2.8 Billion Credentials Stolen As Password Attacks Surge

Summary

The article describes the alarming rise in password credential theft, with 2.86 billion compromised credentials stolen in 2025. The article highlights the increasing reliance on stolen credentials as the primary access method for cybercriminals. The article also emphasizes the importance of using password managers, enabling two-factor authentication, and switching to passkeys as a more secure alternative to passwords.

Davey Winder May 01, 2026, 05:31am EDT

The infostealer password credential theft crimewave exposed.
getty

A newly published analysis of cybercrime statistics across 2025 has revealed that the number of ransomware victims surged by 45% over the previous year. But that's not the revelation that you need to pay the most attention to. Rather, the underlying reliance on stolen credentials as the primary access method takes center stage as far as I am concerned. No matter what platform you use, no matter what accounts you are protecting, the time to start taking password security seriously has long since passed.

The State of Cybercrime 2026 report from KELA identified no less than 2.86 billion compromised credentials, including passwords and session cookies that enable 2FA bypass. Shockingly, business cloud and authentication services accounted for more than 30% of this exposed data across 2025. What's more, the analysis showed that infostealer malware responsible for compromising credentials doesn't care about your operating system assumptions: "infections on macOS devices increased from fewer than 1,000 cases in 2024 to more than 70,000 in 2025, a 7,000% increase," the report confirmed.

Forbes No Microsoft Patch—All Windows Versions Likely At Risk From PhantomRPC By Davey Winder

Password Security — From Clicks To Credentials

I have been warning readers of the danger posed by infostealer malware for a number of years now. From millions of Gmail passwords contained in leaked infostealer logs,

to FBI operations aimed at taking down the cybercrime gangs behind the stolen password databases. Yet, as the KELA analysis has shown all too plainly, the threat continues. Not only does it continue, in fact, but it also surges year on year.

Infostealer malware, Kela explained, is "designed to exfiltrate sensitive data from compromised machines, including login credentials, authentication tokens, and other critical account information." And with the now almost universal availability of malware-as-a-service operations to the infostealer criminal world, the barrier to entry has not only been lowered but kicked to the curb completely.

Between January 1 and December 31, 2025, KELA said, it "observed approximately 3.9 million unique machines infected with infostealer malware globally, which collectively yielded 347.5 million compromised credentials." In total, however, KELA tracked a total of 2.86 billion compromised credentials across all sources, including databases of infostealer logs and the like that are available from criminal marketplaces.

ForbesGmail Accounts Under Persistent Hacking Attacks—'Always Be Wary'By Davey Winder

The Prompt: Get the week's biggest AI news on the buzziest companies and boldest breakthroughs, in your inbox.

The most common methods used by infostealers last year, according to the KELA report, were as follows:

- Email, messaging apps, and AI-generated personalized scams, often bypassing MFA via Phishing-as-a-Service.
- Users tricked into manually executing scripts, evading traditional security tools, in so-called hack your own password attacks.
- Malicious ads and search results push trojanized software, boosting infection rates.
- Poisoned packages and DevTools impersonation target high-privilege credentials in supply chain attacks.
- Compromised browser extension updates enable form-grabbing and cookie theft.
- Pirated apps and fake software updates also remained effective.

To mitigate against the risk of becoming just another statistic in next year's cybercrime report, it is advised that you **keep all software and operating systems updated**, **using official channels only**, and **never follow links in unsolicited emails or messages**, no matter how genuine they may seem. **Use a password manager** to ensure there is no sharing of passwords across accounts, limiting the impact of any single compromise. Always ensure that you **employ 2FA on all accounts where**

available, as this provides an additional layer of protection against password theft. That said, infostealers that compromise session cookies to bypass 2FA protections are now becoming commonplace. So, the final advice is to **switch to using passkeys** instead of a password wherever possible as these offer strength by default, phishing resistance and, importantly, because passkeys are randomly generated and never shared during the sign-in process, and your private keys never leave your device, they are all but impossible to compromise through interception or by the kind of infostealer malware covered by this article.

Forbes Update Safari Browser Before May 24—1Password Users Warned By Davey Winder