ZEROFOX

Deep and Dark Web Intelligence Reporting

Here is a curated list of critical incidents and compromised data observed in deep and dark web ransomware sites, forums, and marketplaces ingested into the ZeroFox Platform in the past 24 hours.

July 8, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

5 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
Akira Ransomware	Chisholm, Persson & Ball
SafePay Ransomware	Hahn Airport
BASHE Ransomware	Western International Group
Chaos Ransomware	Air Creebec
DragonForce Ransomware	HIVE360

DEEP AND DARK WEB INTELLIGENCE

8 findings

CRITICAL FINDINGS

CRITICAL **Scattered Lapsus$ Hunters Claim Access to Unidentified AT&T Dashboards**

On July 8, 2026, threat actor group Scattered Lapsus$ Hunters (SLH) made a post on their Telegram channel “International Global Network (SLSH).”

July 8, 2026 Telegram

CRITICAL **Alleged Data Associated with the United States Social Security Administration Advertised**

On July 5, 2026, an untested threat actor "gerome99" advertised a dataset allegedly associated with the United States Social Security Administration, on a predominantly English-language dark web forum DarkForums.

July 5, 2026 DarkForums gerome99

CRITICAL **Alleged Data of Arabia Falcon Insurance and Atlas Medical Advertised**

On July 7 and 8, 2026, untested threat actor “erresira” advertised data associated with Atlas Medical and Arabia Falcon Insurance, on a predominantly English-language dark web forum BreachForums (breached[.]su).

BreachForums erresira

CRITICAL **Alleged Breach of Nayax Data**

On July 7, 2026, an untested threat actor with a positive reputation "TheSyndicate" allegedly breached data associated with Nayax, on a predominantly English-language deep and dark web forum PwnForums.

July 7, 2026 Leak Site/PwnForums TheSyndicate

CRITICAL **Alleged Data Associated with Follow Health Advertised**

On July 7, 2026, a moderately-credible threat actor "Saturne" advertised data associated with Follow Health, on a predominantly English-language deep and dark web forum PwnForums.

July 7, 2026 PwnForums Saturne

UNAUTHORIZED ACCESS CLAIMS

HIGH **Alleged SSH and FortiGate Access Bundle Associated with 3,197 Mexico-Based Companies Advertised**

On July 7, 2026, an untested threat actor "APL-BRK" advertised to sell SSH and FortiGate access bundle with super_admin rights allegedly associated with 3,197 undisclosed Mexico-based companies, on a predominantly Russian language deep and dark web forum XSS.

July 7, 2026 XSS APL-BRK

HIGH **Alleged Data Associated with Pakistan International Airlines Advertised**

On July 7, 2026, an untested threat actor "jamboman" advertised to sell a dataset allegedly associated with Pakistan International Airlines, on a predominantly Russian-language deep and dark web forum Exploit.

July 7, 2026 Exploit jamboman

HIGH **Alleged Fortinet VPN Access Bundle Associated with 300 Undisclosed Companies Advertised**

On July 6, 2026, a well-known threat actor "Big-Bro" advertised an auction for Fortinet VPN access bundle likely affecting 300 undisclosed companies, on a predominantly Russian-language deep and dark web forum Exploit.

July 6, 2026 Exploit Big-Bro

COLLECTED, PROCESSED DATA BREACHES

6 entries

VICTIM	SOURCE	THREAT ACTOR	PROCESSED RECORDS
mylovely[.]ai	PwnForums	Blastoise	106.8K
qntsport[.]in	XSS	Nimori	24.4K
livequeenofhearts[.]com	BreachForums	vulture	13.7K
shopslateandtell[.]com	LeakBase	Chucky	410K
smartschools[.]network	BreachForums	iotseek	142.9K
seeqle[.]com	BreachForums	gaard	325

PROCESSED DATASET STATISTICS

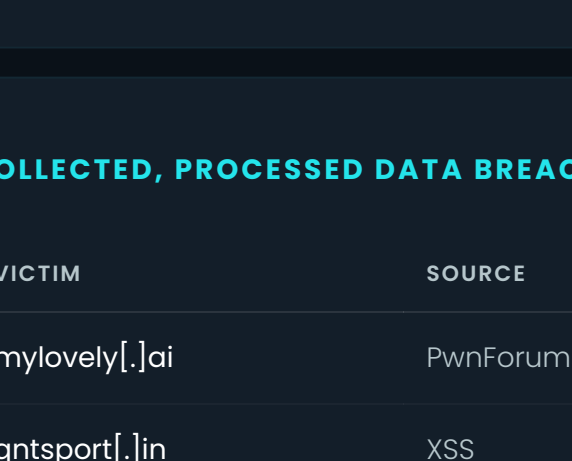
Past 4 Weeks

671.5M CAC RECORDS

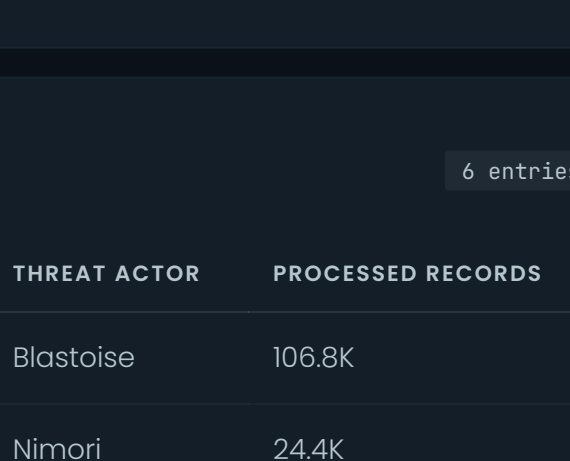
1.1B BOTNET CAC RECORDS

827 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, bizarre tactics, and significant operational spikes that deviate from the baseline threat landscape.