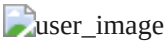
BlackGuard Stealer Targets the Gaming Community

By Shmuel Gihon

Published: 2022-06-19 · Archived: 2026-04-05 18:48:43 UTC

- Table of contents

The author



Shmuel Gihon

Research Team Leader at Cyberint

Related Articles

Executive Summary

BlackGuard is a fairly new info stealer from the end of January 2022 with a business model of Malware-as-a-Service (MaaS). The malware is sold in underground forums and a dedicated Telegram channel of the operators' named `blackteam007`.

The malware will look to obtain the assets info stealers often look for such as machine's information, cookies, and browsing sessions, Various email and VPN clients' credentials along with instant messaging applications' credentials such as Telegram and Discord. Furthermore, the stealer supports the functionality to obtain browser-based cryptocurrency wallets such as Metamask.

The Cyberint Research Team recently discovered campaigns abusing gaming forums and Discord channels to distribute BlackGuard, along with a new data exfiltration technique using Telegram.

Purchasing BlackGuard

As mentioned, BlackGuard's team advertises their product in underground forums and Telegram channel (Figures 1,2).

Figure 1: BlackGuard's Telegram channel ad


BlackGuard's advertisement on underground forum
Figure 2: BlackGuard's advertisement on underground forum

The purchasing is done via the Telegram channel created by the group. The price varies between 200 and 700USD depending on the subscription period, paid with cryptocurrency of course.

BlackGuard's developers were advertising the malware since January 2021 on underground forums for a very short period of time, although for unknown reason they went silent only to come back on last January.

Delivery

BlackGuard Team does not provide any delivery methods when purchasing the stealer. Therefore, the threat actor that is looking to purchase the stealer will need to apply its own delivery method.

It is very common within this type of threat to use malspam campaigns containing malicious documents that will download or load the BlackGuard stealer sample.

In this report, we have encountered a social engineering technique when a threat actor published a patch for the popular game CountnerStrike, presumably on gaming community forums or Discord channels.

The initial phase begins with a victim being lured to download and run the "patch".

Technical Analysis

Initial Infection

As the victim downloads and executes the malicious patch, the executable creates a new directory in the `%APPDATA%` directory named `"NTDYxmw5zzLIBxcMt"`, a hard-coded name.

Once the directory is created, the loader will create two new executables (Figure 3) within this directory:

- `AnimeSoftware.exe` – a somewhat legitimate file that is the real patch for the CounterStrike game.
- `Natasha.exe` – The BlackGuard sample.


The malicious patch creating the AnimeSoftware.exe and Natasha.exe files
Figure 3: The malicious patch creating the AnimeSoftware.exe and Natasha.exe files

Once both files are created, the loader executes both files (Figure 4). The first one, `AnimeSoftware.exe's` purpose is to make the process look "as intended" while the second, `Natasha.exe`, initiates the information-stealing phase.


The malicious patch executes both loaded files
Figure 4: The malicious patch executes both loaded files

Post Infection

BlackGuard is focusing on valuable information such as cryptocurrency wallets, and browsers information including cookies, sessions, and history. It supports browsers such as Chrome, Edge, Firefox, Opera, Brave and more.

Furthermore, the notorious stealer looks for credentials in applications such as Telegram, Discord, FileZilla, Email and VPN clients. Among the VPN clients, it seems that BlackGuard targets ProtonVPN, OpenVPN and NordVPN.

Working Directory

BlackGuard's working directory is also located within the %APPDATA% directory as it creates and names it with a combination of random 14 characters, the victim's machine name, and the username of the machine (Figure 5).

The information is zipped into a .rar file that will be sent later to the C2.


BlackGuard's working directory
Figure 5: BlackGuard's working directory

Calling Home

Like other malware that looks to use an anonymous and evasive C2 infrastructure, BlackGuard turned to Telegram as the ultimate solution.

Recent campaigns suggest that the info stealer has evolved in the past months and now exports the stolen data to a Telegram channel, presumably given by the operators of the MaaS.

BlackGuard uses the Telegram's API service to create simple calls for the C2 channel as it sends metadata first using the `sendDocument` functionality (Figure 6), followed by a compressed file containing the relevant data.


BlackGuard's HTTP request contains metadata to the C2 Telegram channel
Figure 6: BlackGuard's HTTP request contains metadata to the C2 Telegram channel

IOC

SHA256

Malicious CounterStrike Patch:

- b16bb8ce89c42e0f48deb5ba2a8b5c7495c8702c7c2c5c0af7d38739f6281ebb

BlackGuard Samples:

- a0cc5f36b04eae3db5582ec2563ed77e83783765addd3460313377c6fcd1b96d
- 5293c26f29b4af6bc2f3f74ae1ed93537e6c311a695cc0a6920a635c57383617
- 352c936eaf45ffd2f99ba2a9e726eaa39af29d4c37a6ad5106849f07aa35896c

---