

Deep and Dark Web Intelligence Reporting

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

October 20, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

6 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
Qilin Ransomware	SkyWorld Air Cargo
Qilin Ransomware	GardaWorld
Everest	Taekwang Network Information
Vexy Ransomware	Data-Core Systems
Play Ransomware	WSBI-ESBG
N0n Ransomware	ABT

VULNERABILITY DISCLOSURES

3 disclosures

CVE-2026-97205

Use After Free Vulnerability in F5 NGINX

CVE-2026-93479

Heap-Based Buffer Overflow Vulnerability in F5 NGINX

CVE-2026-15176

Heap-Based Buffer Overflow Vulnerability in F5 NGINX

DEEP AND DARK WEB INTELLIGENCE

10 findings

DATA BREACHES & LEAKS

CRITICAL

Data Allegedly Associated with U.S. Department of Homeland Security Advertised

On October 19, 2026, untested threat actor "INS" advertised data allegedly associated with the U.S. Department of Homeland Security (DHS) on a predominantly English-language DDW forum PwnForums.

Source: PwnForums Actor: INS

HIGH

Data and Source Code Allegedly Associated with Safety, Health and Environment National Authority Leaked

On October 19, 2026, moderately credible threat actor "bytestobreach" leaked data and source code allegedly associated with the Safety, Health and Environment National Authority (SHENA) of Brunei on a predominantly Russian-language DDW forum Exploit.

Source: Exploit Actor: bytestobreach

HIGH

Data Allegedly Tied to Argentine Airlines Advertised

On October 17, 2026, an untested threat actor "maiuishi" advertised a data set likely associated with the Argentina-based company Aerolíneas Argentinas (Argentine Airlines) on Exploit.

Source: Exploit Actor: maiuishi

HIGH

Data Allegedly Tied to U.S.-Based Platform ZoomInfo Advertised

On October 18, 2026, an untested threat actor "Compiler" advertised a data set allegedly associated with Zoominfo on a predominantly Russian-language DDW forum XSS.

Source: XSS Actor: Compiler

HIGH

Data Allegedly Tied to U.S.-Based Company FV Bank Advertised

On October 15, 2026, an untested threat actor "Marx1337" advertised a data set allegedly associated with the U.S.-based global digital banking company, FV Bank, on XSS.

Source: XSS Actor: Marx1337

UNAUTHORIZED ACCESS CLAIMS

HIGH

Network Access Allegedly Tied to France-Based Mutual Insurance Company Advertised

On October 17, 2026, a moderately credible threat actor "Syrv4x" advertised intranet portal access allegedly associated with an unnamed France-based mutual insurance company on PwnForums.

Source: PwnForums Actor: Syrv4x

HIGH

Network Access Allegedly Tied to U.S.-Based Investment Company Advertised

On October 18, 2026, an untested threat actor "xzaffair" advertised access allegedly tied to a U.S.-based investment company on Exploit.

Source: Exploit Actor: xzaffair

HIGH

Fortinet Access Allegedly Tied to Turkey-Based Financial Services Company Advertised

On October 18, 2026, a well-known threat actor "Big-Bro" advertised an auction for Fortinet access with domain user rights allegedly tied to an unnamed Turkey-based financial services company on Exploit.

Source: Exploit Actor: Big-Bro

HIGH

Shell Access Allegedly Tied to Slovakia-Based Telecommunications Company Advertised

On October 17, 2026, an untested threat actor "scorpius-xi" advertised shell access with root rights allegedly tied to an unnamed Slovakia-based telecommunications company on Exploit.

Source: Exploit Actor: scorpius-xi

VULNERABILITY EXPLOITATION

HIGH

Alleged Zero-Day Exploit for Ledger Wallet Desktop Application Advertised

On October 16, 2026, an untested threat actor "work159" advertised an alleged zero-day exploit for the Ledger Wallet desktop application on XSS.

Source: XSS Actor: work159

COLLECTED, PROCESSED DATA BREACHES

1 entries

VICTIM	SOURCE	THREAT ACTOR	PROCESSED RECORDS
udemy[.]com	ShinyHunters	ShinyHunters	1.4M

PROCESSED DATA SET STATISTICS

Past 4 Weeks

530.43M

CAC RECORDS

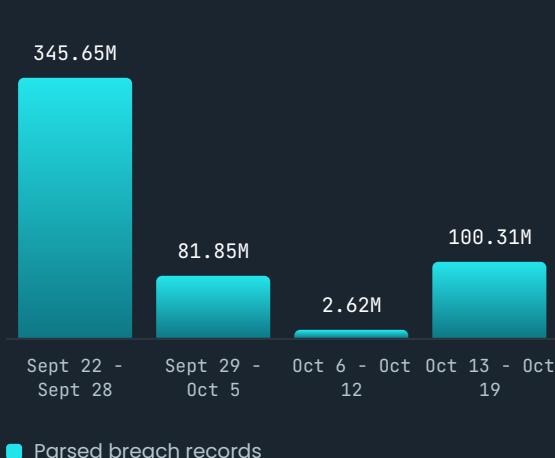
1.08B

BOTNET CAC RECORDS

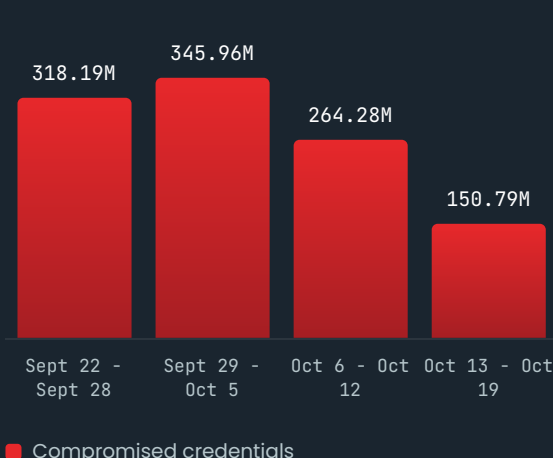
1.01K

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.