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.

July 28, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

7 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
ShinyHunters	Ernst & Young
Qilin Ransomware	Principle Diagnostics Laboratory
BLACKWATER	MSGÁS
Triple X	Bank of Baroda
Kairos Ransomware	Thermalex
Insomnia	Brooklyn Defender Services
BravoX Ransomware	A&A Safety

VULNERABILITY DISCLOSURES

3 disclosures

CVE-2026-16723
Remote Code Execution Vulnerability in Alibaba Fastjson

CVE-2026-16812
OS Command Injection Vulnerability in Arista VeloCloud Orchestrator

CVE-2026-54121
Improper Authorization Vulnerability in Microsoft Active Directory Certificate Services

DEEP AND DARK WEB INTELLIGENCE

12 findings

CRITICAL FINDINGS

CRITICAL **Alleged Data Associated with NúcleoGov Leaked**

On July 27, 2026, untested threat actor "BL33DR00T" leaked data allegedly associated with NúcleoGov on the predominantly English-language deep and dark web forum PwnForums.

Source: PwnForums **Actor:** BL33DR00T

CRITICAL **Leak Site Lists 29 New Victims**

On July 27, 2026, ZeroFox observed that CRPx0 ransomware group listed 29 new victims on their leak site.

Source: CRPx0 Ransomware

CRITICAL **Alleged Persistent Administrative Access Associated with Saudi Arabia-Based Government Web Ecosystem Advertised**

On July 27, 2026, untested threat actor "skra1a" advertised persistent administrative access allegedly associated with the Saudi Arabia-based government web ecosystem operating under the ".gov.sa" domain, on the predominantly English-language deep and dark web forum DarkForums.

Source: DarkForums **Actor:** skra1a

CRITICAL **Alleged Data Associated with Federal Authority For Identity, Citizenship, Customs & Port Security Leaked**

On July 25, 2026 untested threat actor "404Crew Cyber Team" leaked data allegedly associated with Federal Authority For Identity, Citizenship, Customs & Port Security on the predominantly English-language deep and dark web forum BreachForums(breached[.]su.)

Source: BreachForums **Actor:** 404Crew Cyber Team

UNAUTHORIZED ACCESS CLAIMS

HIGH **Alleged MariaDB, SSH and SFTP Access Tied to South Korea-Based Software Company Advertised**

On July 26, 2026, a well-reputed threat actor "888" advertised MariaDB, SSH and SFTP access allegedly associated with an unnamed South Korea-based software company on the predominantly English-language deep and dark web forum PwnForums.

Source: PwnForums **Actor:** 888

HIGH **Alleged AWS STS Access Tied to Undisclosed Telecommunications Company Advertised**

On July 24, 2026, a moderately credible threat actor "CHINA" advertised network access allegedly associated with AWS Security Token Service (STS) of an undisclosed telecommunications company on the predominantly English-language deep and dark web forum PwnForums.

Source: PwnForums **Actor:** CHINA

HIGH **Alleged Fortinet VPN Access Tied to U.S.-Based Hospitality Company Advertised**

On July 25, 2026, a moderately credible threat actor "molotov477" advertised an auction for Fortinet VPN access allegedly associated with an unnamed U.S.-based hospitality company on the predominantly Russian-language deep and dark web forum Exploit.

Source: Exploit **Actor:** molotov477

HIGH **Alleged Zabbix Access Tied to Cyber Security and IT Services Company Operating in South Africa and Netherlands Advertised**

On July 27, 2026, an untested threat actor "crack3r" advertised Zabbix access with Super-Admin rights allegedly associated with an unnamed cyber security and IT services company operating in South Africa and Netherlands, on the predominantly Russian-language deep and dark web forum Exploit.

Source: Exploit **Actor:** crack3r

DATA BREACHES & LEAKS

CRITICAL **Alleged PII Data of U.S.-Based Individuals Advertised**

On July 27, 2026, an untested threat actor "raojee" advertised two datasets associated with U.S.-based individuals on the predominantly Russian-language deep and dark web forum Exploit.

Source: Exploit **Actor:** raojee

NEW LEAKSITES, MARKETPLACES, FORUMS

HIGH **New Dark Web Leak Site Emerges**

On July 27, 2026, ZeroFox observed a new leak site named "ExfilSquad." As of this report, the leak site lists 15 victims and is accessible via the following dark web address: hXXp://exfil5gqmbxrg6yky5aeitkdj7kfwxxjh3wxzrtlewjqi2x67o634iyd[.]onion/

Source: Leak Site **Actor:** ExfilSquad

HIGH **New Dark Web Leak Site Emerges**

On July 27, 2026, ZeroFox observed a new leak site named "SECTION9." As of this report, the leak site lists 25 undisclosed victims and is accessible via the following dark web address: hXXp://v76bdil3v7hczufr7kwk75eq6oks27d3qwj6v5ajj6v6rubbvwhcq2qd[.]onion

Source: Leak Site **Actor:** SECTION9

HIGH **New Dark Web Site Emerges**

On July 28, 2026, ZeroFox observed a new dark web site named "SHIBA." As of the time of reporting, no victims have been listed on the leak site. The site remains accessible via the following Tor hidden service address: hXXp://shibaitobajtr6yctvrijfitnugfulkmprrqbmu2ysk3zyzx2ufe3yqd[.]onion

Source: SHIBA

COLLECTED, PROCESSED DATA BREACHES

5 entries

VICTIM	SOURCE	THREAT ACTOR	PROCESSED RECORDS
700M_6	Telegram	Satanic Cloud	79.45M
Mon Compte Formation (moncompteformation[.]gouv[.]fr)	PwnForums	Saturne	596.26K
Aude (aude[.]fr)	PwnForums	Saturne	19.85K
Rennes Métropole (metropole[.]rennes[.]fr)	PwnForums	misere	8.73K
STARLINK 20 kk	-	-	5.18M

PROCESSED DATA SET STATISTICS

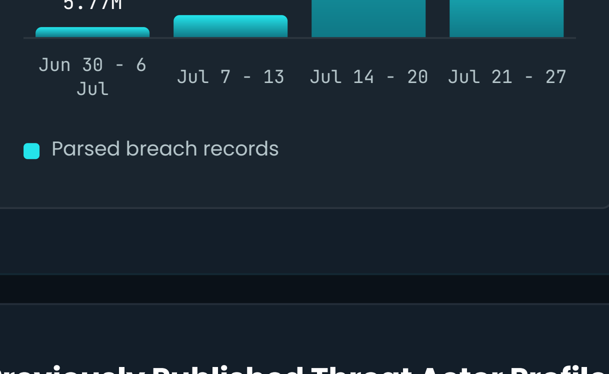
Past 4 Weeks

241.82M
CAC RECORDS

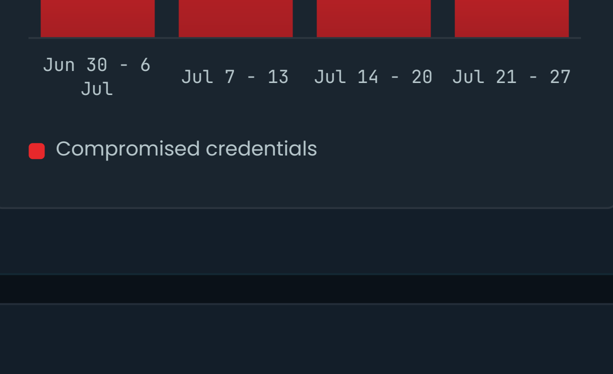
1.05B
BOTNET CAC RECORDS

752
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.