New Password-Stealing Malware Sells on Hacking Forum! Chrome, Binance, Outlook, Telegram Users Affected?

By Teejay Boris

Published: 2022-04-01 · Archived: 2026-04-05 15:11:59 UTC

New password-stealing malware is now being sold on dark hacking forum sites, which goes by the name BlackGuard.

Google Chrome Users Beware: Emergency Update Releases to Fix Zero-Day Security Vulnerability
In this file photo taken on August 04, 2020, Prince, a member of the hacking group Red Hacker Alliance who refused to give his real name, uses his computer at their office in Dongguan, China's southern Guangdong province. - As the number of online devices surges and super-fast 5G connections roll out. NICOLAS ASFOURI/AFP via Getty Images

New Password-Stealing Malware: BlackGuard

The new malware vows to attempt to steal user data from numerous platforms, such as Google Chrome, Binance, Microsoft's Outlook, Telegram, and tons more, as per a news story by Bleeping Computer.

The password-stealing malware primarily harvests sensitive information after cracking open various accounts on the platforms that it supports.

The news outlet further noted in the same report that the BlackGuard was first seen on Russian forums way back in January, which back then was still undergoing its testing phase.

But, this time around, the info-stealing malware is now being sold on numerous online hacker forums.

In fact, BlackGuard has rapidly grown into popularity-perhaps due to the recent demise of another malware aptly named the Raccoon Stealer.

BlackGuard vs. Apps

As mentioned, the new password-stealing malware seen in various hacking forums has an extensive list of apps that it vows to steal data from.

That said, users of top web browsers, such as Google Chrome, Firefox, Vivaldi, Microsoft Edge, and Opera, along with other less popular ones out there, could be affected by the new malware.

The data-stealing virus will try to steal various data from these browsers, including their history, autofill, cookies, and saved login credentials.

LONDON, ENGLAND - MAY 25: A close-up view of the Telegram messaging app is seen on a smart phone on May 25, 2017 in London, England. Telegram, an encrypted messaging app, has been used as a secure communications tool by Islamic State. Carl Court/Getty Images

What's more, users of messaging platforms like Signal, Telegram, Pidgin, and Discord should also beware of this malware, according to a recent report by ZDNet.

BlackGuard also targets wallet browser extensions, including Metamask, Ronin wallet, and Binance, to name a few.

On top of that, the password-stealing malware would also attempt to steal the data of cryptocurrency wallet users, namely, LitecoinCore, AtomicWallet, Electrum, Ethereum, Exodus, and a lot more.

ZDNet said in the same report that the malware would attempt to harvest the wallet address and private keys of the users of these crypto platforms.

It attempts to steal data from users of massive VPN apps, such as OpenVPN, ProtonVPN, and NordVPN.

For email clients, BlackGuard will only attempt to crack the accounts of Outlook users.

However, it is worth noting that the malware also includes the giant gaming platform, Steam, to its list of targeted apps.

This article is owned by Tech Times

Written by Teejay Boris