

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 21, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

7 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
N0n	Fanatics
Dragonforce Ransomware	ARS Renacer
Threeam ransomware	Newman Tractor
Rhysida Ransomware	MPA Pharma
Storm Ransomware	First Secure Community Bank
Storm Ransomware	First Secure Bank & Trust
Metaencryptor Ransomware	AECOM

VULNERABILITY DISCLOSURES

3 disclosures

[CVE-2026-53266](#)

Out-of-Bounds Write Vulnerability in Linux Kernel Netfilter Bridge (ebt_snat)

[CVE-2026-58138](#)

Unauthenticated Remote Code Execution Vulnerability in Orkes Conductor

[CVE-2026-28326](#)

Use of Hard-Coded Cryptographic Key in SolarWinds Access Rights Manager

DEEP AND DARK WEB INTELLIGENCE

8 findings

NEW LEAKSITES, MARKETPLACES, FORUMS

CRITICAL

New Data Leak Site Emerges (n0n)

On September 21, 2026, ZeroFox observed a new data leak site operating under the name "n0n."

Actor: n0n

DATA BREACHES & LEAKS

HIGH

Data Allegedly Associated with Pakistan Navy Defense Procurement and Projects Advertised (Cyb3R_Shubh4M)

On September 18, 2026, untested threat actor "Cyb3R_Shubh4M" advertised documents allegedly related to Pakistan Navy defense procurement and projects with Chinese defense entities on the predominantly Russian-language DDW forum Exploit.

Source: Exploit **Actor:** cyb3r Shubh4m

HIGH

Data Allegedly Associated with Parler Advertised (pepela)

On September 21, 2026, moderately credible threat actor "pepela" advertised a database allegedly associated with Parler (Sovren Technologies), a U.S.-based social media platform, on Exploit.

Source: Exploit **Actor:** pepela

CRITICAL

Data Allegedly Associated with National Health Insurance Service Advertised (666op)

On September 21, 2026, moderately credible threat actor "666op" advertised an alleged database belonging to the National Health Insurance Service, South Korea, on the predominantly English-language DDW forum PwnForums.

Source: Pwnforums **Actor:** 666op

HIGH

Data Allegedly Associated with Breakthrough Broker Advertised (bleedingout)

On September 17, 2026, moderately credible threat actor "bleedingout" advertised an alleged database belonging to users of Breakthrough Broker, U.S.-based a real-estate marketing platform, on Exploit.

Source: Exploit **Actor:** bleedingout

HIGH

Data Allegedly Associated with Greffe du Tribunal de Paris Personnel Advertised (Alduin)

On September 17, 2026, threat actor "Alduin" leaked an alleged database belonging to the Greffe du Tribunal des Activités Économiques de Paris (Registry of the Tribunal of Economic Activities of Paris) on PwnForums.

Source: Pwnforums **Actor:** alduin

VULNERABILITY EXPLOITATION

HIGH

Alleged Turnkey Exploitation Solution for Veeam 12.x Deployment Advertised (eigen)

On September 18, 2026, an untested threat actor "eigen" advertised an alleged turnkey solution for exploiting Veeam versions 12.x on Exploit.

Source: Exploit **Actor:** eigen

THREAT ACTOR COMMUNICATIONS

MEDIUM

Extortion Campaign Against C10p Ransomware Group (ShinyHunters)

On September 21, 2026, ZeroFox observed an update posted on the ShinyHunters leak site targeting C10p's ransomware leak site.

Source: Leak site **Actor:** shinyhunters

PROCESSED DATA SET STATISTICS

Past 4 Weeks

50.47M

CAC RECORDS

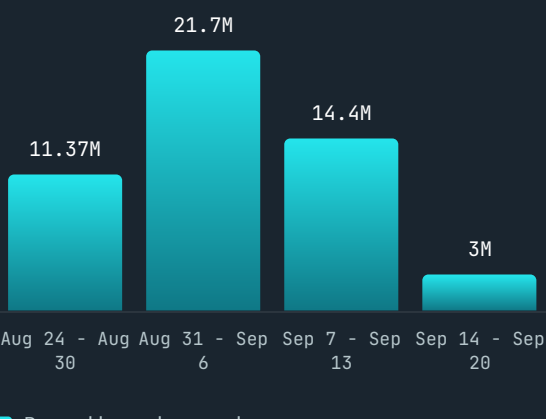
1.07B

BOTNET CAC RECORDS

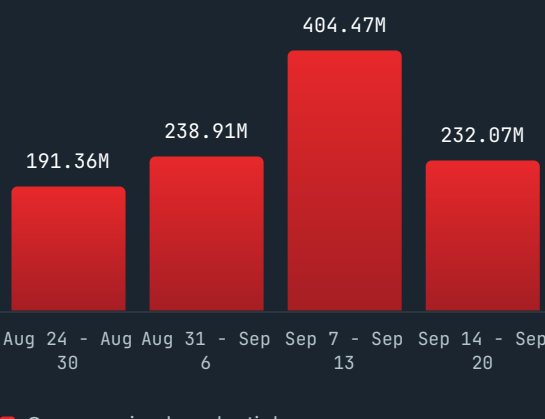
1.13K

RANSOMWARE & DIGITAL EXTORTION

PROCESSED DATA BREACH RECORDS



INFESTEALER 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.