



USA 2024

AUGUST 7-8, 2024

BRIEFINGS

# Modern Anti-Abuse Mechanisms in Competitive Video Games

Julien Voisin — [dustri.org](https://dustri.org)

# Agenda

- Cheats & abuses?
- Countermeasures
  - Technical
  - Social
  - Exotic
- Conclusion



0

1:59

2



?

?

?

?

?

MATCH POINT



Player and trap status:

- valk cam [29 m]
- barbwire [24 m]
- kapkan [33 m]
- kapkan [17 m]
- mute jammer [24 M]
- bandit [21 m]
- kapkan [21 m]
- mute jammer [21 m]
- kapkan kapkan
- barbwire
- mute jammer



DROP

2F Library Hallway



100 / 100



Weapon and ammo status:

- 1 1
- G 3
- 6 1
- 1 30 120
- 2 8 70



 **nProtect GameGuard**



**ANTICHEAT**  
**INJECTED**  
E.GAMES . FAIR . PLAY  
Página Oficial | Official WebSite

**easy**<sup>TM</sup>  
ANTI-CHEAT



# Toxicity?

Play Counter Strike or League of Legends for 10 minutes to get vivid examples.

# Cheats, abuses, toxicity, ...

Cheats aren't hunted down because they're morally questionable: they're hunted down because they disturb the way the game is meant to be enjoyed.

Toxic and abusive behaviours lead to the very same effects.

Those aren't purely technical issues: they can't be solved by technical means only.

# Technical countermeasures

Like a EDR, but shadier.

# Integrity-based countermeasures

- Open network connections to know cheat servers, C2-style



# Integrity-based countermeasures

- Open network connections to know cheat servers, C2-style
- Presence of some specific files on the filesystem

# Integrity-based countermeasures

- Open network connections to know cheat servers, C2-style
- Presence of some specific files on the filesystem
- Process names and signatures

# Integrity-based countermeasures

- Open network connections to know cheat servers, C2-style
- Presence of some specific files on the filesystem
- Process names and signatures
- Windows names/titles/icons/...

# Integrity-based countermeasures

- Open network connections to know cheat servers, C2-style
- Presence of some specific files on the filesystem
- Process names and signatures
- Windows names/titles/icons/...
- Loaded modules/dll/...

# Integrity-based countermeasures

- Open network connections to know cheat servers, C2-style
- Presence of some specific files on the filesystem
- Process names and signatures
- Windows names/titles/icons/...
- Loaded modules/dll/...
- Specific hardware

# Integrity-based countermeasures

- Open network connections to know cheat servers, C2-style
- Presence of some specific files on the filesystem
- Process names and signatures
- Windows names/titles/icons/...
- Loaded modules/dll/...
- Specific hardware
- Phone number

# Integrity-based countermeasures

- Open network connections to know cheat servers, C2-style
- Presence of some specific files on the filesystem
- Process names and signatures
- Windows names/titles/icons/...
- Loaded modules/dll/...
- Specific hardware
- Phone number
- TPM

# Integrity-based countermeasures

- Open network connections to know cheat servers, C2-style
- Presence of some specific files on the filesystem
- Process names and signatures
- Windows names/titles/icons/...
- Loaded modules/dll/...
- Specific hardware
- Phone number
- TPM

Inspect **everything**, exfiltrate on suspicion



# Integrity-based countermeasures

- Check return addresses/chain of pointers/memory regions/...

# Integrity-based countermeasures

- Check return addresses/chain of pointers/memory regions/...
- HVCI/VBS/... hypervisors all the way down!

# Integrity-based countermeasures

- Check return addresses/chain of pointers/memory regions/...
- HVCI/VBS/... hypervisors all the way down!
- Kernel-level anti-cheats

# Integrity-based countermeasures

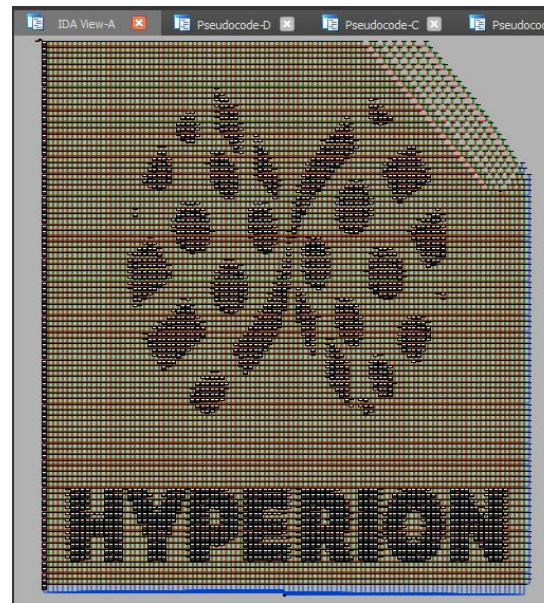
- Check return addresses/chain of pointers/memory regions/...
- HVCI/VBS/... hypervisors all the way down!
- Kernel-level anti-cheats
- TPM and Secure Boot

# Integrity-based countermeasures

- Check return addresses/chain of pointers/memory regions/...
- HVCI/VBS/... hypervisors all the way down!
- Kernel-level anti-cheats
- TPM and Secure Boot
- IOMMU all the things!

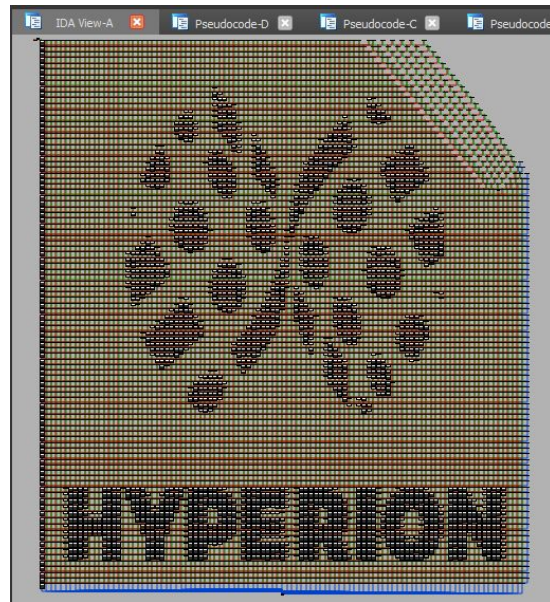
# Obfuscation

- Classic things: junk code, bogus CFG, CFG flattening, inline functions, implicit flows, instructions substitution, mixed boolean arithmetics ...



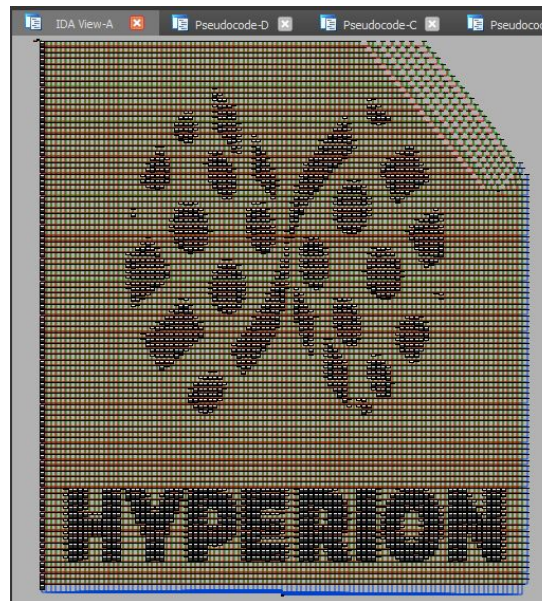
# Obfuscation

- Classic things: junk code, bogus CFG, CFG flattening, inline functions, implicit flows, instructions substitution, mixed boolean arithmetics ...
- Anti debugging/vm/modifications/...



# Obfuscation

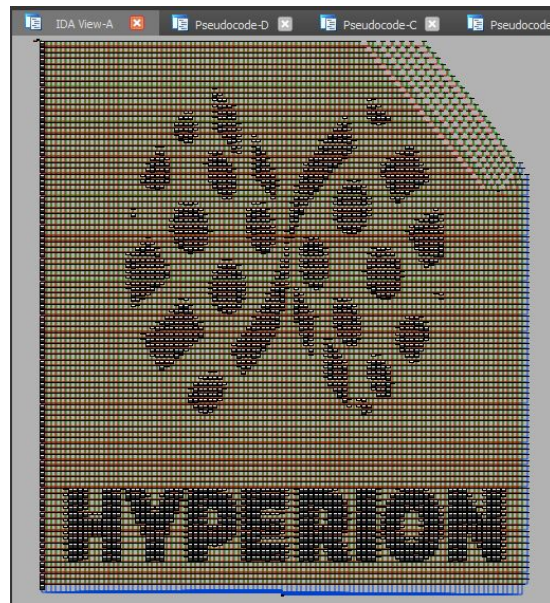
- Classic things: junk code, bogus CFG, CFG flattening, inline functions, implicit flows, instructions substitution, mixed boolean arithmetics ...
- Anti debugging/vm/modifications/...
- Move-value-on-change





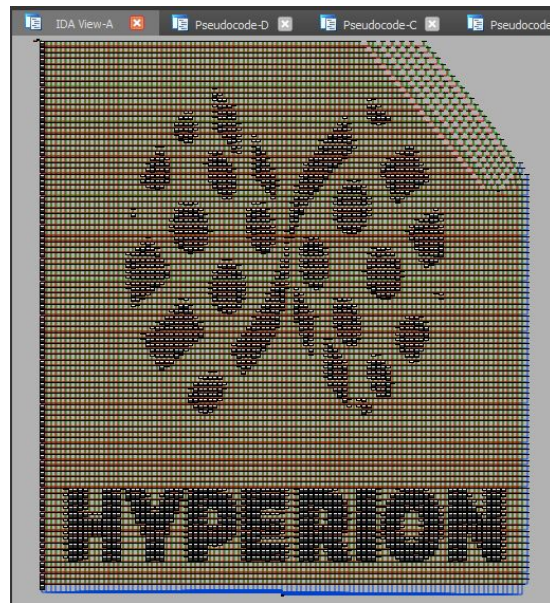
# Obfuscation

- Classic things: junk code, bogus CFG, CFG flattening, inline functions, implicit flows, instructions substitution, mixed boolean arithmetics ...
- Anti debugging/vm/modifications/...
- Move-value-on-change
- Shellcode streaming



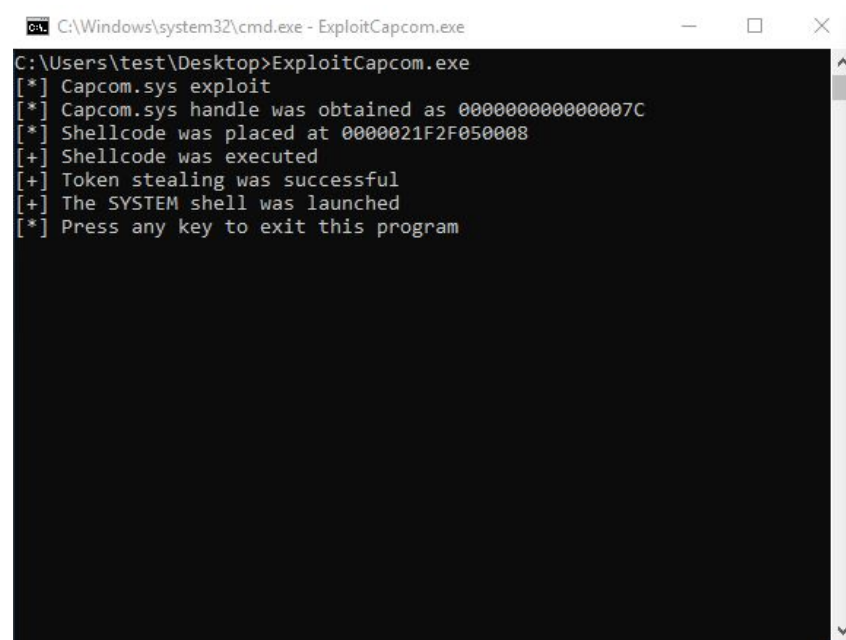
# Obfuscation

- Classic things: junk code, bogus CFG, CFG flattening, inline functions, implicit flows, instructions substitution, mixed boolean arithmetics ...
- Anti debugging/vm/modifications/...
- Move-value-on-change
- Shellcode streaming
- Virtualization



## Side-note: anti-cheats are software too

- Genshin Impact's mhyprot2.sys
- razer-based injection
- capcom.sys
- EACKPF
- ...



```
C:\Windows\system32\cmd.exe - ExploitCapcom.exe
C:\Users\test\Desktop>ExploitCapcom.exe
[*] Capcom.sys exploit
[*] Capcom.sys handle was obtained as 000000000000007C
[*] Shellcode was placed at 0000021F2F050008
[+] Shellcode was executed
[+] Token stealing was successful
[+] The SYSTEM shell was launched
[*] Press any key to exit this program
```

# Social countermeasures

Human powered mitigations!

# Just send the legal department

DMCA, CFAA and even RICO!

- Bossland GmbH vs. Blizzard Entertainment (2017): ~\$8.5M
- EngineOwning UG vs Activision (2024): ~\$14.5M
- Elite Boss Tech vs. Bungie (2022): \$13.5M
- Aimjunkies vs. Bungie (2024): \$63,000
- LeagueSharp vs. Riot: (2017): \$10M
- ...

Cheat manufacturing/distribution is illegal in South Korea and China.

# Make it expensive to cheat: hardware

Buy Call of Duty®: Modern Warfare® III

69,99€

Add to Cart

Buy Call of Duty®: Modern Warfare® III - Vault Edition

99,99€

Add to Cart

Buy Diablo® IV

69,99€

Add to Cart

Buy Diablo® IV - Digital Deluxe Edition

89,99€

Add to Cart

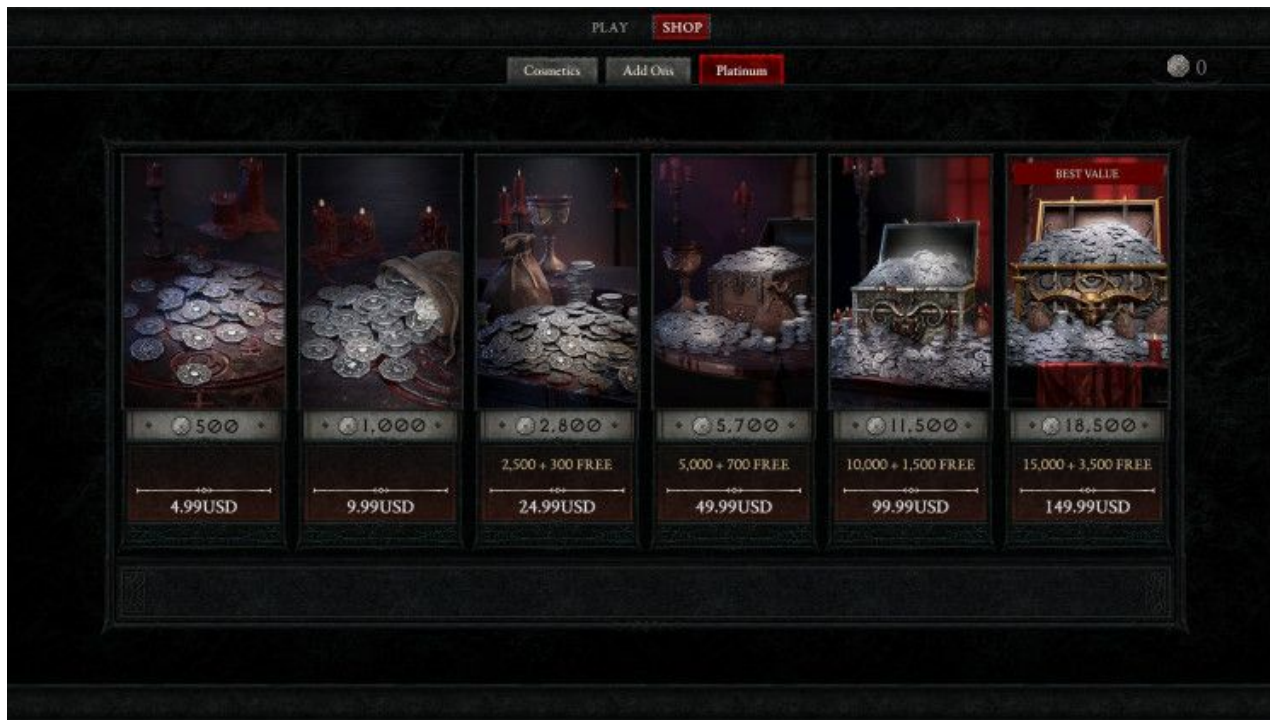
Buy Diablo® IV - Ultimate Edition

99,99€

Add to Cart



# Make it expensive to cheat: DLC



# Make it expensive to cheat: grind

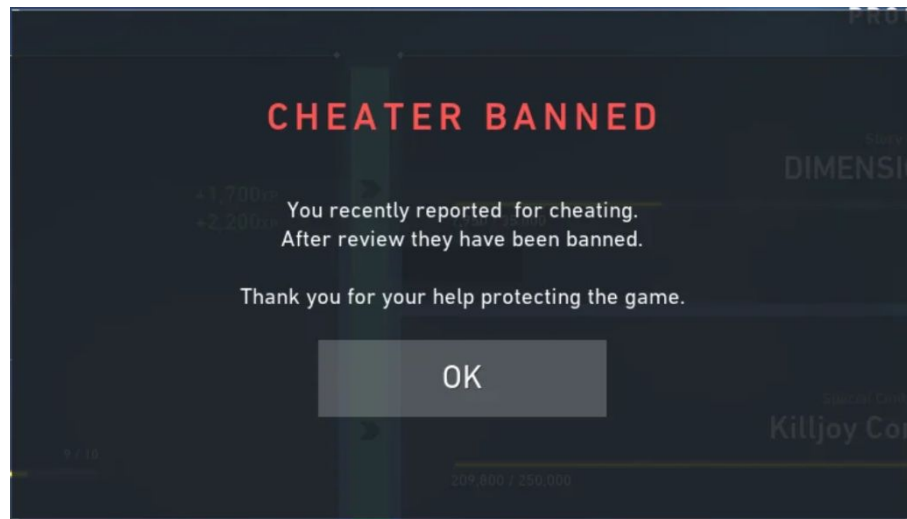
- Lock competitive behind a number of hours played requirement
- Make player grind useful equipment





## Empower players

- Reporting (positive and negative) with penalized slander
- Penalties for those benefiting from cheating
- Provide mute/ignore features
- Provide profanity filters
- Peer-based reputation
- Streamer mode
- Private lobbies
- Blocking



# Machine Learning, AI, blockchain, web3!

- Record matches, use ML to pre-filter, have humans validate
- Huge dataset: deviation is easy to spot
- Issue challenges when in doubt
- Use AI for voice chat “moderation”



# Bug-bounties and FUD

- Increase the number of eyeballs, incentivise reporting
- Interesting pricing dynamics
  
- Blog posts, reports and community managers

## Cheats & Exploits in Our Games

Category	Examples	You can win with 100% certainty
In-game Exploits, cheating	Infinite damage, item duplication, bypassing deck restrictions, aimbot, wallhack	\$2,500 - \$7,000
Cheat Development	Methods to bypass obfuscation, debugging protection, techniques that enable reverse engineering our games	\$250 - \$20,000

# Accounts-level countermeasures

- Add just the right amount of friction: MFA via SMS/tokens, OTP, ...
- Account-level "cheater" mark, like Steam is doing
- Account-level DLC/cosmetics/achievements/...

Deters occasional cheaters

# No more instabans

- Makes it hard to understand how/when a cheat was detected
- Incentivise and reward positive behaviours
- Allows players to correct their conduct

## AFK OFFENSE: PENALTY ADMINISTERED

Your account has been flagged for repeated AFKs and/or Queue Dodges. AFKKing ruins the experience for other players, and as a result, you have received a timer before you can queue again; you will not receive XP for that game, and your restriction from playing ranked has extended to 14 days. If you continue to AFK from your games, you may be banned from playing VALORANT.

This penalty will reduce as you continue to play games without AFKKing.

I Understand

# Exotic measures

And now, their weird stuff.

# Cheating is fun, let's make it tedious!

- Quicksand: random input drops/lag/swap, alter movement speed, ...

# Cheating is fun, let's make it tedious!

- Quicksand: random input drops/lag/swap, alter movement speed, ...
- Handicaps: damage output reduction, lame loot, items drop, ...



# Cheating is fun, let's make it tedious!

- Quicksand: random input drops/lag/swap, alter movement speed, ...
- Handicaps: damage output reduction, lame loot, items drop, ...
- Nonsensical error messages: "Unable to shade polygon normals."

# Cheating is fun, let's make it tedious!

- Quicksand: random input drops/lag/swap, alter movement speed, ...
- Handicaps: damage output reduction, lame loot, items drop, ...
- Nonsensical error messages: "Unable to shade polygon normals."
- Help honest players: cloaking, damages shield, ...

# Cheating is fun, let's make it tedious!

- Quicksand: random input drops/lag/swap, alter movement speed, ...
- Handicaps: damage output reduction, lame loot, items drop, ...
- Nonsensical error messages: "Unable to shade polygon normals."
- Help honest players: cloaking, damages shield, ...
- Group players by reputation

# Cheating is fun, let's make it tedious!

- Quicksand: random input drops/lag/swap, alter movement speed, ...
- Handicaps: damage output reduction, lame loot, items drop, ...
- Nonsensical error messages: "Unable to shade polygon normals."
- Help honest players: cloaking, damages shield, ...
- Group players by reputation
- Crank up gravity x10,000

# Cheating is fun, let's make it tedious!

- Quicksand: random input drops/lag/swap, alter movement speed, ...
- Handicaps: damage output reduction, lame loot, items drop, ...
- Nonsensical error messages: "Unable to shade polygon normals."
- Help honest players: cloaking, damages shield, ...
- Group players by reputation
- Crank up gravity x10,000
- Hallucinations

# Cheating is fun, let's make it tedious!

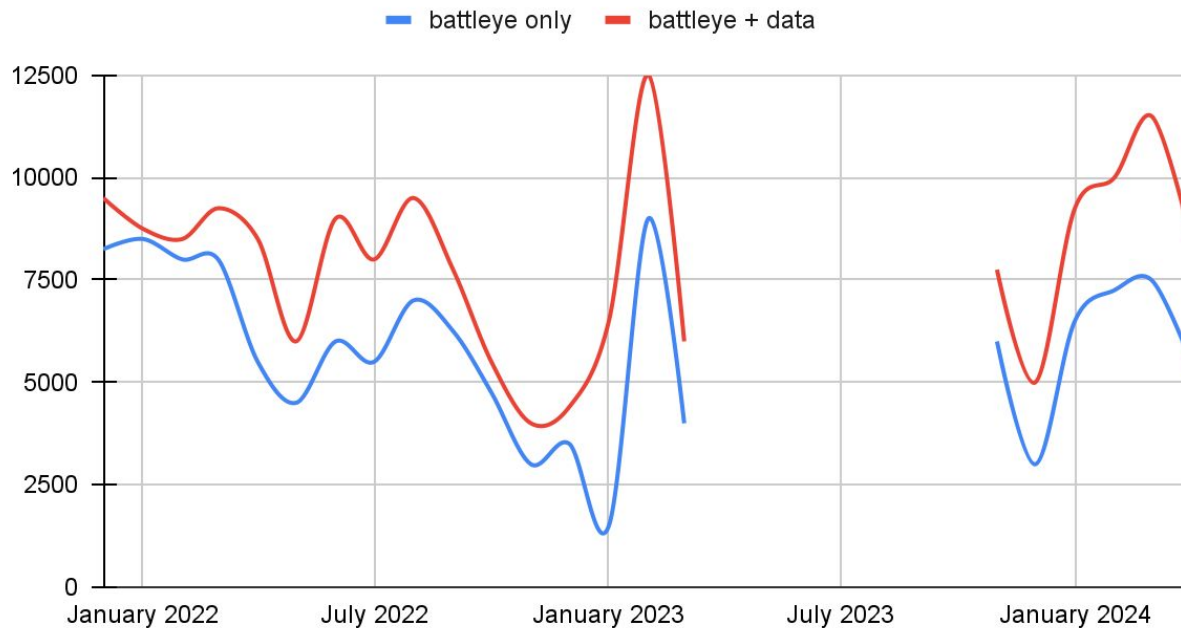
- Quicksand: random input drops/lag/swap, alter movement speed, ...
- Handicaps: damage output reduction, lame loot, items drop, ...
- Nonsensical error messages: "Unable to shade polygon normals."
- Help honest players: cloaking, damages shield, ...
- Group players by reputation
- Crank up gravity x10,000
- Hallucinations
- ...

Complement proper anti-cheat, it doesn't replace it.

Good good.  
But is it working?

It's complicated

## Rainbow Six Siege bans





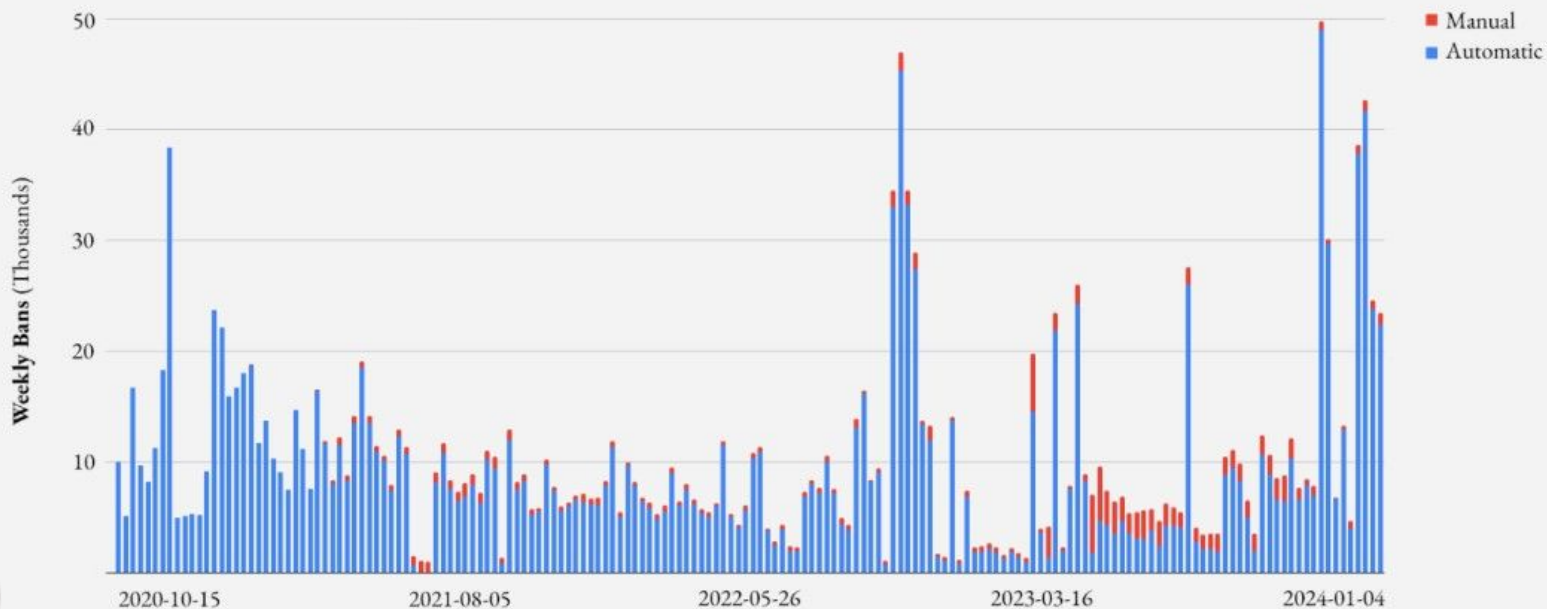
## League: Games with a Cheater Weekly

% of Games Globally Played with a Scripter (or a Bot)



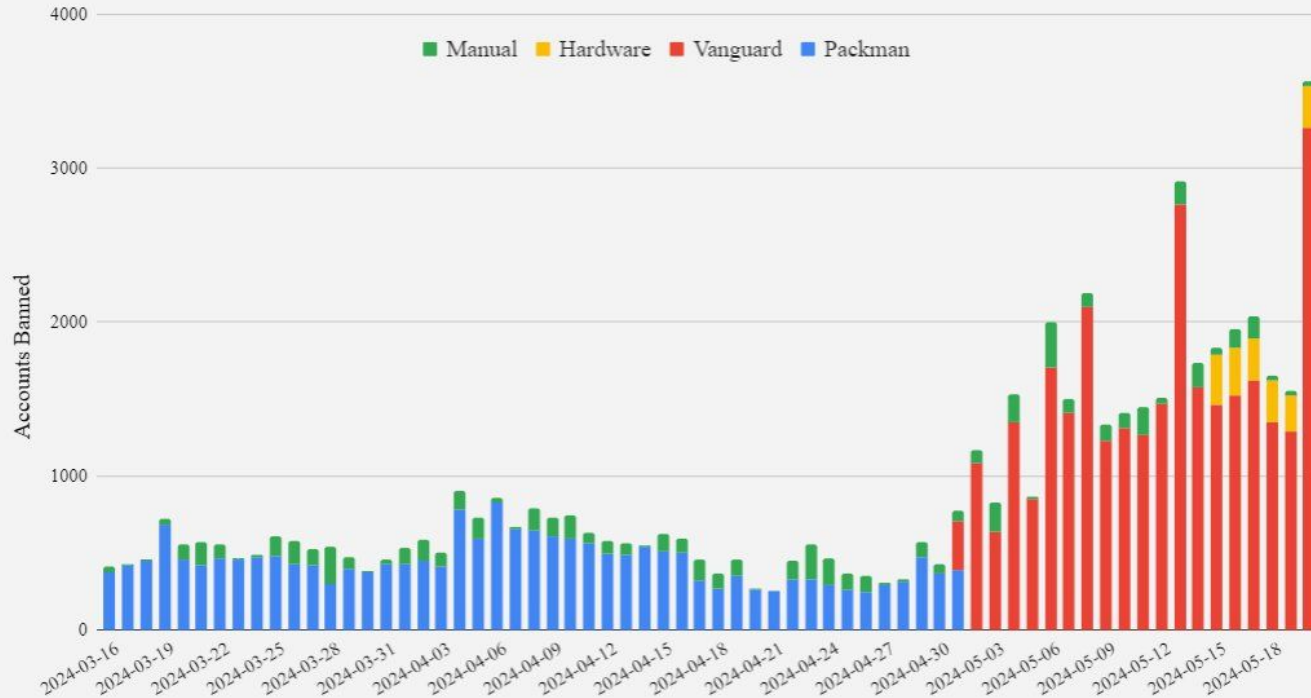
## Packman: Suspensions by Type

LoL Anti-Cheat Scripting Bans, Aggregated Weekly

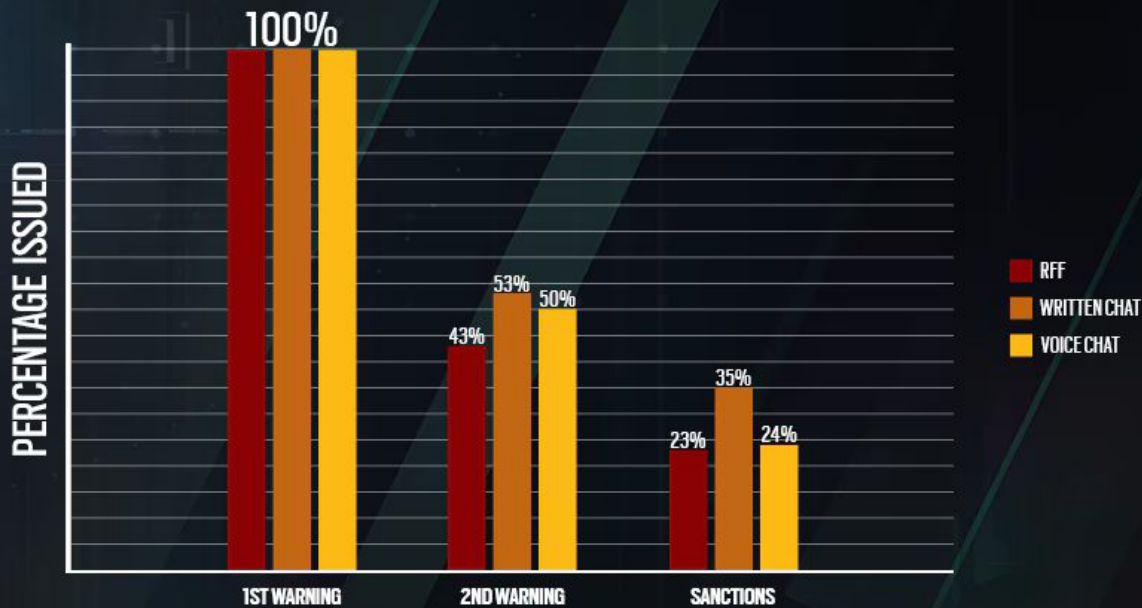


## League of Legends: Bans by System

Suspensions Bucketed by Issuer



## WARNINGS TO PENALTIES



# Conclusion

This is all interesting, but what's your point anyway?

# Reflections on the future

- Feedback and guidance go a long way

# Reflections on the future

- Feedback and guidance go a long way
- Technical means alone aren't the answer

# Reflections on the future

- **Feedback and guidance go a long way**
- Technical means alone aren't the answer
- The cat and mouse game will continue



# Reflections on the future

- **Feedback and guidance go a long way**
- Technical means alone aren't the answer
- The cat and mouse game will continue
- Private cheats will keep working

# Reflections on the future

- **Feedback and guidance go a long way**
- Technical means alone aren't the answer
- The cat and mouse game will continue
- Private cheats will keep working
- Measuring success is hard

# Reflections on the future

- **Feedback and guidance go a long way**
- Technical means alone aren't the answer
- The cat and mouse game will continue
- Private cheats will keep working
- Measuring success is hard
- DMA is the current frontier

# Reflections on the future

- **Feedback and guidance go a long way**
- Technical means alone aren't the answer
- The cat and mouse game will continue
- Private cheats will keep working
- Measuring success is hard
- DMA is the current frontier
- AI will make things worse

# Reflections on the future

- **Feedback and guidance go a long way**
- Technical means alone aren't the answer
- The cat and mouse game will continue
- Private cheats will keep working
- Measuring success is hard
- DMA is the current frontier
- AI will make things worse

Cheating will always be funnier.

# Questions?

# Sources

- [Valorant's blog](#), especially the [Game Health's series](#)
- [League of Legends' blog](#)
- [Rainbow 6: Siege's blog](#)
- [Call of Duty's blog](#)
- [UnKnoWnCheaTs](#)
- [The Secret Club](#)
- [TorrentFreak](#)
- [CheatEngine](#)