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 24 hours.

August 26, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

6 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
DYSPHORIA Ransomware	University of Delhi
Storm Ransomware	City of Mitchell
Akira Ransomware	Davis & Ferber
BEAST Ransomware	Cosmon
Dark Project	Design-Aire Engineering
Booba Project Ransomware	Country-Wide Insurance

DEEP AND DARK WEB INTELLIGENCE

9 findings

CRITICAL FINDINGS

CRITICAL **Data Allegedly Associated with the Ministry of Interior, Palestinian Territories Leaked**

On August 26, 2026, moderately credible threat actor "GordonFreeman" leaked data allegedly associated with the Ministry of Interior, Palestinian territories, on the predominantly English-language DDW forum DarkForums.

Source: DarkForums **Actor:** GordonFreeman

CRITICAL **Surge in Activity with 21 New Victims Added**

On August 25, 2026, ZeroFox observed that The Gentlemen ransomware group listed 21 new victims on their leak site.

Source: The Gentlemen Ransomware

CRITICAL **Alleged Visa Data Breach Advertised—Possible Repost of Earlier Leak**

On August 25, 2026, untested threat actor "Roxym3ln" advertised data allegedly associated with Visa, a U.S.-based payments technology company, on DarkForums.

Source: DarkForums **Actor:** Roxym3ln

CRITICAL **Alleged Polish Bank Employee Data Leak Advertised**

On August 25, 2026, untested threat actor "LuckyRaku1" advertised a leak allegedly containing data associated with Poland-based Banks, on the predominantly Russian-language DDW forum Exploit.

Source: Exploit **Actor:** LuckyRaku1

HIGH **Data Allegedly Associated with Undisclosed Healthcare Company Advertised**

On August 24, 2026, moderately credible threat actor "Galaher" advertised a data set allegedly associated with an undisclosed healthcare company on the predominantly Russian-language DDW forum XSS.

Source: XSS **Actor:** Galaher

DATA BREACHES & LEAKS

HIGH **Data Allegedly Associated with Quest Apartment Hotels Leaked**

On August 25, 2026, untested threat actor "uawrongteam" leaked data allegedly associated with Quest Apartment Hotels, Australia, on Exploit.

Source: Exploit **Actor:** uawrongteam

HIGH **Data Allegedly Associated with Canada-Based Appointment Management Platform Yocale Advertised**

On August 24, 2026, untested threat actor "Kazu" advertised a 51.02 GB dataset allegedly associated with the Canada-based appointment management platform Yocale on Exploit.

Source: Exploit **Actor:** Kazu

UNAUTHORIZED ACCESS CLAIMS

HIGH **Network Access Allegedly Tied to U.S.-Based Technology Company Advertised**

On August 24, 2026, untested threat actor "tarakanas" advertised alleged network access associated with an unnamed U.S.-based Cloud and AI technology company on the predominantly English-language DDW forum PwnForums.

Source: PwnForums **Actor:** tarakanas

HIGH **SimpleHelp Access Allegedly Tied to U.S.-Based Dental Office Technology Provider Advertised**

On August 25, 2026, untested threat actor "Mark1777" advertised an auction for SimpleHelp access allegedly associated with an unnamed U.S.-based business services company on Exploit.

Source: Exploit **Actor:** Mark1777

COLLECTED, PROCESSED DATA BREACHES

1 entries

VICTIM	SOURCE	THREAT ACTOR	PROCESSED RECORDS
microsoft[.]com	ExfilSquad	ExfilSquad	3.73M

PROCESSED DATA SET STATISTICS

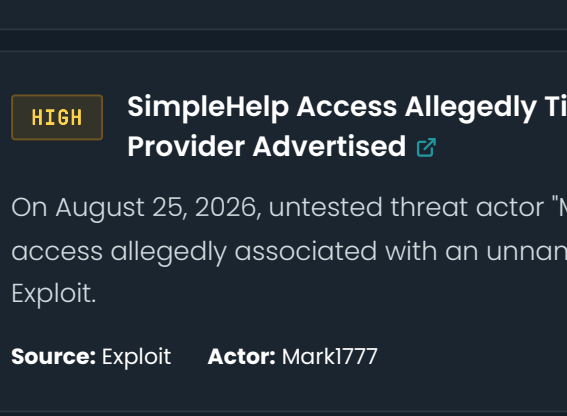
Past 4 Weeks

1.27B CAC RECORDS

990.28M BOTNET CAC RECORDS

1.04K 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.