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 17, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

5 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
ShinyHunters	Baxter International
ShinyHunters	Sharecare
Clop Ransomware	Shell
Rhysida Ransomware	Pierce Township
LeakedData	Riker Danzig

VULNERABILITY DISCLOSURES

1 disclosure

CVE-2026-65400

Authentication Bypass Vulnerability in Apple macOS Screen Sharing

DEEP AND DARK WEB INTELLIGENCE

6 findings

CRITICAL FINDINGS

CRITICAL **Data Allegedly Associated with National Grid Leaked**

On August 14, 2026, untested threat actor "Amiri" leaked a dataset allegedly associated with National Grid on the predominantly English-language DDW forum PwnForums.

Source: PwnForums **Actor:** Amiri

CRITICAL **Data Allegedly Associated with SafePal Advertised (supermonk44)**

On August 16, 2026, untested threat actor "supermonk44" advertised a database allegedly associated with SafePal on the predominantly English-language DDW forum Spear.

Source: Spear **Actor:** supermonk44

CRITICAL **Corporate Azure Tenant Databases Allegedly Tied to Multiple Companies Advertised**

On August 16, 2026, untested threat actor "TheHatman" advertised alleged internal employee databases of three major global corporations for sale on the predominantly English-language DDW forum DarkForums.

Source: DarkForums/PwnForums **Actor:** TheHatman

VULNERABILITY EXPLOITATION

HIGH **Alleged SQL Injection Vulnerabilities in Three OpenCart Plugins Advertised**

On August 14, 2026, moderately credible threat actor "grantall" advertised an auction for three SQL injection vulnerabilities allegedly present in OpenCart plugins on the predominantly Russian-language DDW forum Exploit.

Source: Exploit **Actor:** grantall

DATA BREACHES & LEAKS

HIGH **Data Allegedly Associated with CoFoundersLab Advertised**

On August 13, 2026, well-reputed threat actor "betway" advertised a dataset allegedly associated with CoFoundersLab, on Exploit.

Source: Exploit **Actor:** betway

UNAUTHORIZED ACCESS CLAIMS

HIGH **AnyDesk Access Allegedly Tied to UK-Based Financial Services Company Advertised**

On August 13, 2026, untested threat actor "Toton" advertised AnyDesk access with domain user rights allegedly tied to an unnamed UK-based financial services company on DarkForums.

Source: DarkForums **Actor:** Toton

COLLECTED, PROCESSED DATA BREACHES

2 entries

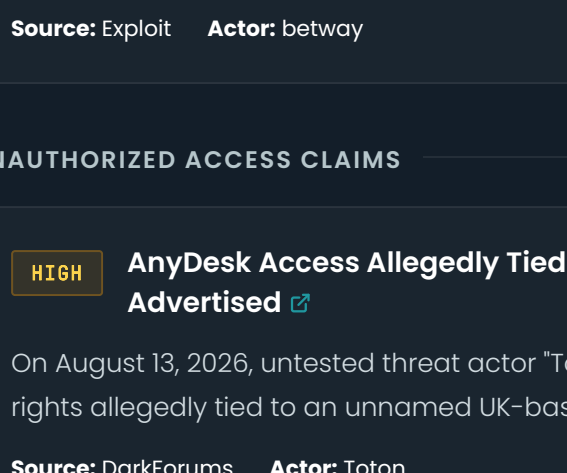
VICTIM	SOURCE	THREAT ACTOR	PROCESSED RECORDS
apps.education[.]fr	PwnForums	misere	143.47K
nanaricloud[.]com	PwnForums	0xSec	214

PROCESSED DATA SET STATISTICS

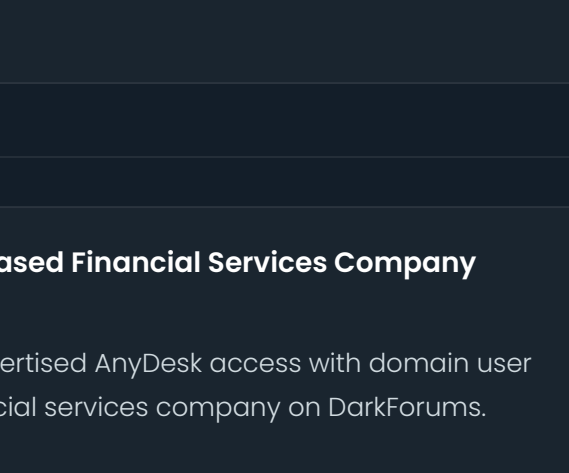
Past 4 Weeks

858.32M	865.44M	919
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.