MOTHERBOARD
TECH BY VICE

Hackers Are Using Anti-Cheat in 'Genshin Impact' to Ransom Victims

The game’s anti-cheat system has well-known vulnerabilities that hackers are now abusing to get access to sensitive parts of victims’ operating systems and deploy ransomware.

By Lorenzo Franceschi-Bicchierai

August 26, 2022, 9:00am

IMAGE: HOYOVERSE

A ransomware gang is allegedly hacking victims by abusing the anti-cheat system of the massively popular free-to-play game Genshin Impact.

The cybersecurity firm Trend Micro published a report on Wednesday with details about the attack, highlighting how anti-cheat systems, which are installed by default as part of many online games, can be abused to hack players. The unnamed hackers are taking advantage of the fact that *Genshin Impact’s* anti-cheat system has known vulnerabilities, that it’s signed by a legitimate company—meaning Windows will run it—and because it has high privileges, meaning it has access to sensitive parts of the operating system.

“I’ve been expecting to see ransomware abuse an anti-cheat driver for a while. We’ve seen cheats abuse anti-cheat drivers for years,” an employee of a games company, who asked to remain anonymous because they weren't allowed to speak to the press, told Motherboard. “It was just a matter of time before a ransomware group noticed and started co-opting exploits that are openly shared.”

The hackers’ goal is to “mass-deploying ransomware,” according to Trend Micro. *Genshin Impact* was released in 2020 by Chinese developer HoYoverse (miHoYo in China) and has millions of players, who log into its game world via mobile devices, consoles, or on PC.

From Trend Micro’s report, it’s unclear how the hackers gain the initial foothold into a targeted computer. But once they are in, the hackers are exploiting *Genshin Impact*’s anti-cheat system to get access to the computer’s kernel, a core part of the operating system that controls and has access to most of the computer's functions. At that point the hackers have the ability to turn off antivirus and install ransomware on the victims’ computers.

In other words, they are abusing the anti-cheat system as a way to get access to more sensitive parts of the operating system and avoid getting caught by an antivirus before deploying the ransomware.

Trend Micro researchers note that the game “does not need to be installed on a victim’s device for this to work,” meaning hackers can just install the anti-cheat system as a preliminary step to then deploy the ransomware.

> ***Do you have information about these attacks? Or other ransomware incidents? We'd love to hear from you. Using a non-work phone or computer, you can contact Lorenzo Franceschi-Bicchierai securely on Signal at +1 917 257 1382, Wickr/Telegram/Wire @lorenzofb, or email lorenzofb@vice.com***

Genshin Impact’s anti-cheat system is called mhyprot2. For years, security researchers have warned about the anti-cheat’s flaws. In 2020, a researcher showed that the system could be abused to read the computer’s memory and processes. Then in July of last year, a researcher who goes by Kento Oki published a proof-of-concept that turned the anti-cheat system into malicious software that could access the kernel.

These concerns have been publicly discussed outside security circles as well. The website Pro Game Guides reported after the game’s launch that users were concerned about the anti-cheat system because it had kernel-level privileges and was running in the background even when the game was closed, going as far as wondering if it was spyware. The company responded to these concerns by updating the anti-cheat system so that it would turn off when users were not playing the game.

In other words, HoYoverse, the company that develops Genshin Impact, has known that this version of the game’s anti-cheat system is vulnerable and can be exploited for a couple of years.

“We're currently working on this case, and will find a solution as soon as possible to safeguard players' safety and stop potential abuse of the anti-cheat function,” a HoYoverse spokesperson told Motherboard in an email.

Despite the long-running concerns, the vulnerable anti-cheat system is still getting installed on players’ computers, and has not been patched. And, according to Trend Micro researchers, “there are no solutions at this time” because the anti-cheat system is a legitimate program signed by a real company, and thus it’s not flagged by antivirus or Windows.

There are other anti-cheat systems that run in the kernel, giving them access and visibility into what’s running on the operating system with the goal of spotting cheat programs. The first one that gathered attention and led some to ask whether it was going too far was Vanguard, the anti-cheat system for Riot Games’ online first person shooter *Valorant*. Activision followed suit with RICOCHET, a kernel-level anti-cheat system for its uber popular *Call of Duty* games.

When making anti-cheat systems like these, developers have to be aware that the system could be turned against users if there are vulnerabilities, according to Paul Chamberlain, who was Riot's anti-cheat lead when the company developed Vanguard.

"It was one of the primary worries we had when making Vanguard at Riot, we put a lot of resources into security audits to try and ensure something like this couldn't happen," Chamberlain told Motherboard.

Abusing drivers and other programs to push ransomware is a tried and true tactic for cybercriminals, according to Allan Liska, a researcher at cybersecurity firm RecordedFuture who focuses on ransomware.

"Signed drivers are usually going to slip pass endpoint detection systems [such as antivirus] unnoticed," he said.

UPDATE, *Friday Aug. 26, 10:31 a.m.* ET: *This story was updated to include the comment from a HoYoverse spokesperson.*

Subscribe to our podcast, CYBER. Subscribe to our new Twitch channel.

TAGGED: VIDEO GAMES,CYBER,GENSHIN IMPACT,RANSOMWARE,ANTI-CHEAT,CHEATING,GAME HACKING,CYBERSECURITY,CYBERCRIME,WORLDNEWS

MORE FROM VICE

Tech

Cybercriminals Leak LA School Data After It Refuses to Ransom

LORENZO FRANCESCHI-BICCHIERAI

10.03.22

Tech

Inside Ukraine's Decentralized Cyber Army

LORENZO FRANCESCHI-BICCHIERAI

07.19.22

Tech

Head of Ukraine's Cybersecurity Says Russia Has Committed 'Cyber War Crimes'

LORENZO FRANCESCHI-BICCHIERAI

08.15.22

Tech

The Uber Hack Shows Push Notification 2FA Has a Downside: It's Too Annoying

LORENZO FRANCESCHI-BICCHIERAI

09.16.22

Tech

Hackers Say They Can Unlock and Start Honda Cars Remotely

LORENZO FRANCESCHI-BICCHIERAI

LORENZO FRANCESCHI-BICCHIERAI

07.12.22