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 12, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

5 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
Qilin Ransomware	City of Winchester, Kentucky
The Gentlemen Ransomware	Eva Care Group
The Gentlemen Ransomware	LanceSoft
Space Bears Ransomware	Elixi International
The Gentlemen Ransomware	AnMed

DEEP AND DARK WEB INTELLIGENCE

6 findings

CRITICAL FINDINGS

CRITICAL **Metabase**

On August 12, 2026, ZeroFox observed an update on the ShinyHunters leak site targeting Metabase, a U.S.-based open-source business intelligence and data analytics platform.

Source: ShinyHunters

CRITICAL **Threat Actor Claims Responsibility for Minnesota Water Infrastructure Incident**

On August 12, 2026, a pro-Iran threat actor group, "APT IRAN," claimed joint responsibility for the Minnesota water infrastructure incident alongside "CyberAv3ngers" on their Telegram channel, characterizing the operation as a warning.

Source: Telegram **Actor:** APT IRAN, CyberAv3ngers

UNAUTHORIZED ACCESS CLAIMS

HIGH **VNC and VPN Access Allegedly Tied to U.S.-Based Real Estate, Hospitality and Advertising Company Advertised**

On August 11, 2026, untested threat actor "yurikino" advertised an auction for VNC and VPN access with domain user rights, allegedly associated tied to an unnamed U.S.-based real estate, hospitality and advertising company, on the predominantly Russian-language deep and dark web forum Exploit.

Source: Exploit **Actor:** yurikino

HIGH **RDP Access Allegedly Tied to Canada-Based Company Advertised**

On August 10, 2026, well-regarded threat actor "sudo" advertised RDP access allegedly associated with an undisclosed Canada-based company on the predominantly Russian-language deep and dark web forum Exploit.

Source: Exploit **Actor:** sudo

HIGH **RDP Access Allegedly Tied to India-Based Technology Company Advertised**

On August 10, 2026, untested threat actor "Executive" advertised RDP access with domain user rights allegedly associated with an unnamed India-based technology company on the predominantly Russian-language deep and dark web forum Exploit.

Source: Exploit **Actor:** Executive

HIGH **FortiGate Access Bundle Allegedly Tied to Over 400 U.S.-Based Companies Advertised**

On August 11, 2026, untested threat actor "zobento" advertised FortiGate access bundle with SuperAdmin rights allegedly tied to over 400 undisclosed U.S.-based companies on the predominantly English-language deep and dark web forum DarkForums.

Source: DarkForums **Actor:** zobento

COLLECTED, PROCESSED DATA BREACHES

3 entries

VICTIM	SOURCE	THREAT ACTOR	PROCESSED RECORDS
ronis.com[.]au	PwnForums	2019	34.34K
isam.edu[.]pe	PwnForums	NAJASOR	75.73K
builderslog[.]com	PwnForums	chinebase	4.63K

PROCESSED DATA SET STATISTICS

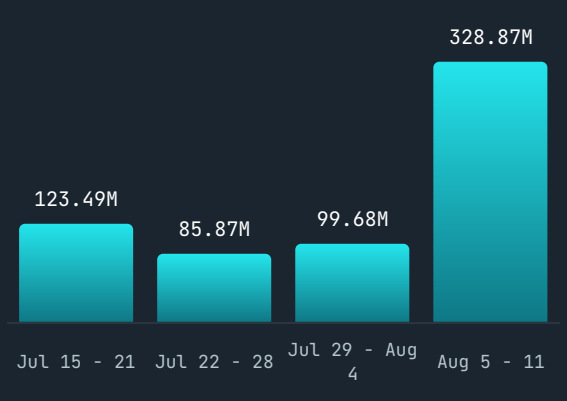
Past 4 Weeks

637.91M CAC RECORDS

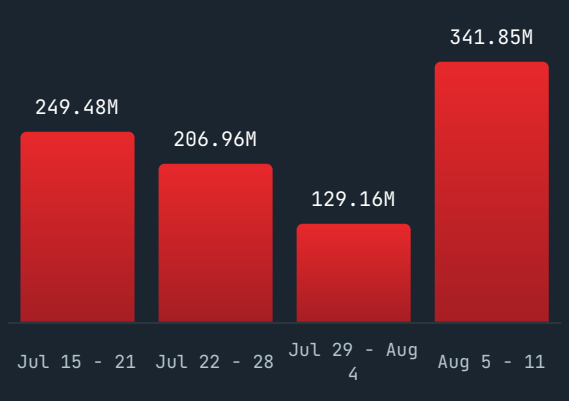
927.45M BOTNET CAC RECORDS

885 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.