DARKNETSEARCH
BY KADUU

DARK & DEEP WEB CREDENTIAL LEAK COMPARISON REPORT

for

Monthly Report

Analysis Date Range: 2024-10-01 to 2025-10-15
Creation Date: October 15, 2025

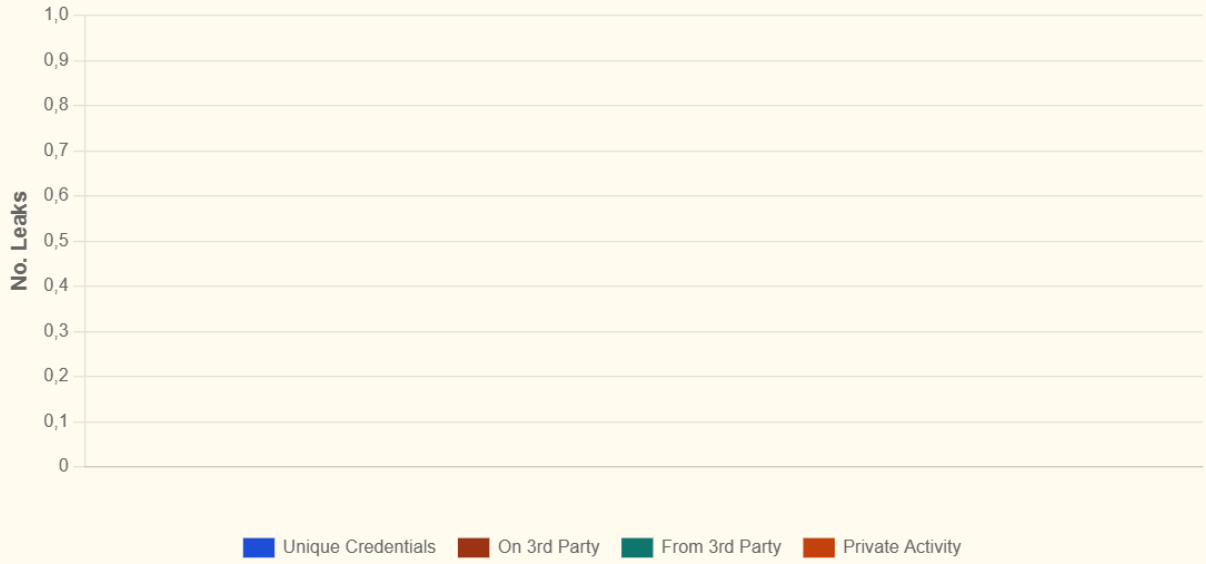
LEAK CREDENTIALS SUMMARY - 2024-10-01 to 2025-10-15

We display credentials (emails and passwords) for all **1** organization domain(s). The "Unique" column shows only accounts that appeared for the first time during the selected reporting period - **2024-10-01 to 2025-10-15**. Since threat actors often redistribute the same leaks multiple times across different hacker channels, many credentials tend to reappear in later leaks.

Leaked Credential Statistic Type	Unique Totals
Total Number of leaked credentials This number represents the aggregate count of credential records (email/username + password pairs) discovered across all data sources monitored by the system. It includes entries from stealer logs, combo lists, public breach dumps, paste sites, and proprietary feeds. Because the same credential can appear in multiple sources, this figure may include duplicates and should be treated as an indicator of exposure volume rather than a count of unique affected accounts.	**1093**
Credentials originating from Stealer Logs A stealer log is a dataset generated by malware known as a stealer. This type of malware is specifically designed to infiltrate a victim's device and extract sensitive information, which is then sent back to the attacker. As a result, stealer logs typically originate directly from infected victim machines. In contrast, a combolist is simply a collection of email and password pairs, usually with an unclear or unknown origin.	**793**
Credentials found in Combo Lists A combo list is a bulk collection of email/password pairs aggregated from many places—breach archives, automated scrapes, marketplace dumps and other public or semi-public sources. These lists are usually compiled without provenance and often contain old, recycled, or invalid pairs; they rarely indicate how or when the credentials were collected. Compared with stealer logs (which typically come directly from infected machines and are higher confidence), combo lists are lower fidelity but still valuable: presence in multiple combo lists or in both combo lists and stealer logs raises the likelihood that credentials are actively reused or valid.	**249**

3 Month Historical Leak Trends

Cumulative leak exposure across the past full three months.



TOP 3 EXTERNAL SYSTEMS WITH LEAKED EMPLOYEE CREDENTIALS

Employees may use their corporate email addresses to log in to applications provided by third-party vendors. These can include business-related platforms (e.g., Google Workspace or Office 365), but may also extend to non-business services—for example, when an employee uses their organizational account to sign in to platforms like Netflix.

**displaying accumulated data from analysis done over all 1 organization domain(s).*

Affected External Systems from Stealer Logs	Total
xxxxx	3
xxxxx	3
xxxxx/de/register	2

TOP 3 INTERNAL SYSTEMS WITH LEAKED CLIENT OR PARTNER CREDENTIALS

It is common for organizations to offer web services to clients, partners, or potential employees. For example, job applicants may register and apply for positions through the organization's website, or clients may access a dedicated client portal. In this section, we analyse how many login credentials associated with email addresses not belonging to the organization appear in stealer logs

**displaying accumulated data from analysis done over all 1 organization domain(s).*

Internal Systems used by 3rd party	Total
xxxxx	78
xxxxx	29
xxxxx	11

PASSWORD ANALYSIS

We found that **94** passwords are insecure. These passwords has less than 8 characters (or) no capital letters (or) no special characters (or) no numbers.

LEAKED CREDENTIALS COMPARISON BY DOMAIN - 2024-10-01 to 2025-10-15

- **Unique**: Removes duplicate accounts with the same server, username and password
- **Organization:** Filters accounts that contain the specified username substring
- **On Third Party:** Filters employee accounts on personal or sensitive services including streaming, adult content, gambling, dating, cryptocurrency, piracy, VPN/proxy, and social media platforms
- **Private Activity:** Filters employee accounts on personal or sensitive services including streaming, adult content, gambling, dating, cryptocurrency, piracy, VPN/proxy, and social media platforms
- **From Third Party:** Filters accounts that use external email addresses to log into the organization's infrastructure
- **Policy Match:** Credentials that meet your organization's password policy requirements
- **Weak Passwords:** Passwords that do not meet policy requirements

Domain	Unique	Org	On 3rd Party	Private	From 3rd Party	Policy Match	Weak Passwords
xxxxx	1093	94	101	0	198	0	94