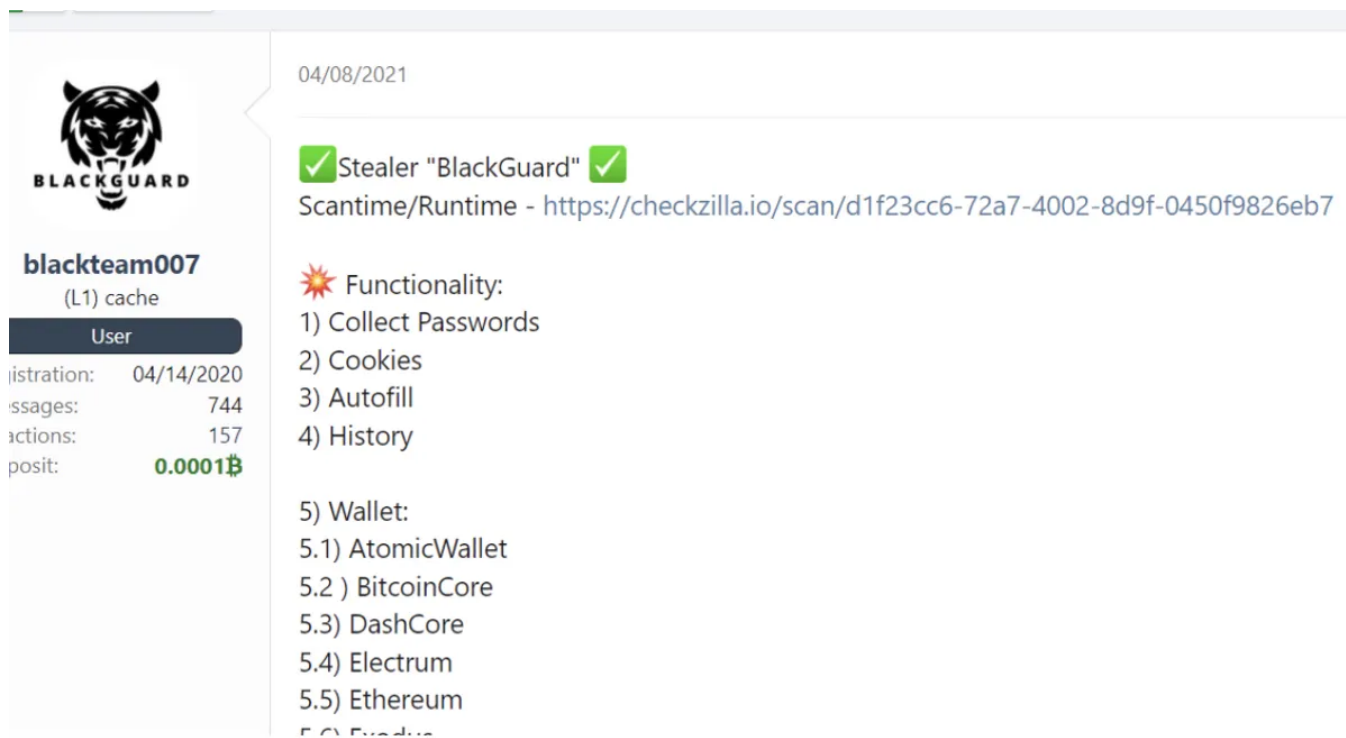


# Meet BlackGuard: a new infostealer peddled on Russian hacker forums

zdnet.com/article/meet-blackguard-a-new-infostealer-peddled-on-russian-hacker-forums/



The screenshot shows a forum post for a malware called "BlackGuard". On the left is a user profile for "blackteam007" (L1) cache, with a "User" button and statistics: registration 04/14/2020, messages 744, actions 157, and a deposit of 0.0001\$. The post itself is dated 04/08/2021 and features a green checkmark icon. The title is "Stealer 'BlackGuard'" with another green checkmark. Below the title is a URL: "Scantime/Runtime - https://checkzilla.io/scan/d1f23cc6-72a7-4002-8d9f-0450f9826eb7". The post lists the malware's functionality:

- ☀️ Functionality:
  - 1) Collect Passwords
  - 2) Cookies
  - 3) Autofill
  - 4) History
  - 5) Wallet:
    - 5.1) AtomicWallet
    - 5.2) BitcoinCore
    - 5.3) DashCore
    - 5.4) Electrum
    - 5.5) Ethereum

Home Innovation Security  
Sophisticated, but potentially cheap.



Written by [Charlie Osborne, Contributor](#) on March 31, 2022

- 
- 
- 
- 
- 

Researchers have uncovered a new infostealer malware being peddled in Russian underground forums.

Dubbed [BlackGuard](#), zScaler says that the new malware strain is "sophisticated" and has been made available to criminal buyers for a monthly price of \$200.

Infostealers are forms of malware designed to harvest valuable data, potentially including operating system information, contact lists, screenshots, network traffic, and online account credentials including those used to access financial services and banking.

A range of malicious software and exploit kits are sold every day underground, some of which are purchased outright. In contrast, others are offered on a malware-as-a-service (MaaS) basis: subscribers pay on a weekly, monthly, or yearly basis, and the developer keeps their malicious creations updated in return.

Perhaps to build a customer base for this malware, or to generate cash quickly, BlackGuard is also being sold for \$700 in return for a lifetime subscription.

screenshot-2022-03-31-at-14-30-11.png

zScaler

According to the cybersecurity researchers, BlackGuard can steal information, including saved browser credentials and history, email client data, FTP accounts, autofill content, conversations in messenger software, cryptocurrency credentials, and other account information. Messengers targeted include Telegram, Signal, Tox, Element, and Discord.

---

## Security

---



## **Cyber security 101: Protect your privacy from hackers, spies, and the government**

---

Simple steps can make the difference between losing your online accounts or maintaining what is now a precious commodity: Your privacy.

### Read now

When it comes to cryptocurrency theft, the malware will target files such as wallet.dat that may contain wallet addresses and private keys. BlackGuard may also go after Chrome and Edge cryptocurrency wallet browser extensions.

Written in .NET, the infostealer is still in active development but is already equipped with a crypto-based packer, base64 decoding, obfuscation, and antidebugging capabilities to make reverse-engineering more difficult.

Once it lands on a vulnerable machine, the malware will also check the operating system's processes and will try to stop any activities related to antivirus software or sandboxing.

The infostealer is also selective when it comes to its targets. For example, the malware will exit if the OS appears to be located in a CIS country, such as Russia, Belarus, or Azerbaijan.

If an exit isn't necessary, the infostealer then grabs all of the information it can, packages it up into a .zip archive, and sends it to a command-and-control (C2) server through a POST request.

"While applications of BlackGuard are not as broad as other stealers, BlackGuard is a growing threat as it continues to be improved and is developing a strong reputation in the underground community," the researchers say.

Infostealers can be used on their own or packaged up with other forms of malware, such as Trojans or ransomware variants.

In other malware news, researchers from Aqua Security have recently uncovered a new strain of ransomware designed to target Jupyter Notebook environments.

### **Previous and related coverage**

---

**Have a tip?** Get in touch securely via WhatsApp | Signal at +447713 025 499, or over at Keybase: charlie0

---