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.

July 27, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

6 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
Qilin Ransomware	Stryker
Nova Ransomware	Digital Edge
Akira Ransomware	Emerge2 Digital
The Gentlemen Ransomware	Mattek
Play Ransomware	The DeBruler Company
SETTRA Ransomware	Royal Chain Group

DEEP AND DARK WEB INTELLIGENCE

6 findings

CRITICAL FINDINGS

CRITICAL **Root CMS Access Allegedly Tied to Nine Organizations Across Multiple Regions and Sectors Advertised**

On July 25, 2026, untested threat actor "xpl0itrs" advertised root-level Content Management System (CMS) access allegedly associated with nine organizations across the pharmaceutical, fintech, banking, healthcare IT, logistics, and government sectors, on the predominantly English-language deep and dark web forum Spear.

Source: Spear **Actor:** xpl0itrs

CRITICAL **Alleged Credentials for Multiple Geospatial and Satellite Imagery Platforms Advertised**

On July 23, 2026, untested threat actor "NightOwl" advertised alleged login credentials for multiple geospatial and satellite imagery platforms on the predominantly English-language dark web forum DarkForums.

Source: DarkForums **Actor:** NightOwl

CRITICAL **Alleged Pre-Configured Google Workspace Enterprise Plus Email Infrastructure Advertised**

On July 23, 2026, an untested threat actor "OmniMarketer" advertised pre-configured Google Workspace Enterprise Plus email infrastructure packages on the predominantly Russian-language deep and dark web forum Exploit.

Source: Exploit **Actor:** OmniMarketer

UNAUTHORIZED ACCESS CLAIMS

HIGH **Alleged RDWeb Access Tied to Sweden-Based Marine and Industrial Engines Supplying Company Advertised**

On July 24, 2026, an untested threat actor "dogs" advertised an auction for RDWeb access with local administrator rights allegedly associated with an unnamed Sweden-based marine and industrial engines supplying company on the predominantly Russian-language deep and dark web forum Exploit.

Source: Exploit **Actor:** dogs

HIGH **Alleged RDWeb Access Tied to U.S.-Based Real Estate Company Advertised**

On July 24, 2026, an untested threat actor "dogs" advertised an auction for RDWeb access with domain user rights allegedly associated with an unnamed U.S.-based real estate company on the predominantly Russian-language deep and dark web forum Exploit.

Source: Exploit **Actor:** dogs

NEW LEAKSITES, MARKETPLACES, FORUMS

HIGH **New Ransomware Leak Site Emerges**

On July 27, 2026, ZeroFox observed a new ransomware leak site named "GLOBAL SECRET GROUP." As of this report, the leak site lists 25 disclosed and 6 undisclosed victims and is accessible via the following dark web addresses:
hXXp://4xfjswmkehxwjoa2dgpvfezdepf6c7qfj5gdm2kkdwhkgyxirhn6mbqd[.]onion/
hXXp://o5lsqyar7ox25z734k6zaxt2vf7bsyi4q5rturi5iyxzqo3ica7bjsad[.]onion

Source: Leak Site **Actor:** GLOBAL SECRET GROUP

COLLECTED, PROCESSED DATA BREACHES

1 entries

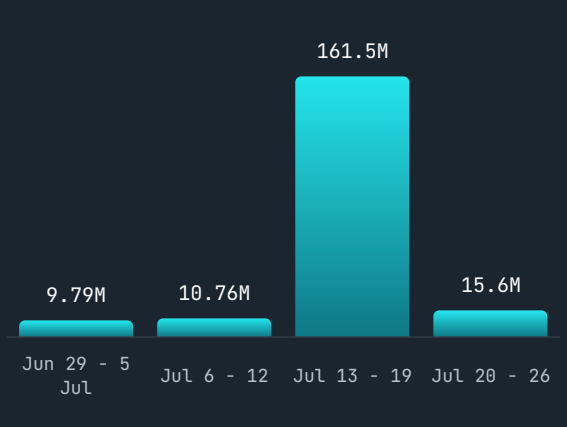
VICTIM	SOURCE	THREAT ACTOR	PROCESSED RECORDS
Timer Immobilier (timer-immobilier[.]fr)	PwnForums	0xSec	993

PROCESSED DATA SET STATISTICS

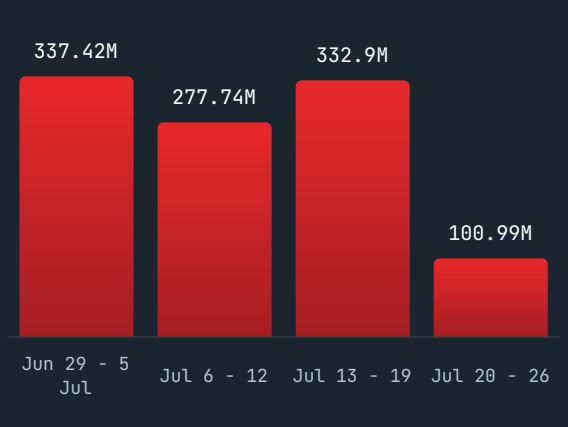
Past 4 Weeks

197.65M	1.04B	701
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.