

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 29, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

5 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
M3RX Ransomware	Cipher Systems
Qilin Ransomware	Island Corporation
Qilin Ransomware	Willatt & Flickinger
INC Ransomware	North Slope Borough School District
INTERLOCK Ransomware	The Center for Kidney Care

DEEP AND DARK WEB INTELLIGENCE

11 findings

CRITICAL FINDINGS

CRITICAL

Live PMS Access and Databases Allegedly Associated with India-Based Hospitality Sector Advertised

On September 26 and 27, 2026, moderately credible threat actor "DDEEAALLEERR" published two separate posts on a predominantly Russian-language DDW forum Exploit, advertising live property management system (PMS) access and associated databases allegedly affecting the Indian hospitality sector.

Source: Exploit Actor: DDEEAALLEERR

CRITICAL

Data Allegedly Associated with Bouclair Advertised

On September 27, 2026, untested threat actor "bleedingout" advertised a data allegedly associated with Bouclair on Exploit.

Source: Exploit Actor: bleedingout

CRITICAL

Data Allegedly Associated with Easy Cosmetic Advertised

On September 27, 2026, untested threat actor "bleedingout" advertised data allegedly associated with Easy Cosmetic on Exploit.

Source: Exploit Actor: bleedingout

CRITICAL

Data Allegedly Associated with Alaxione Advertised

On September 28, 2026, moderately credible threat actor "ChimeraZ" advertised a database allegedly associated with Alaxione on a predominantly English-language DDW forum PwnForums.

Source: PwnForums Actor: ChimeraZ

CRITICAL

Alleged Compromise of Indian Government, ISP, and Healthcare Infrastructure Advertised

On September 28, 2026, well-reputed threat actor "bytestobreach" advertised the alleged compromise of multiple Indian networks—including government infrastructure, ISP Microscan, and GVK EMRI Healthcare—on Exploit.

Source: Exploit Actor: bytestobreach

UNAUTHORIZED ACCESS CLAIMS

HIGH

Alleged Insider Access to Anthropic Advertised

On September 26, 2026, untested threat actor "sydneysweeneywhy" advertised alleged insider access to Anthropic's infrastructure and services on a predominantly English-language DDW forum BreachForums (bf[.]st).

Source: BreachForums Actor: sydneysweeneywhy

VULNERABILITY EXPLOITATION

HIGH

Alleged Oracle PeopleSoft Pre-Auth RCE and WAF Bypass Exploit Advertised

On September 28, 2026, untested threat actor "ShinyHunters" advertised a working pre-authentication remote code execution exploit allegedly associated with Oracle PeopleSoft, along with an accompanying web application firewall bypass, on BreachForums (bf[.]st).

Source: BreachForums Actor: ShinyHunters

HIGH

Alleged Windows Defender Update Pipeline DoS Exploit Advertised

On September 29, 2026, well-reputed threat actor "QatarRat" advertised a Windows Defender update pipeline Denial of Service (DoS) exploit on Exploit.

Source: Exploit Actor: QatarRat

HIGH

Alleged WhatsApp Android RCE Exploit Advertised

On September 26, 2026, untested threat actor "xynapse" advertised an alleged remote code execution (RCE) exploit for WhatsApp on Android on BreachForums (bf[.]st).

Source: BreachForums Actor: xynapse

HIGH

Alleged Chromium Remote Code Execution Exploit Chain Advertised

On September 26, 2026, the untested threat actor "xynapse" advertised an alleged remote code execution exploit chain targeting Google Chrome and Chromium-based browsers on Windows 10 and Windows 11 environments on BreachForums (bf[.]st).

Source: BreachForums Actor: xynapse

HIGH

Alleged iOS Zero-Day Exploit dubbed "VERMAN" Advertised

On September 26, 2026, untested threat actor "sydneysweeneywhy" advertised an alleged iOS zero-day exploit dubbed "VERMAN" on the predominantly English-language deep and dark web forum BreachForums (bf[.]st).

Source: BreachForums Actor: sydneysweeneywhy

COLLECTED, PROCESSED DATA BREACHES

4 entries

VICTIM	SOURCE	THREAT ACTOR	PROCESSED RECORDS
carhartt[.]com	ShinyHunters	ShinyHunters	21.37M
verisure[.]se	PwnForums	Emzywemzy	33.14K
deliver2alaska[.]com	PwnForums	gloomer	3.31K
uptapachula[.]edu[.]mx	PwnForums	Z3r00	743

PROCESSED DATA SET STATISTICS

Past 4 Weeks

378.29M

CAC RECORDS

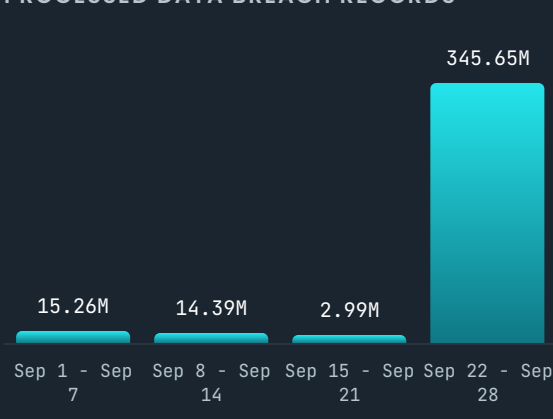
1.19B

BOTNET CAC RECORDS

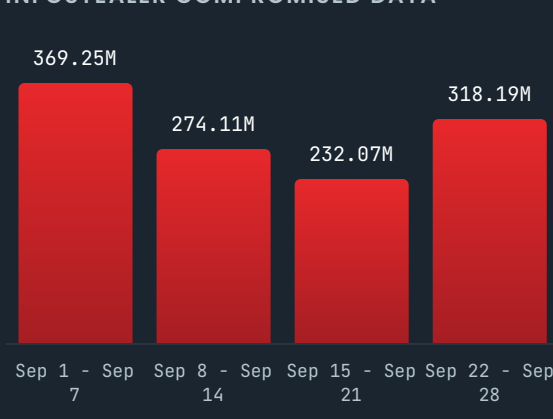
867

RANSOMWARE & DIGITAL EXTORTION

PROCESSED DATA BREACH RECORDS



INFESTEALER 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.