat actor "betway" advertised five distinct corporate data set on the predominantly Russian-language DDW forum Exploit.

Source: Exploit **Actor:** betway

CRITICAL **Data Allegedly Associated with Digital Nirvana Advertised**

On September 13, 2026, a moderately credible threat actor "zestix" advertised a database allegedly associated with Digital Nirvana on Exploit.

Source: Exploit **Actor:** zestix

VULNERABILITY EXPLOITATION

MEDIUM **Alleged Windows 11 Local Privilege Escalation (LPE) Zero-Day Exploit Advertised**

On September 13, 2026, untested threat actor "mslover3000" advertised an alleged zero-day Local Privilege Escalation (LPE) exploit affecting Windows 11 on the predominantly English-language DDW forum PwnForums.

Source: PwnForums **Actor:** mslover3000

COLLECTED, PROCESSED DATA BREACHES

2 entries

VICTIM	SOURCE	THREAT ACTOR	PROCESSED RECORDS
nius[.]de	PwnForums	EndOfTheFile	6.1K
kernelseasonsgiveaways[.]com	PwmForums	jail	49.07K

PROCESSED DATA SET STATISTICS

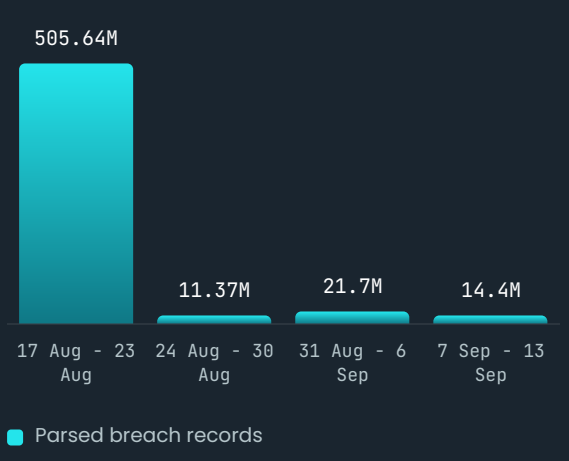
Past 4 Weeks

553.12M CAC RECORDS

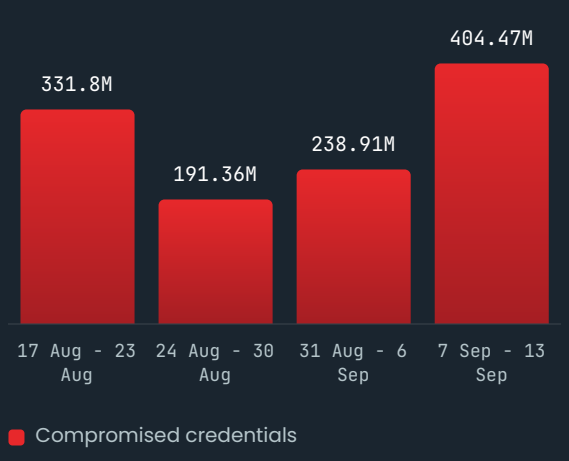
1.17B BOTNET CAC RECORDS

971 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.