Fake Valorant cheats on YouTube infect you with RedLine stealer

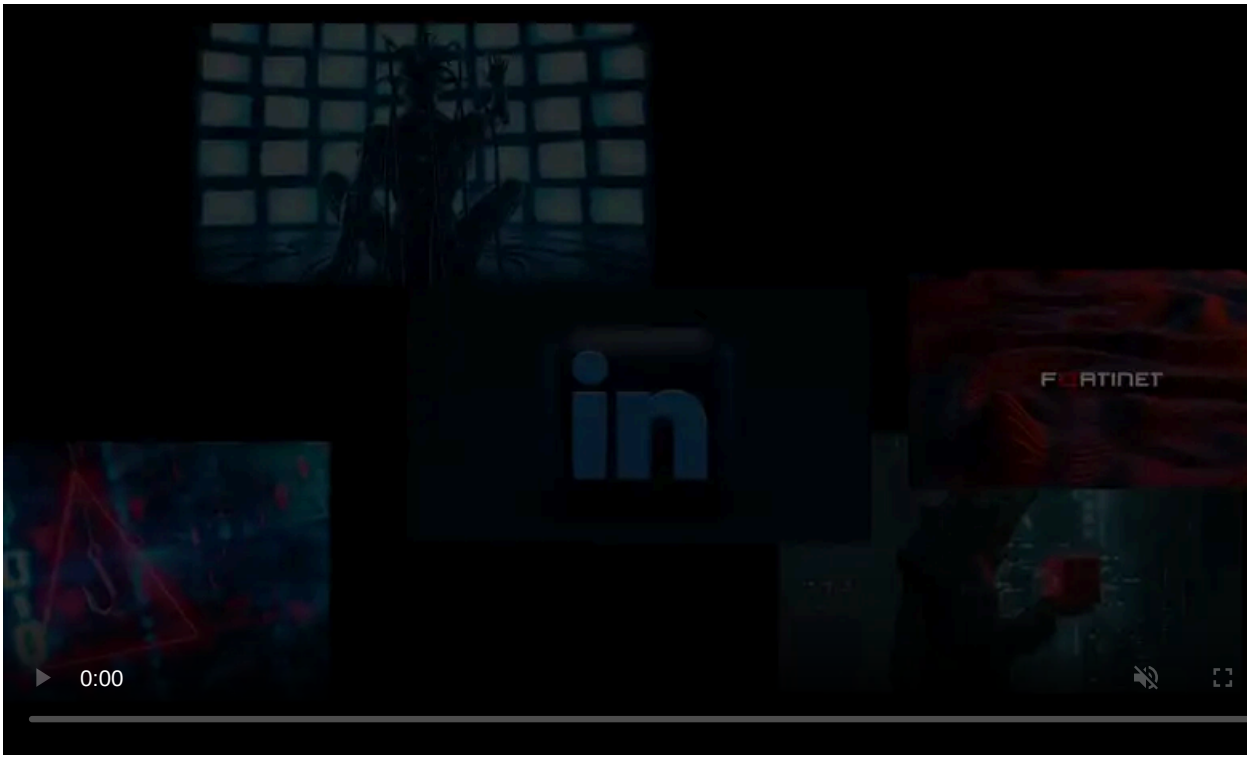
By Bill Toulas

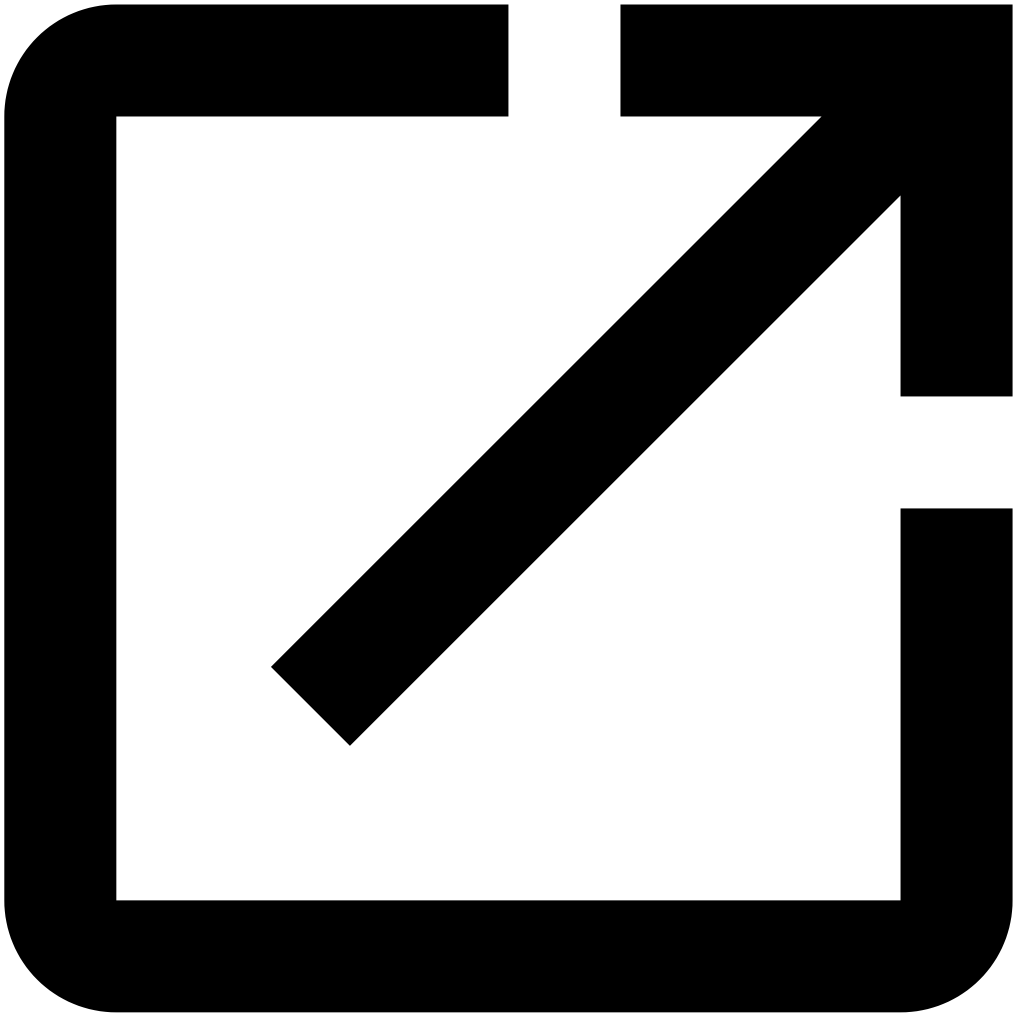
Published: 2022-03-13 · Archived: 2026-04-05 19:24:52 UTC

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.


0:00



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.

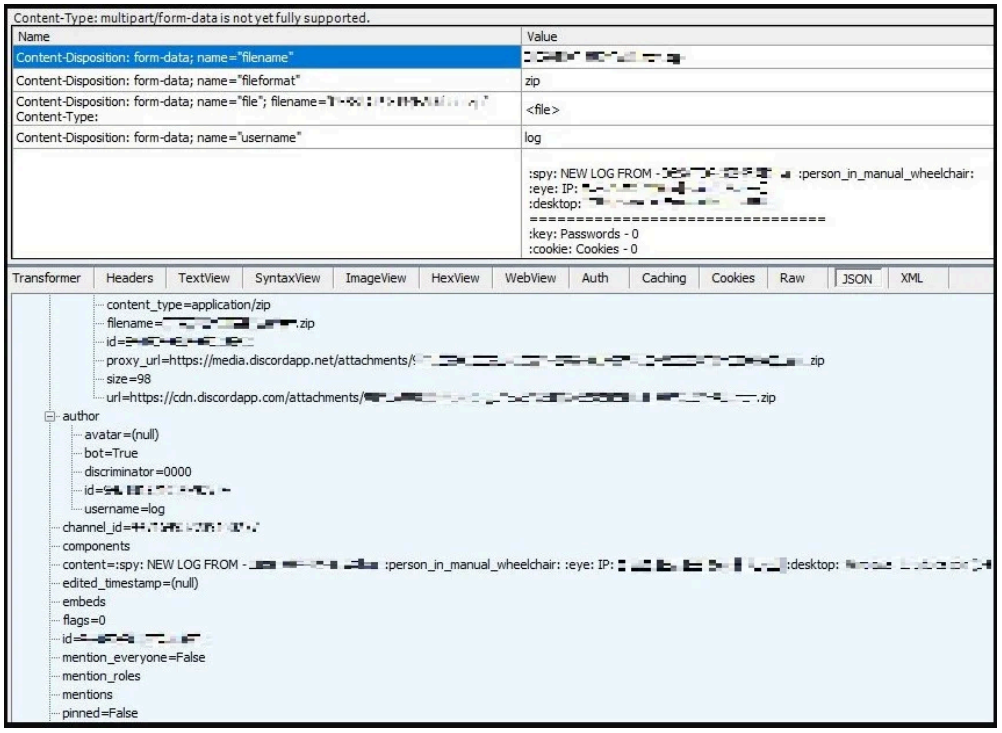
Dropping Redline

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
- **VPN clients:** ProtonVPN, OpenVPN, and NordVPN
- **Others:** FileZilla (host address, port number, user name, and passwords), Minecraft (account credentials, level, ranking), Steam (client session), Discord (token information)

After collecting this information, RedLine neatly packs it in a ZIP archive named "().zip" and exfiltrates the files via a WebHook API POST request to a Discord server.



Exfiltrating stolen information via Discord WebHook *(ASEC)*

Don't trust links in YouTube videos

Apart from the fact that cheating in video games takes the fun out of playing and ruins the game for others, it is always a potentially severe security risk.

None of these cheat tools are authored by trustworthy entities, none are digitally signed (so AV warnings are bound to be ignored), and many are indeed malware.

ASEC's report contains a recent example, but that's just a drop in the sea of malicious download links under YouTube videos that promote free software of various types.

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.
