ZEROFOX

Deep and Dark Web Intelligence Reporting

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

July 10, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

4 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
Nova Ransomware	Hynet
Payload Ransomware	Commune de Castries
Qilin Ransomware	Alan F Burke
Qilin Ransomware	Inter Power Engineering

VULNERABILITY DISCLOSURES

1 disclosure

CVE-2026-50656

Elevation of Privilege in Microsoft Defender Malware Protection Engine

DEEP AND DARK WEB INTELLIGENCE

8 findings

CRITICAL FINDINGS

CRITICAL **Data Allegedly Tied to Indian Armed Forces Advertised**

On July 9, 2026, untested threat actor "Slepra" (slepra on DarkForums) advertised alleged data associated with "Army Air Defence India Data" likely refering to Indian Armed Forces, on predominantly English- and Russian-language deep and dark web forums DarkForums and XSS respectively.

Source: XSS/DarkForums **Actor:** Slepra

CRITICAL **Data Allegedly Associated with Glassnode Advertised**

On July 10, 2026, an untested threat actor "iluvxmr" advertised data allegedly associated with Glassnode, on a predominantly Russian-language deep and dark web forum Exploit.

Source: Exploit **Actor:** iluvxmr

CRITICAL **Partial Data Allegedly Associated with Moove Leaked**

On July 9, 2026, an untested threat actor “slvsh3r” breached partial data allegedly associated with Moove, on a predominantly English-language deep and dark web forum PwnForums.

Source: PwnForums **Actor:** slvsh3r

CRITICAL **Data Allegedly Associated with L’Assurance Maladie Advertised**

On July 9, 2026, an untested threat actor "yaserbakhtiary0111" advertised data allegedly associated with L’Assurance Maladie, on a predominantly English-language dark web forum DarkForums.

Source: DarkForums **Actor:** yaserbakhtiary0111

UNAUTHORIZED ACCESS CLAIMS

HIGH **Alleged SSH and FortiGate Access Bundle Associated with 1,985 UAE-Based Companies Advertised**

On July 9, 2026, an untested threat actor "APL-BRK" advertised to sell SSH and FortiGate access bundle with super_admin rights allegedly associated with 1,985 undisclosed UAE-based companies, on a predominantly Russian-language deep and dark web forum XSS. Notably, on that same date, an identical advertisement was posted on the dark web forum DarkForums by the threat actor "Dark_Alpha.

Source: XSS/DarkForums **Actor:** APL-BRK, Dark_Alpha

HIGH **Alleged Network Access Tied to Undisclosed Argentina-Based Company Advertised**

On July 9, 2026, a well-known threat actor "Big-Bro" advertised an auction for network access with domain user rights allegedly associated with an undisclosed Argentina-based company, on a predominantly Russian-language deep and dark web forum Exploit.

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

HIGH **Alleged RDP and Fortinet Access Tied to Israel-Based Business Services and Software Testing Company Advertised**

On July 9, 2026, a moderately credible threat actor "HelluvaHack" advertised to sell RDP and Fortinet access allegedly associated with an unnamed Israel-based business services and software testing company, on a predominantly Russian-language deep and dark web forum Exploit.

Source: Exploit **Actor:** HelluvaHack

NEW LEAKSITES, MARKETPLACES, FORUMS

HIGH **New Ransomware Leak Site Emerges**

On July 9, 2026, ZeroFox observed a new ransomware data leak site (DLS) operating under the name "CRPx0." At the time of reporting, the leak site listed six alleged victims, all of which operate in the healthcare sector based out of the United States and China. The leak site is accessible through the following dark web and clearnet addresses: hXXps://crpx0[.]su hXXp://tlxoddx4odmc2qvsmtsbgwwsv5j45osb5sox7mz6izxliuju5mkulzad[.]onion

Source: Leak Site **Actor:** CRPx0

COLLECTED, PROCESSED DATA BREACHES

4 entries

VICTIM	SOURCE	THREAT ACTOR	PROCESSED RECORDS
picwpost[.]com	BreachForums	X0Frankenstein	38.5K
cyprusairways[.]com	PwnForums	purplepancake49	7.9K
[MEXICO] SEED Durango Schools Leak – 19 Primaries, 3k Students & Parents	DarkForums	D3spair157	2.1K
ralphlauren[.]global	ShinyHunters	ShinyHunters	140.3K

PROCESSED DATASET STATISTICS

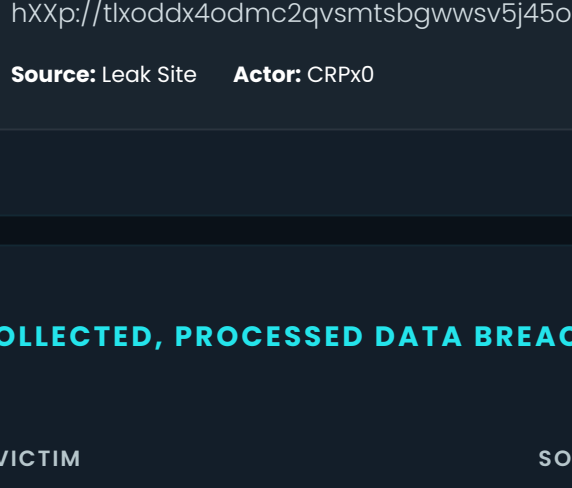
Past 4 Weeks

672.1M CAC RECORDS

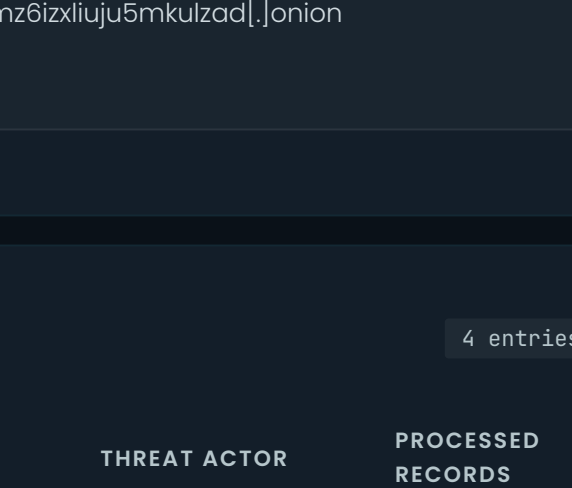
1.1B BOTNET CAC RECORDS

792 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, bizarre tactics, and significant operational spikes that deviate from the baseline threat landscape.