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 72 hours.

August 24, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

7 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
The Gentlemen Ransomware	Biopharma
ShinyHunters	Novocure
PEAR Ransomware	Club One Casino
ShinyHunters	ReliaQuest
ShinyHunters	CyrusOne
ShinyHunters	BOK Financial
The Gentlemen Ransomware	Community Connections

VULNERABILITY DISCLOSURES

2 disclosures

CVE-2026-72529
Missing Authentication Vulnerability for Critical Function in TrueConf Server

CVE-2026-72530
Code Injection Vulnerability in TrueConf Server

DEEP AND DARK WEB INTELLIGENCE

6 findings

CRITICAL FINDINGS

CRITICAL **15 New Victims Listed**

Between August 21 and 23, 2026, Qilin ransomware group reportedly listed 15 new victims on their leak site.

Source: Qilin Ransomware

CRITICAL **14 New Victims Listed**

On August 22 and 23, 2026, CoinbaseCartel ransomware group listed 14 new victims on their leak site.

Source: CoinbaseCartel Ransomware

NEW LEAKSITES, MARKETPLACES, FORUMS

CRITICAL **New Ransomware Group Emerges**

On August 24, 2026, ZeroFox observed new threat actor claiming to be a ransomware group, operating under the name "Black-Lotus." The group outlined its modus operandi and rules of engagement in a post on its Telegram channel.

Source: Telegram **Actor:** Black-Lotus

UNAUTHORIZED ACCESS CLAIMS

HIGH **Fortinet VPN Access Allegedly Tied to U.S.-Based Legal Services Company Advertised**

On August 21, 2026, untested threat actor "DkSehersnes" advertised an auction for Fortinet VPN access with domain administrator rights allegedly associated with an unnamed U.S.-based legal services company on the predominantly Russian-language DDW web forum Exploit.

Source: Exploit **Actor:** DkSehersnes

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

On August 21, 2026, untested threat actor "SCP-2013" (likely known as "APL-BRK" and "Dark_Alpha") advertised to sell FortiGate, FortiCloud, SSH, and Fortinet SSL-VPN access with domain administrator rights allegedly associated with an undisclosed Canada-based company on the predominantly English-language DDW forums DarkForums and Exploit.

Source: Exploit/DarkForums **Actor:** SCP-2013, Dark_Alpha

DATA BREACHES & LEAKS

HIGH **Alleged Visa Information of Foreigners in Turkey Advertised**

On August 21, 2026, untested threat actor "SilentHex" advertised data allegedly containing visa information of foreigners in Turkey on Exploit.

Source: Exploit **Actor:** SilentHex

COLLECTED, PROCESSED DATA BREACHES

3 entries

VICTIM	SOURCE	THREAT ACTOR	PROCESSED RECORDS
atlantaga[.]gov	ExfilSquad	ExfilSquad	283.32K
sports.gouv[.]fr	PwnForums	peluche911	44.68K
login.resana.numerique.gouv[.]fr	PwnForums	xMetah (Kobayashi)	888K

PROCESSED DATA SET STATISTICS

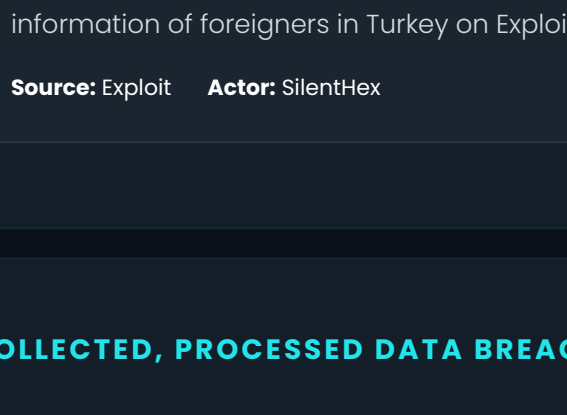
Past 4 Weeks

1.35B CAC RECORDS

1.1B BOTNET CAC RECORDS

991 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.