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 18, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

5 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
BLACKWATER	Shalina Healthcare
Akira Ransomware	Keystops
Akira Ransomware	Cozad Asset Management
LockBit 5.0 Ransomware	TECOSIM Group
CoinbaseCartel Ransomware	Sweetwater Holdings

DEEP AND DARK WEB INTELLIGENCE

8 findings

CRITICAL FINDINGS

CRITICAL **Data Allegedly Associated with Republic Health Insurance Fund Advertised**

On August 18, 2026, a moderately credible threat actor "ByteToBreach" advertised data allegedly associated with Republic Health Insurance Fund on the predominantly English-language DDW forum DarkForums. Notably, the same actor published identical post on the predominantly English-language DDW forum PwnForums and Spear.

Source: DarkForums **Actor:** ByteToBreach

CRITICAL **Data Allegedly Associated with Tata Housing Development Company Advertised**

On August 17, 2026, untested threat actor "saotome" advertised a database allegedly associated with Tata Housing Development Company, an India-based real estate developer, on DarkForums.

Source: DarkForums **Actor:** saotome

CRITICAL **Data and API Keys Allegedly Associated with Stripe Leaked**

On August 18, 2026, well-reputated threat actor "Satanic" leaked a 33 GB dataset and compromised API keys allegedly associated with Stripe on PwnForums.

Source: PwnForums **Actor:** Satanic

UNAUTHORIZED ACCESS CLAIMS

HIGH **SSH and FortiGate Access Allegedly Tied to U.S.-Based Company Advertised**

On August 15, 2026, untested threat actor "SCP-2013" advertised SSH and FortiGate access allegedly associated with an undisclosed U.S.-based company on Exploit.

Source: Exploit **Actor:** SCP-2013

HIGH **Access Allegedly Tied to Github Project Containing Mobile App Source Code Advertised**

On August 16, 2026, untested threat actor "GoGoDuck1984" advertised access allegedly associated with Github project containing the source code of a mobile application with over 10 million downloads on Google Play, on Exploit.

Source: Exploit **Actor:** GoGoDuck1984

HIGH **Data Allegedly Associated with U.S.-Based Live Streaming Platform BallerTV Advertised**

On August 16, 2026, well-regarded threat actor "betway" advertised data allegedly associated with BallerTV, a U.S.-based live streaming platform on Exploit.

Source: Exploit **Actor:** betway

HIGH **RDWeb Access Allegedly Associated with Italy-Based Cloud and IT Services Company Advertised**

On August 17, 2026, untested threat actor "impotent4000" advertised an auction for RDWeb access allegedly associated with an unnamed Italy-based Cloud and IT services company on Exploit.

Source: Exploit **Actor:** impotent4000

VULNERABILITY EXPLOITATION

HIGH **Alleged Windows Local Privilege Escalation Zero-Day Advertised for Sale**

On August 17, 2026, untested threat actor "David8" advertised an alleged Windows Local Privilege Escalation (LPE) zero-day exploit on Exploit.

Source: Exploit **Actor:** David8

COLLECTED, PROCESSED DATA BREACHES

5 entries

VICTIM	SOURCE	THREAT ACTOR	PROCESSED RECORDS
chat-coco[.]fr	PwnForums	misere	14.14K
ketone[.]com	PwnForums	GoreTurbine	57.06K
mywaggle[.]com	PwnForums	2019	113.19K
brevibrushes[.]com	PwnForums	jail	87.29K
groomit[.]me	PwnForums	GoreTurbine	37.32K

PROCESSED DATA SET STATISTICS

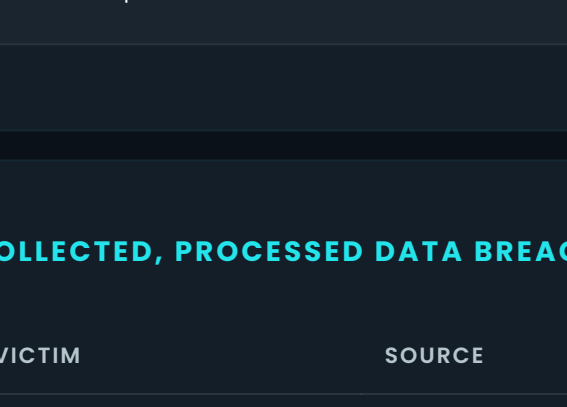
Past 4 Weeks

858.27M CAC RECORDS

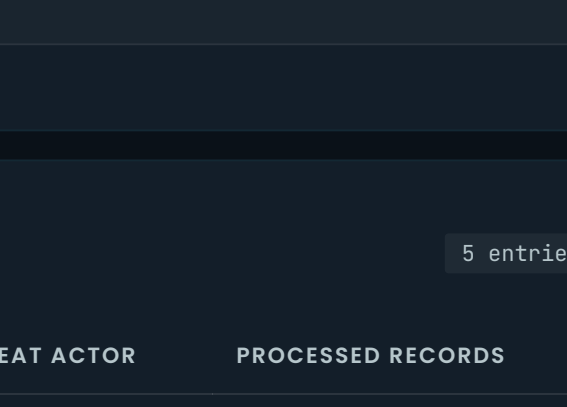
950.48M BOTNET CAC RECORDS

913 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.