

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 22, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

8 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
Leakeddata	Hogan Lovells Cadwalader
Termite ransomware	Truamerica Multifamily
Global secret group ransomware	KJLA TV 57
Qilin ransomware	Telrad Networks
Doommageddon ransomware	Charlottesville Police Department
Nightspire ransomware	Great Bay Bio Group
Bravox ransomware	Towill
Lockbit 5.0 ransomware	Siinqee Bank

DEEP AND DARK WEB INTELLIGENCE

7 findings

DATA BREACHES & LEAKS

HIGH

Data Allegedly Associated with flydubai Advertised (SilentHex)

On September 21, 2026, moderately reputed threat actor "SilentHex" advertised "passenger leads" allegedly associated with flydubai, UAE-based airline, on the predominantly DDW forum Exploit.

Source: Exploit Actor: silenthex

HIGH

Data Allegedly Associated with Federal Capital Territory Internal Revenue Service Advertised (Individual)

On September 21, 2026, untested threat actor "Individual" advertised data allegedly associated with Federal Capital Territory Internal Revenue Service (FCT-IRS), Nigeria, on the predominantly English-language DDW forum PwnForums.

Source: Pwnforums Actor: individual

HIGH

Alleged 1.9 Million U.S.-Based Credit Cards Data Advertised (VlkIn9)

On September 19, 2026, well regarded threat actor "VlkIn9" advertised an auction for a private dataset allegedly containing 1.9 million U.S.-based used credit cards with CVV codes on Exploit.

Source: Exploit Actor: vlkIn9

VULNERABILITY EXPLOITATION

HIGH

Alleged N-day Exploit Targeting Zimbra Advertised (xanxpills)

On September 21, 2026, untested threat actor "xanxpills" advertised an alleged N-day exploit targeting Zimbra on the predominantly Russian-language DDW forum RehubCom.

Source: Rehubcom Actor: xanxpills

UNAUTHORIZED ACCESS CLAIMS

HIGH

RDWeb Access Allegedly Tied to France-Based Pharmaceutical Company Advertised (BarackOllama)

On September 20, 2026, untested threat actor "BarackOllama" advertised RDWeb access with domain administrator rights allegedly associated with an unnamed France-based pharmaceutical company on PwnForums.

Source: Pwnforums Actor: barackollama

HIGH

Fortinet Access Allegedly Tied to Brazil-Based Telecommunications Company Advertised (Big-Bro)

On September 20, 2026, well regarded threat actor "Big-Bro" advertised an auction for Fortinet access with domain user rights allegedly associated with an unnamed Brazil-based telecommunications company on Exploit.

Source: Exploit Actor: big-bro

HIGH

VPN Access Allegedly Tied to Brazil-Based Company Ecorodovias Advertised (vellu)

On September 18, 2026, untested threat actor "vellu" advertised VPN access allegedly associated with Ecorodovias, Brazil-based transportation infrastructure and logistics company on PwnForums.

Source: Pwnforums Actor: vellu

COLLECTED, PROCESSED DATA BREACHES

1 entries

VICTIM	SOURCE	THREAT ACTOR	PROCESSED RECORDS
chess[.]com	Exploit	BlackBeans	4.68M

PROCESSED DATA SET STATISTICS

Past 4 Weeks

49.05M

CAC RECORDS

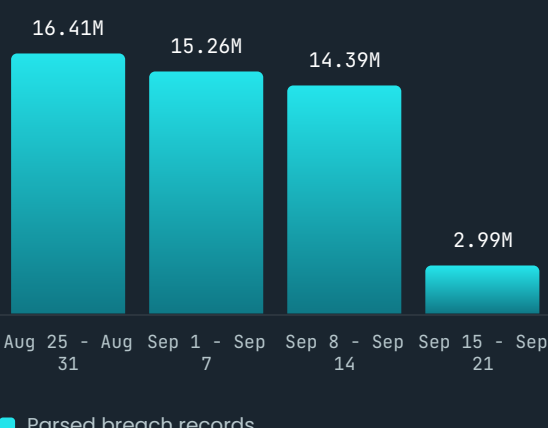
1.07B

BOTNET CAC RECORDS

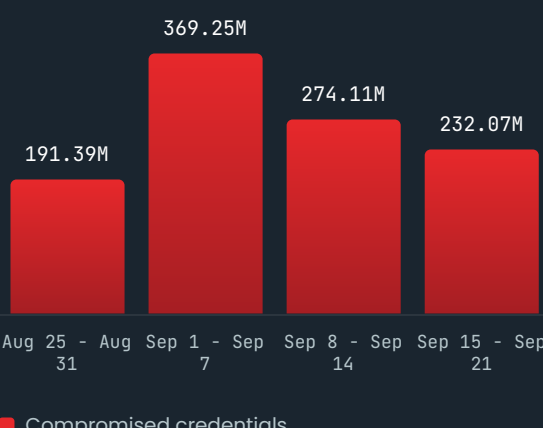
917

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.