

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 15, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

5 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
Qilin Ransomware	Imperial Healthcare Solutions
GENESIS Ransomware	Bernath & Rosenberg
Eclipse Ransomware	Dublin City Schools
MedusaLocker Ransomware	NSW Health
Cinder	Veritiv

DEEP AND DARK WEB INTELLIGENCE

4 findings

CRITICAL FINDINGS

CRITICAL

Data Allegedly Associated with ROHTO Pharmaceutical Co. Advertised

On September 14, 2026, moderately credible threat actor "sta6" advertised data allegedly associated with ROHTO Pharmaceutical Co., Japan, on the predominantly English-language DDW forum PwnForums.

Source: PwnForums Actor: sta6

CRITICAL

Data Allegedly Associated with CenterPoint Energy Leaked

On September 12, 2026, untested threat actor "Hex_4d722e4d656f77" leaked data allegedly associated with CenterPoint Energy on the predominantly English-language deep web forum BreachForums (bf[.]st).

Source: BreachForums Actor: Hex_4d722e4d656f77

CRITICAL

Data Allegedly Associated with Versace Advertised

On September 14, 2026, untested threat actor "RedStone" advertised employee data allegedly associated with Versace V-SIDE on PwnForums.

Source: PwnForums Actor: RedStone

HACKTIVISM

MEDIUM

Actor Claims DDoS Attacks Targeting Saudi Ministry of Foreign Affairs and Saudi National Bank

On September 12 and 13, 2026, a pro-Palestinian threat actor group "313 Team" claimed, via its Telegram channel, to have carried out Distributed Denial-of-Service (DDoS) attacks against the Saudi Ministry of Foreign Affairs and the Saudi National Bank (SNB).

Source: Telegram Actor: 313 Team

PROCESSED DATA SET STATISTICS

Past 4 Weeks

537.16M

CAC RECORDS

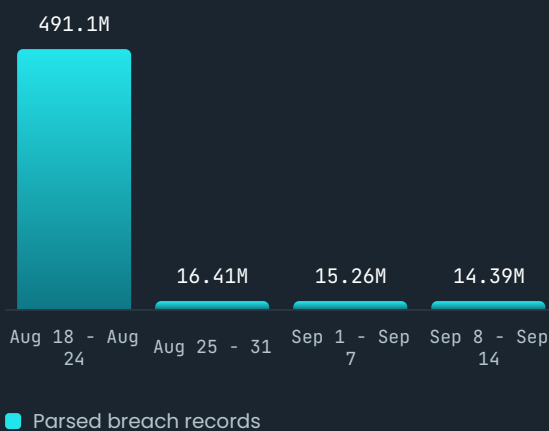
1.08B

BOTNET CAC RECORDS

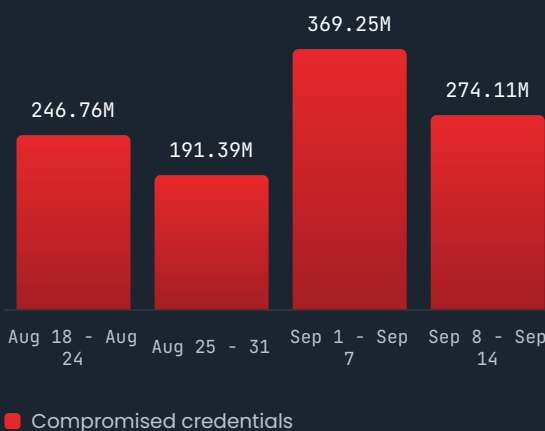
934

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.