ZEROFOX

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.

September 9, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

7 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
SafePay Ransomware	Assiprime
SafePay Ransomware	Recovery Cafe
Eclipse Ransomware	Zhou Law Group
Metaencryptor Ransomware	ST Engineering
Qilin Ransomware	PARTNERS GROUP SK
INC Ransomware	Community Wellness Partners
The Gentlemen Ransomware	University of San Francisco

VULNERABILITY DISCLOSURES

4 disclosures

CVE-2026-81963
Elevation of Privilege Vulnerability in Microsoft Windows Update Stack

CVE-2026-85880
Heap-Based Buffer Overflow Vulnerability in Microsoft Windows ALPC

CVE-2026-76578
Missing Authentication Vulnerability for Critical Function in FreeIPA

CVE-2026-58240
Missing Authentication Vulnerability for Critical Function in SAP NetWeaver Message Server

DEEP AND DARK WEB INTELLIGENCE

7 findings

CRITICAL FINDINGS

CRITICAL **Threat Actor Claims Cyberattacks on U.S. Telecommunications and Water Utility Infrastructure in Texas**

On September 9, 2026, a pro-Iran threat actor group "APT IRAN" claimed, via their Telegram channel, to have conducted cyberattacks against telecommunications and water infrastructure in Texas.

Source: Telegram **Actor:** APT IRAN

CRITICAL **Alleged LPE Targeting Windows Advertised**

On September 8, 2026, well-regarded threat actor "wdosx" advertised an alleged local privilege escalation (LPE) exploit, targeting Windows, on the predominantly Russian-language DDW forum Exploit.

Source: Exploit **Actor:** wsdosx

UNAUTHORIZED ACCESS CLAIMS

CRITICAL **Network Access Allegedly Tied to U.S.-Based Healthcare Company Advertised**

On September 8, 2026, untested threat actor "MrW3ite" advertised network access allegedly associated with an unnamed U.S.-Based healthcare company on the predominantly English-language DDW forum PwnForums.

Source: PwnForums **Actor:** MrW3ite

HIGH **RDP Access Allegedly Tied to Serbia-Based Company Advertised**

On September 7, 2026, well-known threat actor "Big-Bro" advertised an auction for RDP access with domain user rights allegedly associated with an unnamed Serbia-based company on Exploit.

Source: Exploit **Actor:** Big-Bro

HIGH **VPN Access Bundle Allegedly Tied to Three Portugal-Based Companies Advertised**

On September 7, 2026, moderately credible threat actor "personX" advertised VPN access bundle with domain administrator, domain user and local administrator rights allegedly associated with three undisclosed Portugal-based companies on Exploit.

Source: Exploit **Actor:** personX

DATA BREACHES & LEAKS

HIGH **Document Allegedly Associated with SpaceX Starshield Architecture Advertised**

On September 8, 2026, untested threat actor "Zerotrace61" advertised internal documents allegedly associated with the SpaceX Starshield program, on the predominantly English-language DDW forum DarkForums.

Source: DarkForums **Actor:** Zerotrace61

HIGH **Data Allegedly Associated with Italy-Based Financial Institutions Advertised**

On September 8, 2026, untested threat actor "KimOCW" advertised a dataset allegedly associated with Italy-based financial institutions on Exploit.

Source: Exploit **Actor:** KimOCW

COLLECTED, PROCESSED DATA BREACHES

1 entries

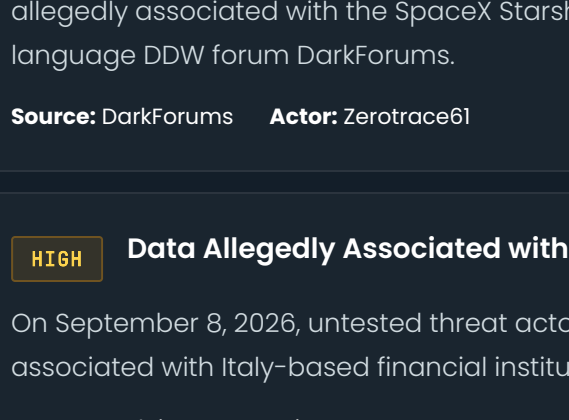
VICTIM	SOURCE	THREAT ACTOR	PROCESSED RECORDS
bcdtravel[.]com	ShinyHunters	ShinyHunters	301.46K

PROCESSED DATA SET STATISTICS

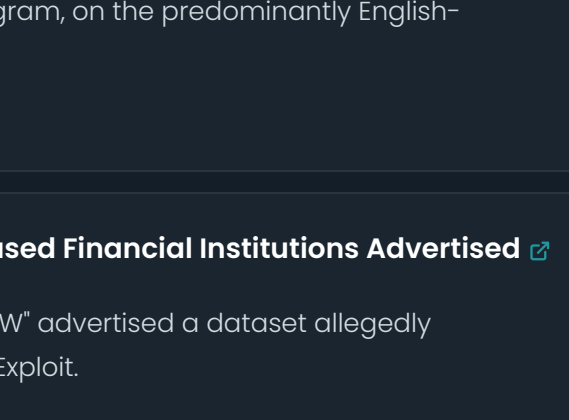
Past 4 Weeks

882.36M	1.08B	1.05K
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.