

Deep and Dark Web Intelligence Reporting

Here is a curated list of critical incidents and compromised data observed on DDW ransomware sites, forums, and marketplaces ingested into the ZeroFox Platform in the past 24 hours.

October 15, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

6 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
BYOD	DECOROLALA
The Gentlemen Ransomware	Martin
Dragonforce Ransomware	Lane Equipment Company
Qilin Ransomware	Vadeto Group
Qilin Ransomware	Foxstone Financial
Lockbit 5.0 Ransomware	Kord Hotels

VULNERABILITY DISCLOSURES

3 disclosures

[CVE-2026-76519](#)

Arbitrary File Write Vulnerability in Cisco Secure Email Gateway

[CVE-2026-0322](#)

Remote Code Execution Vulnerability in Palo Alto Networks PAN-OS

[CVE-2026-92392](#)

Use-After-Free Vulnerability in curl

DEEP AND DARK WEB INTELLIGENCE

7 findings

THREAT ACTOR PROFILE

HIGH

Threat Actor Profile: Medusa RaaS

Medusa is a ransomware-as-a-service (RaaS) operation that the FBI first identified in June 2021. The operation initially operated as a closed group, with the same actors controlling both development and attacks, before moving to an affiliate model by at least early 2023.

CRITICAL FINDINGS

CRITICAL

Surge in Activity with 31 New Victims Added

On October 15, 2026, ZeroFox observed that The Gentlemen ransomware group listed 31 new victims on their leak site.

Source: The Gentlemen Ransomware **Actor:** The Gentlemen

DATA BREACHES & LEAKS

HIGH

Alleged Access to U.S. Government-Issued Documents Lookup Service Advertised

On October 14, 2026, an untested threat actor "MEKANIST" advertised access to an alleged administrative panel for searching United States identification documents, including driver licenses, passports, and other government-issued IDs, on a predominantly Russian-language DDW forum Exploit.

Source: Exploit **Actor:** MEKANIST

HIGH

Data Allegedly Tied to Bangladesh Navy Advertised

On October 14, 2026, untested threat actor "Cyb3R_Shubh4M" advertised an alleged 135 GB data set associated with the Bangladesh Navy on Exploit.

Source: Exploit **Actor:** Cyb3R_Shubh4M

UNAUTHORIZED ACCESS CLAIMS

HIGH

Web Panel Access Allegedly Tied to India-Based Company Nexa Solutions Advertised

On October 14, 2026, an untested threat actor "Papurubatafurai" advertised an auction for web panel access with administrator rights allegedly tied to a the India-based software development company Nexa Solutions on Exploit.

Source: Exploit **Actor:** Papurubatafurai

HIGH

RDWeb Access Allegedly Tied to U.S.-Based Insurance Company Advertised

On October 13, 2026, a well-known threat actor "Big-Bro" advertised an auction for RDWeb access with domain user rights allegedly tied to an unnamed U.S.-based insurance company on Exploit.

Source: Exploit **Actor:** Big-Bro

HIGH

RDP and Shell Access Allegedly Tied to UK-Based Events Company Advertised

On October 13, 2026, a well-regarded threat actor "Saturned33" advertised an auction for RDP and shell access with local administrator and SYSTEM rights allegedly tied to an unnamed UK-based events company on Exploit.

Source: Exploit **Actor:** Saturned33

COLLECTED, PROCESSED DATA BREACHES

1 entries

VICTIM	SOURCE	THREAT ACTOR	PROCESSED RECORDS
elekta[.]com	ShinyHunters	ShinyHunters	207.53K

PROCESSED DATA SET STATISTICS

Past 4 Weeks

430.57M

CAC RECORDS

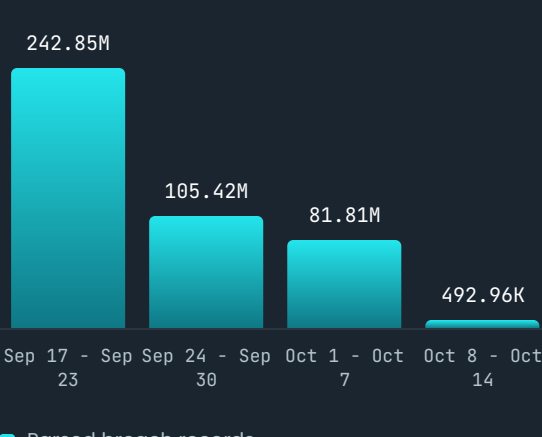
1.13B

BOTNET CAC RECORDS

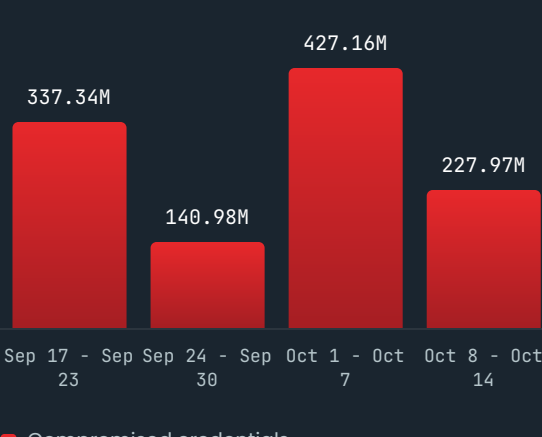
986

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.