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 31, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

5 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
SECUROTROP Ransomware	MAG USA
GLOBAL SECRET GROUP Ransomware	West Nova Fuels & Superline Fuels
The Gentlemen Ransomware	Garfield County Sheriff's Office
BlackNevas Ransomware	Speed Group
Insomnia	Sky Solutions Panama

VULNERABILITY DISCLOSURES

1 disclosure

CVE-2026-63077

Unauthenticated Remote Code Execution Vulnerability in JetBrains TeamCity On-Premises

DEEP AND DARK WEB INTELLIGENCE

7 findings

CRITICAL FINDINGS

CRITICAL **Alleged GitLab and CI/CD Access to a Major UK Bank Advertised**

On July 30, 2026, well-regarded threat actor "888" advertised access to an unnamed entity described as "One of UK's Largest Banks" on the predominantly English-language DDW forum PwnForums.

Source: PwnForums **Actor:** 888

CRITICAL **Data Allegedly Tied to Hungarian State Treasury Advertised**

On July 31, 2026, moderately credible threat actor "bytestobreach" claimed to have breached data associated with the Magyar Államkincstár (Hungarian State Treasury) on the predominantly Russian-language DDW forum Exploit.

Source: Exploit **Actor:** bytestobreach

UNAUTHORIZED ACCESS CLAIMS

HIGH **SSH Access Allegedly Tied to U.S.-Based Electronics Manufacturing Company Advertised**

On July 29, 2026, untested threat actor "missiyaprizrak0" advertised SSH access allegedly associated with an unnamed U.S.-based electronics manufacturing company on PwnForums.

Source: PwnForums **Actor:** missiyaprizrak0

HIGH **VPN and RDP Access Allegedly Tied to India-Based Manufacturing Company Advertised**

On July 30, 2026, moderately credible threat actor "decider" advertised an auction for VPN and RDP access with domain administrator rights allegedly tied to an unnamed India-based manufacturing company on Exploit.

Source: Exploit **Actor:** decider

DATA BREACHES & LEAKS

CRITICAL **Data Allegedly Associated with Grand Est Automobiles Advertised**

On July 29, 2026, well-regarded threat actor "betway" advertised a data set allegedly associated with the France-based company Grand Est Automobiles on Exploit.

Source: Exploit **Actor:** betway

CRITICAL **Data Allegedly Associated with Metrics Call Services Advertised**

On July 29, 2026, betway advertised a data set allegedly associated with the U.S.-based company Metrics Call Services on Exploit.

Source: Exploit **Actor:** betway

NEW LEAKSITES, MARKETPLACES, FORUMS

HIGH **New Ransomware Leak Site Emerges**

On July 31, 2026, ZeroFox observed a new ransomware leak site named "GAMMAX." As of this report, the leak site lists two victims and is accessible via hXXp://gammax6w3dkfdjfrjthtmqzsioue52vzy6lz54qy6jcvmogfpubutjyd[.]onion/

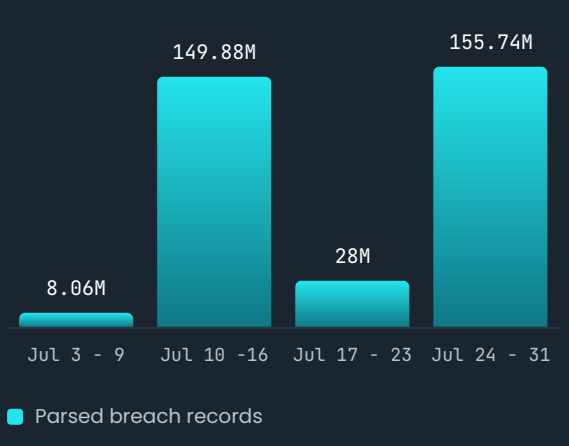
Source: Leak Site **Actor:** GAMMAX

PROCESSED DATA SET STATISTICS

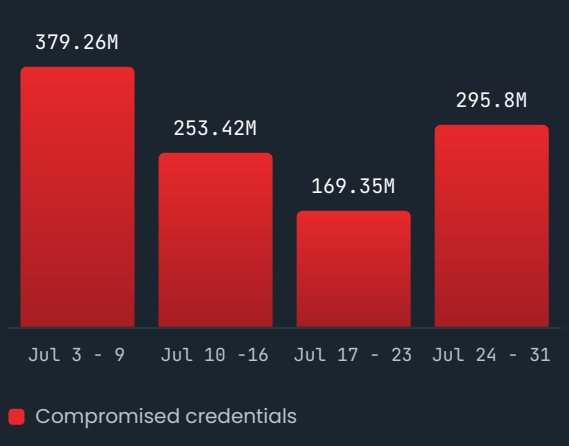
Past 4 Weeks

341.68M	1.09B	874
CAC RECORDS	BOTNET CAC RECORDS	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.