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 2, 2026

RANSOMWARE / DIGITAL EXTORTION VICTIMS

5 incidents

THREAT ACTOR / GROUP	VICTIM ORGANIZATION
The Gentlemen Ransomware	Nutex Health
LockBit 5.0 Ransomware	Susquehanna Valley Federal Credit Union
Akira Ransomware	Gale Credit Union
INTERLOCK Ransomware	Super Systems
Payouts King Ransomware	Proliance Surgeons

DEEP AND DARK WEB INTELLIGENCE

4 findings

CRITICAL FINDINGS

CRITICAL **Alleged Identity Verification Service Breach and "NEXUS" Document Marketplace Advertised**

On August 31, 2026, untested threat actor "databroker1" advertised a custom portal named "NEXUS" on the predominantly Russian-language DDW forum Exploit, claiming the portal hosts a database of over 160 million breached identity documents.

Source: Exploit **Actor:** databroker1

HIGH **RaaS Partnership Program Dubbed "Wallstreet" Advertised**

On August 31, 2026, untested threat actor "Wallstreet" advertised a Ransomware-as-a-Service (RaaS) partnership program called "Wallstreet" on the predominantly Russian-language deep web forum DUTY-FREE.

Source: DUTY-FREE **Actor:** Wallstreet

DATA BREACHES & LEAKS

CRITICAL **Data Allegedly Associated with Manchester Airports Group Leaked By FulcrumSec**

On September 2, 2026, ZeroFox observed the threat actor group "FulcrumSec" released approximately 549 GB of data allegedly exfiltrated from the Manchester Airports Group (MAG) on their data leak site.

HIGH **Data Allegedly Associated with Veronica's Insurance, Labcito, and Fixtman Advertised**

On September 2, 2026, a well-regarded threat actor "betway" published three separate posts on Exploit, each advertising a distinct victim's database of over 680k, 900k, and 147k records respectively, for a combined total of over 1.7 million alleged customer leads exfiltrated from commercial organizations in the United States and Indonesia.

Source: Exploit **Actor:** betway

COLLECTED, PROCESSED DATA BREACHES

1 entries

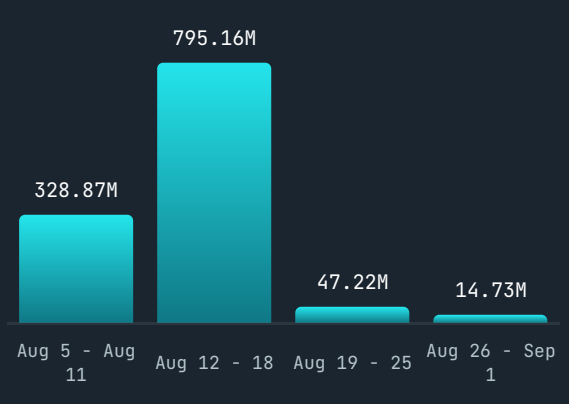
VICTIM	SOURCE	THREAT ACTOR	PROCESSED RECORDS
ringcentral[.]com	Exploit	Mister777	12.4K

PROCESSED DATA SET STATISTICS

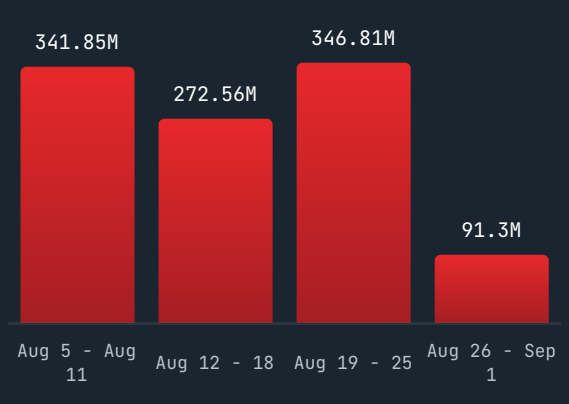
Past 4 Weeks

1.19B	1.05B	1.06K
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.