

Fake Valorant cheats on YouTube infect you with RedLine stealer

bleepingcomputer.com/news/security/fake-valorant-cheats-on-youtube-infect-you-with-redline-stealer/

Bill Toulas

By

[Bill Toulas](#)

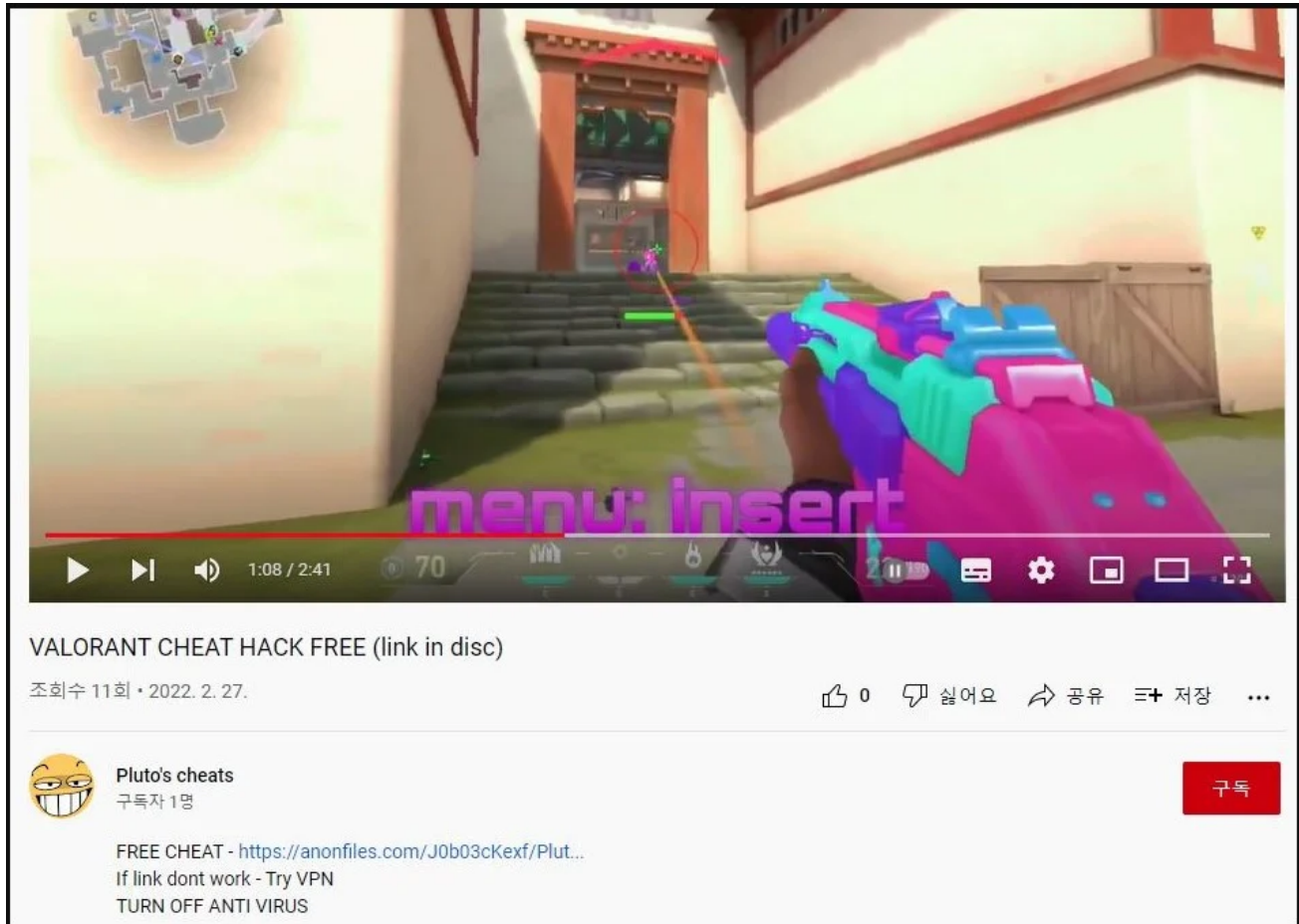
- March 13, 2022
- 10:06 AM
- 0



Korean security analysts have spotted a malware distribution campaign that uses Valorant cheat lures on YouTube to trick players into downloading RedLine, a powerful information stealer.

This type of abuse is quite common, as the threat actors find it easy to bypass YouTube's new content submission reviews or create new accounts when reported and blocked.

The campaign spotted by ASEC targets the gaming community of Valorant, a free first-person shooter for Windows, offering a link to download an auto-aiming bot on the video description.



The image shows a YouTube video player. The video content is a first-person view from the game Valorant, showing a player holding a colorful weapon (a 'Sledgehammer') in a hallway. A purple enemy character is visible in the distance. A large, semi-transparent watermark 'menu: insert' is overlaid on the video. Below the video player, the video title is 'VALORANT CHEAT HACK FREE (link in disc)'. The channel name is 'Pluto's cheats' with a profile picture of a yellow smiley face. The video description includes a link to 'anonfiles.com', instructions to 'Try VPN' if the link doesn't work, and a warning to 'TURN OFF ANTI VIRUS'. The video has 11 views and was uploaded on February 27, 2022.

Video promoting fake auto-aiming bot (ASEC)

These cheats are allegedly add-ons installed in the game to help the players aim at enemies with speed and precision, winning headshots without demonstrating any skill.

Auto-aiming bots are highly sought-after for popular multiplayer games like Valorant because they allow effortless ranking progression.

Dropping Redline

Users who attempt to download the file in the video's description will be taken to an anonfiles page from where they'll get a RAR archive that contains an executable named "Cheat installer.exe".

This file is, in reality, a copy of RedLine stealer, one of the most widely deployed password-stealing malware infections that snatch the following data from infected systems:

- **Basic information:** Computer name, user name, IP address, Windows version, system information (CPU, GPU, RAM, etc.), and list of processes
- **Web browsers:** Passwords, credit card numbers, AutoFill forms, bookmarks, and cookies, from Chrome, Chrome-based browsers, and Firefox
- **Cryptocurrency wallets:** Armory, AtomicWallet, BitcoinCore, Bytecoin, DashCore, Electrum, Ethereum, LitecoinCore, Monero, Exodus, Zcash, and Jaxx

The videos that promote these tools are often stolen from elsewhere and are re-posted from malicious users on newly created channels to act as lures.

Even if the comments below these videos praise the uploader and claim the tool works as promised, they should not be trusted as these can easily be faked.

Related Articles:

[Fake Binance NFT Mystery Box bots steal victim's crypto wallets](#)

[Eternity malware kit offers stealer, miner, worm, ransomware tools](#)

[German automakers targeted in year-long malware campaign](#)

[RIG Exploit Kit drops RedLine malware via Internet Explorer bug](#)

[New powerful Prynt Stealer malware sells for just \\$100 per month](#)

- [Cheating Tool](#)
- [Info Stealer](#)
- [Information Stealer](#)
- [RedLine](#)
- [Valorant](#)
- [YouTube](#)

[Bill Toulas](#)

Bill Toulas is a technology writer and infosec news reporter with over a decade of experience working on various online publications. An open source advocate and Linux enthusiast, is currently finding pleasure in following hacks, malware campaigns, and data breach incidents, as well as by exploring the intricate ways through which tech is swiftly transforming our lives.

- [Previous Article](#)
- [Next Article](#)

[Post a Comment](#) [Community Rules](#)

You need to login in order to post a comment

Not a member yet? [Register Now](#)

You may also like:
