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 27, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

7 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
FALCON	Globus Medical
Qilin Ransomware	KenEp Resources
Dire Wolf Ransomware	National Kidney Registry
Abyss Ransomware	MEMSIC Semiconductor
Qilin Ransomware	Clear Align
Chaos Ransomware	Central Ohio Primary Care
Qilin Ransomware	Northern Leasing Systems

VULNERABILITY DISCLOSURES

1 disclosure

CVE-2026-18431

Unauthenticated Remote Code Execution via Arbitrary File Write in ThemeFusion Avada (Fusion Builder)

DEEP AND DARK WEB INTELLIGENCE

9 findings

CRITICAL FINDINGS

CRITICAL **Data Allegedly Associated with Police Nationale Togolaise Leaked**

On August 27, 2026, moderately credible threat actor "Lagui1337" leaked data allegedly associated with Police Nationale Togolaise, on the predominantly English-language DDW PwnForums.

Source: PwnForums **Actor:** Lagui1337

HIGH **Alleged Email Sending Service 'Tripauls Web Emailer' Advertised**

On August 25, 2026, untested threat actor "Fiaqel" advertised alleged email sending service known as Tripauls Web Emailer on the predominantly Russian-language DDW forum XSS.

Source: XSS **Actor:** Fiaqel

DATA BREACHES & LEAKS

CRITICAL **Data Allegedly Associated with 2020 Tax Form 1040 Advertised**

On August 25, 2026, untested threat actor "larrypat09" advertised an auction for a dataset allegedly containing 2020 tax form 1040 on the predominantly Russian-language DDW forum Exploit.

Source: Exploit **Actor:** larrypat09

HIGH **Data Allegedly Associated with U.S.-Based Company CGETC Advertised**

On August 25, 2026, well-regarded threat actor "betway" advertised data allegedly associated with CGETC, a U.S.-based logistics and fulfillment company on the predominantly Russian-language on Exploit.

Source: Exploit **Actor:** betway

HIGH **Data Allegedly Associated with U.S.-Based Moving Company ABC Movers Advertised**

On August 25, 2026, well-regarded threat actor "betway" advertised data allegedly associated with ABC Movers, a U.S.-based moving company on Exploit.

Source: Exploit **Actor:** betway

UNAUTHORIZED ACCESS CLAIMS

CRITICAL **Network Access Allegedly Associated with Instituto Português do Mar e da Atmosfera Advertised**

On August 26, 2026, moderately credible threat actor "bytetobreach" advertised network access allegedly associated with Instituto Português do Mar e da Atmosfera on the predominantly English-language DDW forum Spear.

Source: Spear **Actor:** bytetobreach

HIGH **Network Access Allegedly Tied to Qatar-Based Pharmaceutical Company Advertised**

On August 25, 2026, well-regarded threat actor "888" advertised network access allegedly associated with an unnamed Qatar-based pharmaceutical company on PwnForums.

Source: PwnForums **Actor:** 888

VULNERABILITY EXPLOITATION

HIGH **Alleged macOS Local Privilege Escalation Zero-Day Exploit Advertised**

On August 26, 2026, untested threat actor "LazaKNOXGroup" advertised a macOS Local Privilege Escalation (LPE) zero-day exploit on the predominantly English-language DDW forum DarkForums.

Source: DarkForums **Actor:** LazaKNOXGroup

HIGH **Vulnerability Allegedly Targeting Canada-Based Company Chatr Advertised**

On August 26, 2026, moderately credible threat actor "NightBroker" advertised a vulnerability allegedly targeting Chatr on PwnForums.

Source: PwnForums **Actor:** NightBroker

COLLECTED, PROCESSED DATA BREACHES

1 entries

VICTIM	SOURCE	THREAT ACTOR	PROCESSED RECORDS
kingofthecurve[.]org	PwnForums	GoreTurbine	298.03K

PROCESSED DATA SET STATISTICS

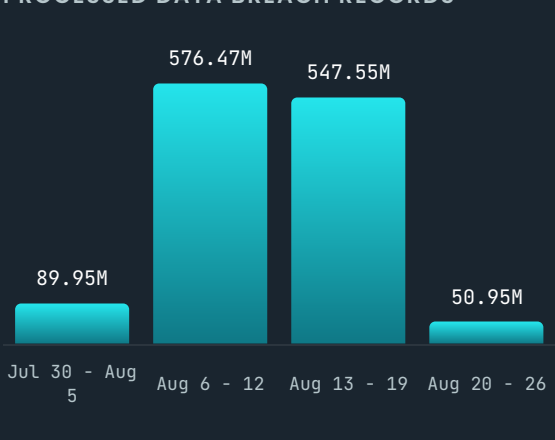
Past 4 Weeks

1.26B CAC RECORDS

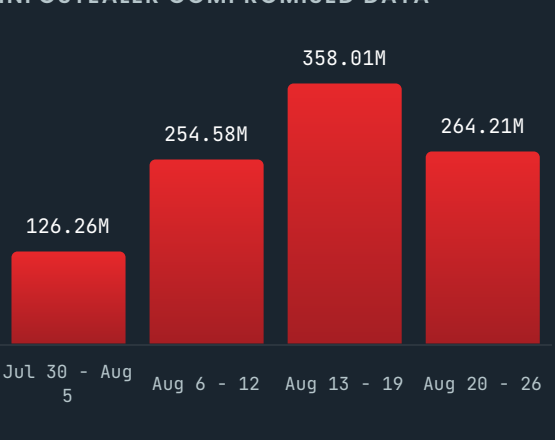
1B BOTNET CAC RECORDS

1.11K 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.