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.

August 19, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

5 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
ShinyHunters	Logitech
SECUROTROP Ransomware	ADL Embedded Solutions
Dire Wolf Ransomware	Colla Health
Qilin Ransomware	Teikoku Pharma USA
Clop Ransomware	G3 Aerospace

VULNERABILITY DISCLOSURES

2 disclosures

CVE-2026-19478

Code Injection Vulnerability in GitLab CE/EE GraphQL API

CVE-2025-62593

Code Injection Vulnerability in Ray-Project Ray

DEEP AND DARK WEB INTELLIGENCE

7 findings

CRITICAL FINDINGS

CRITICAL **Data Allegedly Associated with WorkL Leaked**

On August 18, 2026, well-regarded threat actor "Satanic" leaked a database allegedly associated with WorkL, a UK-based digital workplace intelligence platform, on the predominantly English-language DDW forums PwnForums.

Source: PwnForums **Actor:** Satanic

CRITICAL **Target List and Public POC Allegedly Tied to Citrix NetScaler Pre-Auth RCE CVE-2026-8451 Leaked**

On August 19, 2026, untested threat actor, "caustic," shared a target list and a link to a publicly available proof-of-concept (POC) exploit allegedly tied to CVE-2026-8451 and CVE-2026-8452 on the predominantly Russian-language DDW forums Exploit.

Source: Exploit **Actor:** caustic

NEW LEAKSITES, MARKETPLACES, FORUMS

CRITICAL **New Data Leak Site Emerges**

On August 18, 2026, ZeroFox observed a new data leak site operating under the name "xpl0itrs." As of this report, the leak site lists four disclosed victims and two redacted victims, and is accessible via the following dark web address:hxxp://2kieaq6jnwgrru62wwtxaafg35q6rzweg7y2xjfnbhvq5wd4eojqv6yd[.]onion/

Source: Leak Site **Actor:** xpl0itrs

VULNERABILITY EXPLOITATION

CRITICAL **Alleged RCE Exploit Targeting Chainlink Network Advertised**

On August 17, 2026, untested threat actor "shredder00" advertised an alleged Remote Code Execution (RCE) exploit targeting the Chainlink network on the predominantly English-language DDW forums DarkForums and PwnForums.

Source: DarkForums/PwnForums **Actor:** shredder00

UNAUTHORIZED ACCESS CLAIMS

HIGH **RDWeb Access Allegedly Tied to U.S.-Based Manufacturing Company Advertised**

On August 17, 2026, well-known threat actor "Big-Bro" advertised an auction for RDWeb access with domain user rights allegedly tied to an unnamed U.S.-based manufacturing company on Exploit.

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

HIGH **SSH and FortiGate Access Allegedly Tied to U.S.-Based Retail Company Advertised**

On August 18, 2026, untested threat actor "SCP-2013" (likely known as "APL-BRK" and "Dark_Alpha") advertised SSH and FortiGate access with super_admin rights allegedly tied to an unnamed U.S.-based retail company on the predominantly Russian-language and English-language DDW forums Exploit, XSS, and DarkForums.

Source: Exploit/XSS/DarkForums **Actor:** SCP-2013, APL-BRK, Dark_Alpha

HIGH **RDP Access Allegedly Tied to Crypto Exchange Company Advertised**

On August 17, 2026, untested threat actor "Omsk" advertised RDP access allegedly tied to an undisclosed "MAJOR" crypto exchange company on the predominantly English-language DDW forums Spear.

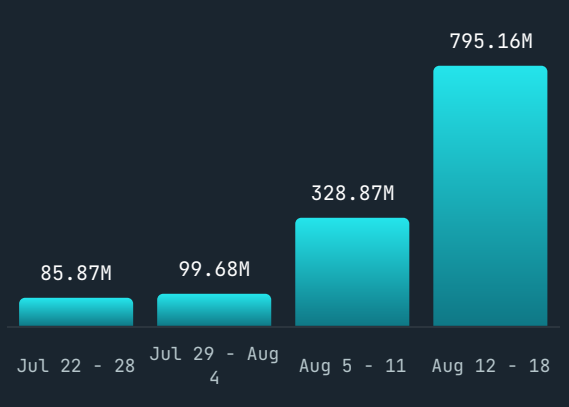
Source: Spear **Actor:** Omsk

PROCESSED DATA SET STATISTICS

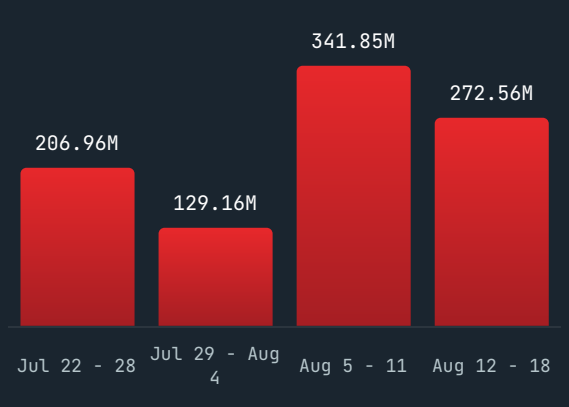
Past 4 Weeks

1.31B	950.53M	976
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.