

How is Riot fighting flooding of Valorant gamers?

Riot is trying to regain the trust of gamers after the Vanguard anti-fraud software they used for Valorant was suspected of being malicious.

Riot is trying to regain the trust of gamers after the Vanguard anti-fraud software they used for Valorant was suspected of being malicious.

As you know, the Vanguard anti-fraud software that Riot created for Valorant, the shooter currently being tested, is the focus of gamers' attention. Besides features such as a 128-tick server, low ping thanks to the Riot Direct network, Vanguard is one of the 'trump cards' that Riot uses to promote Valorant. Therefore, the software encountering the opposition of gamers is a problem that they did not expect, and certainly is a significant obstacle on the way to expand Valorant to gamers in the world. So, what does Riot say and do to reassure his players?

Event

First, let Beetle remind you of the problem that makes gamers feel conflicted with Vanguard. Normally when a multiplayer game is launched, certain anti-cheat software will be activated - Apex Legends has Easy Anti Cheat, PUBG has Battleye, Raid has Xigncode3, . and Valorant is no exception when it has Vanguard. All of these anti-cheat software runs at the kernel driver level - the platform level in the computer and so there is a risk of being used by crooks, but Vanguard attracts attention in that it launches as soon as you turn on the computer. , rather than waiting for you to open Valorant.

Process Name	PID	Status	Session	Private Bytes
unsecapp.exe	5780	Running	SYSTEM	1,440 t
VALORANT-Win64-Shipping.exe	4296	Running	pn	11,88,768 t
VALORANT.exe	15692	Running	pn	972 t
vgc.exe	12728	Running	SYSTEM	12,296 t
Video.UI.exe	13068	Suspended	pn	0 t
wallpaperservice32_c.exe	4160	Running	SYSTEM	692 t
WDDriveService.exe	4552	Running	SYSTEM	5,916 t
WindowsInternal.ComposableShell...	2348	Suspended	pn	0 t
wininit.exe	856	Running	SYSTEM	1,080 t
winloaon.exe	1152	Running	SYSTEM	1,552 t

Vanguard runs whether you open Valorant or not.

Besides, some gamers also find that other games are also affected by Vanguard. The most noticeable phenomenon is that the game lags, or worse, some games do not work when there is Vanguard in the machine

and are only overcome when removing Valorant and Vanguard. Many gamers also expressed concern because Riot is owned by Tencent and said that if Valve asked permission to install the same software, they would click the OK button, but with Riot, the answer would be the Cancel button. Epic Launcher had the same problem at launch just because it belonged to Tencent and was supposed to collect data from users' machines.

What does Riot say?

Before the opposition of the gaming community, Riot had to stand out to explain the reasons why they decided to choose a rudimentary anti-cheat solution, deeply interfering with players' machines like Vanguard. According to Riot, Vanguard consists of three components: the client, the driver (which is the component that gamers are worried about) and the platform, in which the client is responsible for communicating with the driver to allow gamers to run Valorant and detect spaces. cheating while the game is running. If the client does not recognize the driver, it will not trust your PC and will not allow Valorant to be turned on.



If the client does not trust the PC, the player will not be able to see the characters.

Drivers are used to confirm the status of the RAM and system and ensure that the client is not compromised. Riot wants the driver to run from the beginning to prevent fraudsters turning on cheating software before turning on the client. Gamers can remove drivers from their devices at any time, but without them, gamers won't be able to open Valorant. Apart from these activities, Riot promises the driver not to perform any suspicious operations such as collecting data, sending information to Riot's server or anyone else. They also said that they have hired many cyber security organizations to look at Vanguard's security.

Here, gamers may wonder why Riot said it had asked a number of cybersecurity organizations to look into Vanguard but did not mention the names of any individuals or organizations. According to many gamers working in the field of information security, this is completely normal because for those organizations, their reputation is very important and in contracts often have provisions that prohibit mentioning names. just in case the software has confirmed that 'OK' has been successfully hacked. This is entirely possible because even the best experts can miss attacks or make mistakes during the evaluation process.



How will we play the game in the future?

In this article, I will review some of the gaming technology trends that developers from small to large have been following.

And what does Riot do?

It must be confirmed that gamers' concerns about Vanguard being exploited to exploit information in their machines or for personal gain are completely grounded. Like any other software running at kernel driver level, in theory, crooks can take advantage of it to install malicious software on users' computers. Not to mention that sometimes the anti-fraud software itself contains malicious code, such as fraudsters installing cryptocurrency mining into ESEA in 2013 or Garena + in 2016.

Riot hopes to ease these concerns by offering a generous reward for finding a security bug on Vanguard. *'Along with the new game Valorant, we have launched a new anti-cheat solution that Vanguard uses kernel drivers to combat fraud more effectively. To emphasize the player's safety, we offer special awards of up to \$ 100,000 for high-quality reports that demonstrate Vanguard's kernel driver viable methods.'*

Vanguard Bounties

Category	Subcategory	Maximum Bounty
Network attack with no user interaction	Code execution on the kernel level	\$100,000
	Unauthorized access to sensitive data	\$75,000
Network attack requiring user interaction (1 click)	Code execution on the kernel level	\$75,000
	Unauthorized access to sensitive data	\$50,000
Local attack for privilege escalation	Code execution on the kernel level	\$35,000
	Unauthorized access to sensitive data	\$25,000

The awards that Riot hangs for finding Vanguard's loophole.

Specifically, they have hung many awards on the HackerOne website, a place often visited by large companies to hang awards that invite hackers to attack their software. This time, the prizes that Riot offers are attractive, from \$ 25,000 for those who can use Vanguard to get sensitive data on the computer to \$ 100,000 for people

who can run command lines at the kernel level. how to attack through the network without any user action.

This is not the first time Riot has hung a HackerOne bug reward, as they have previously spent more than \$ 1 million on similar prizes. However, perhaps to show his trust in Vanguard, the bonuses that Riot offers this time are huge. Other big companies like Rockstar or Nintendo have similar campaigns, but their bonuses are only around \$ 10,000 to \$ 20,000.

Conclusion

Thus, it can be seen that Riot is trying to reassure the gaming community in the world after choosing a strong anti-fraud solution like Vanguard. Perhaps the company has put itself in a situation of 'on the anvil under the hammer' when entering the field of eSports FPS with Valorant. A game of this genre can only live when there is a growing community, and that community cannot exist if hackers are rampant everywhere.



Paul Chamberlain
@arkem

Well it sucks, but today we had to ban our first cheater (and it looks like more bans are on the horizon).

I was hoping for a little more time before this fight kicked off but we're in it now and we're ready.

2:27 AM · Apr 10, 2020 · [Twitter Web App](#)

Riot knows how to "fight" with the cheater, but does not anticipate confronting gamers.

But even with the strong measures that Riot put into Vanguard, crooks still appeared in Valorant by hacking - fighting hacking is an endless race. Unfortunately, even though Riot was anticipating and getting ready for the battle with hacks & cheats, they didn't expect that they still had to fight gamers' suspicions. According to Mo, Riot can not win on this new front and will certainly have to choose concessions, the problem is just how big those concessions are.

You finished reading the article "**How is Riot fighting flooding of Valorant gamers?**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.