



Playing Dirty Without Cheating - Getting Banned for Fun and No Profit

Sam Collins, Marius Muench and Tom Chothia
The University of Birmingham

NEWS

Fortnite fans forced to apologize to the public after getting banned for life

A Fortnite cheater and DDoS exploiter have detailed punishments on social media

BY PATRICI
Jul 14, 2025 a

BUSINESS INSIDER

DOW JONES ▲ +0.2% NASDAQ ▲ +0.33% S&P 500 ▲ +0.14% AAPL ▼ -0.84% NVDA ▲ +3.93% MSFT ▼ -0.15% AMZN ▲

NEWS

A popular 17-year-old 'Fortnite' streamer was banned from the game for life after he was caught cheating

By Kat Tenbarge



Twitch Streamers Who Got Caught Cheating In-Game

BY KEEGAN MCGUIRE AND BRANDON MORGAN
APRIL 16, 2021 5:42 PM EST



ESI ESPORTS INSIDER

HOME NEWS FEATURES

Home > Latest News

Fortnite sues cheater for \$175,000 and issues lifetime ban

WRITTEN BY
Jonno Nicholson

LAST UPDATED ON
June 26, 2025



News Events Spaces Programs

THWatest Deep tech Sustainability Ecosystems Data and security Fintech and ecommerce Future of work Conference media hub

This article was published on November 19, 2020

GAMING

Twitch bans one of its most popular streamers, xQc, for cheating

Who Are We?



Sam

- PhD Student @ UoB,
- Man At The End Attacks & Reverse Engineering
- Game Dev but all my games are impossible to beat without cheating



Marius

- Assistant Prof @ UoB
- Baseband hacking, Reverse Engineering, & Low-Level Security
- Recently hacked the RP2350



Tom

- Professor @ UoB
- Taught game hacking to his students for the last 5 years
- Hacked Apple Pay, Visa, Square, Bank of America, pacemakers, e-passports.

Difficulties in Understanding Game Bans

- **Getting banned**
 - Anti Cheats may actively prevent banworthy behavior
 - Sometimes we are just getting blocked
- **Knowing that we were banned**
 - Some games ban in waves
 - Some games 'shadow ban'
- **Knowing why we are banned**
 - We tried plenty of different things – what triggered a ban?

Road Map

1: Intro and not getting banned

- Game cheats and anti-cheats
- Methods that don't lead to a ban

3: Staying Banned

- Account vs Hardware Bans
- How Hardware Bans work.

2: Getting Banned

- What gets you banned from various big titles
- How to do it with style

4: Getting Others Banned

- Get someone else banned
- Make any Malware Worse!
- Make your friends go and play outside.

Windows

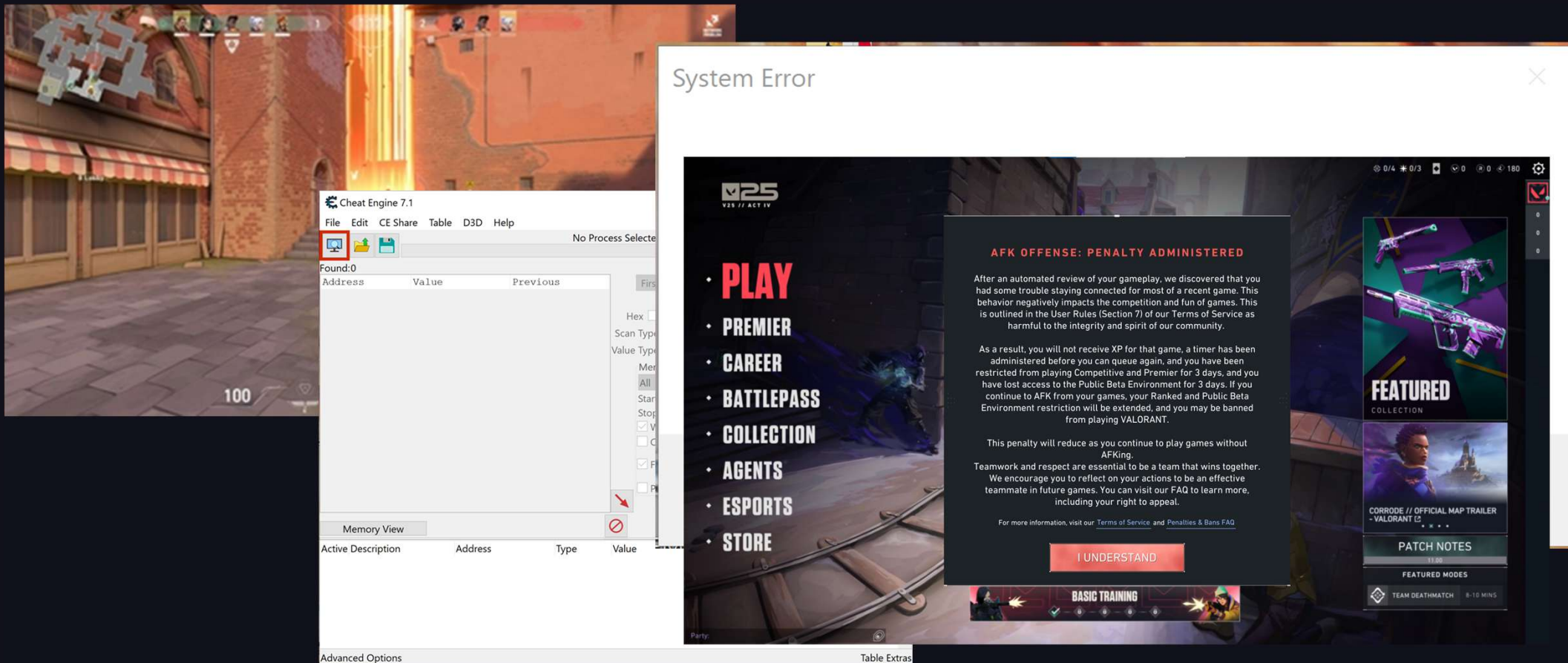
Anti-Cheat

Game

Cheat Process

User level

Let's Try to Get Banned: Cheat Engine.



Let's Try to Get Banned: Cheat Engine.

AFK OFFENSE: PENALTY ADMINISTERED

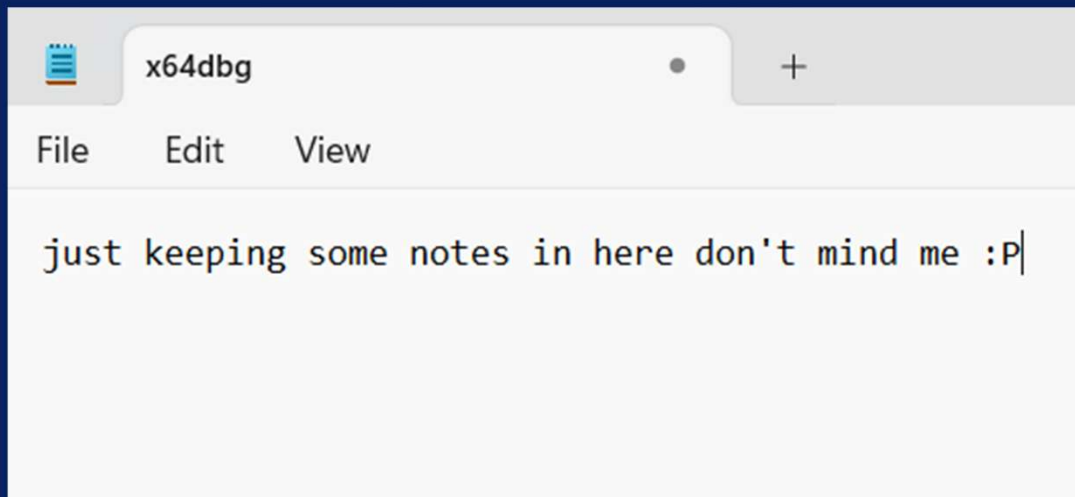
After an automated review of your gameplay, we discovered that you had some trouble staying connected for most of a recent game. This behavior negatively impacts the competition and fun of games. This is outlined in the User Rules (Section 7) of our Terms of Service as harmful to the integrity and spirit of our community.

As a result, you will not receive XP for that game, a timer has been administered before you can queue again, and you have been restricted from playing Competitive and Premier for 3 days, and you have lost access to the Public Beta Environment for 3 days. If you

Is It Just The Process Name?

ERROR

Found active cheat or reverse engineering tool. Please close them before playing Fortnite to avoid account ban.



CONFIRM

Windows

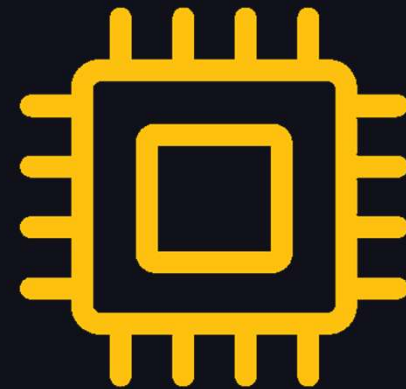
User level

- Runs applications like browsers or games
- Limited access to system resources
- Major fault → program crash

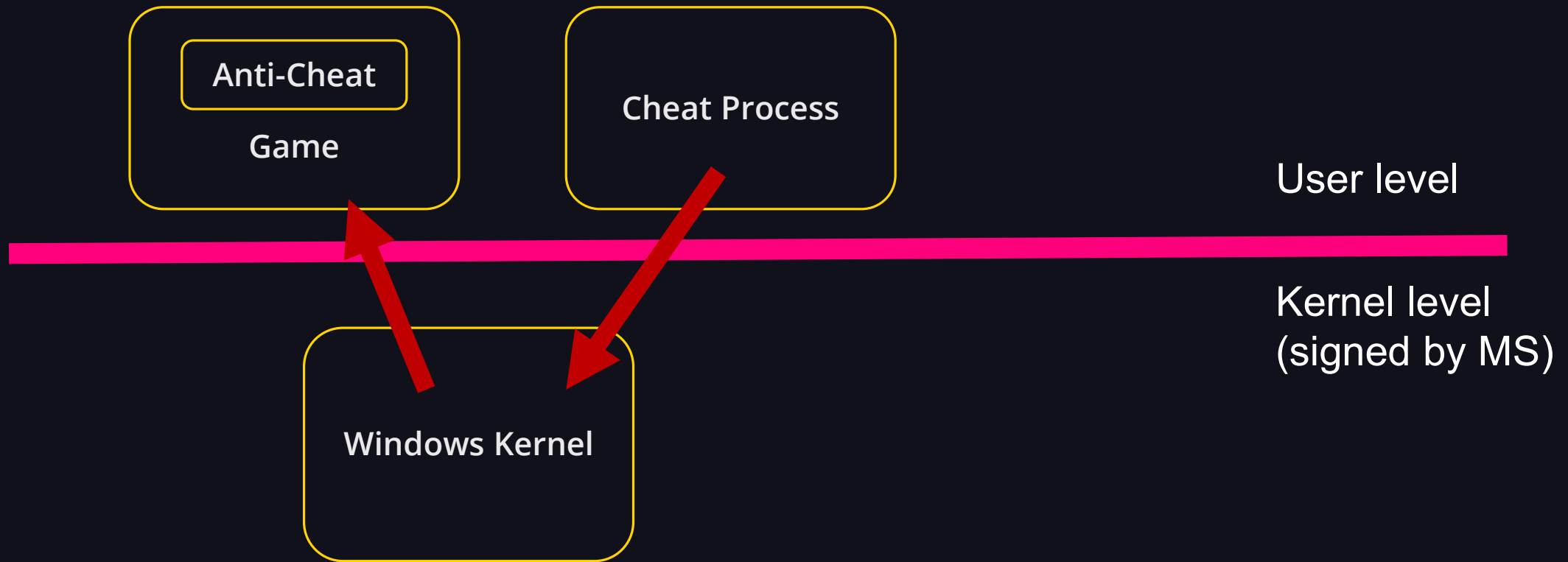


Kernel level

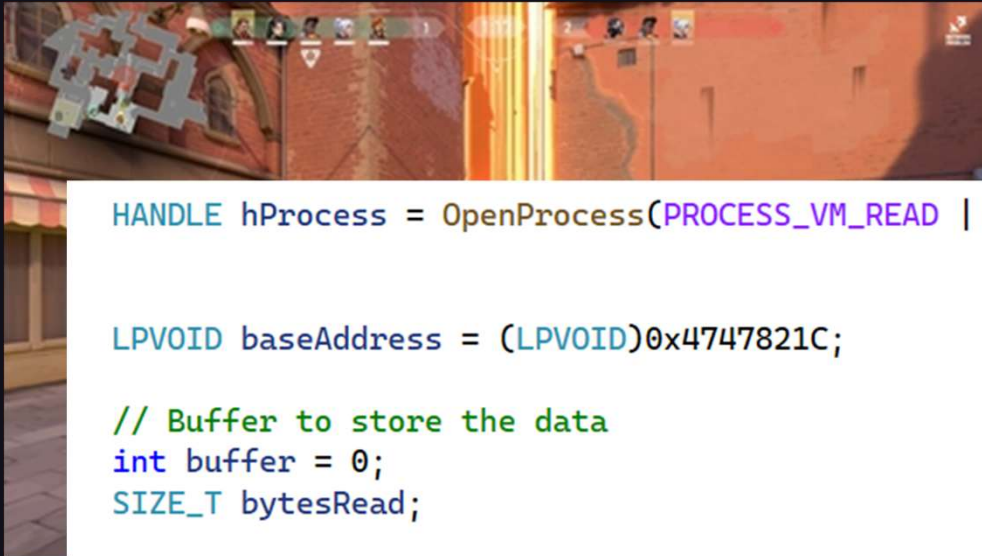
- Runs core system components
- Full access to hardware and memory
- Major fault → machine crash
- ***Code must be signed by Microsoft***



Windows



Let's Try to Get Banned: Read Process Memory



```
HANDLE hProcess = OpenProcess(PROCESS_VM_READ | PROCESS_VM_WRITE | PROCESS_VM_OPERATION
                               | PROCESS_QUERY_INFORMATION, FALSE, pid);

LPVOID baseAddress = (LPVOID)0x4747821C;

// Buffer to store the data
int buffer = 0;
SIZE_T bytesRead;

if (ReadProcessMemory(hProcess, baseAddress, &buffer, sizeof(buffer), &bytesRead)) {
    std::cout << "Value at address " << baseAddress << " is: " << buffer << std::endl;
}
```


Let's Try to Get Banned: Read Process Memory

```
HANDLE hProcess = OpenProcess(PROCESS_VM_R  
  
LPVOID baseAddress = (LPVOID)0x4747821C;  
  
// Buffer to store the data  
int buffer = 0;  
SIZE_T bytesRead;  
  
if (ReadProcessMemory(hProcess, baseAddress  
    std::cout << "Value at address " << ba  
}
```

System Error



A critical error has occurred and the process must be terminated.

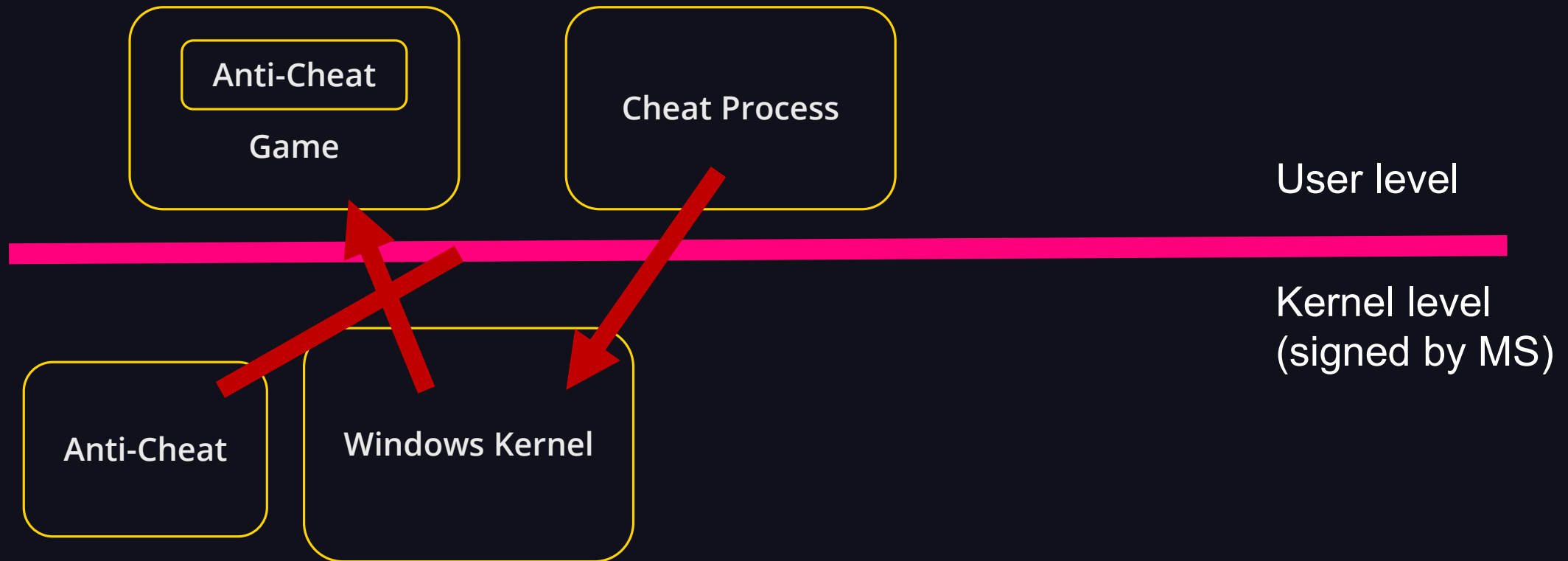
Would you like to create a crash dump to aid the developers in troubleshooting this issue? This may take up to 5 minutes.

NOTE: The process may appear unresponsive during this time.

Yes


No

Windows





Unveiling the underground

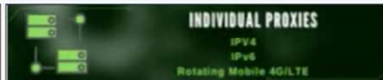



UNKNOWN CHEATS

LEADING THE GAME HACKING SCENE SINCE 2000

[HOME](#) [FORUM](#) [DOWNLOADS](#) [WIKI](#) [DARK MODE](#) [REGISTER](#)


UnKnoWnCheaTs - Multiplayer Game Hacking and Cheats



UnknownCheats is a non-profit website dedicated to game cheats and game hacking, with the goal of maintaining a non-commercial platform for access to information, resources, and a community of gamers and programmers. Additionally, our dedicated volunteer moderators help maintain the site's inclusivity.

[Create a free account](#) to unlock all features and join the #1 game hacking community - Posts: 123456

You are solely responsible for complying with all applicable terms of service and end-user license agreements. Any illegal activity is strictly prohibited. Users who violate these rules will be permanently banned. All content is for personal use only.



GUIDEDHACKING

LEARN GAME HACKING

[Forums](#) [What's new](#) [Downloads](#) [Tutorials](#) [Guides](#) [Anticheat](#) [Info](#) [Log in](#) [Register](#)

Search...

GuidedHacking - Learn Game Hacking

Welcome to GuidedHacking

GH is a website devoted to helping you learn game hacking. We aren't a normal forum, we're a resource. We will soon be re-launched with a new look and more content.

To get an idea of what GuidedHacking is all about, check out our Official GuidedHacking Briefings:

- The Game Hacking Briefing
- Computer Science Briefing



black hat

ASIA 2023

MAY 11-12

BRIEFINGS

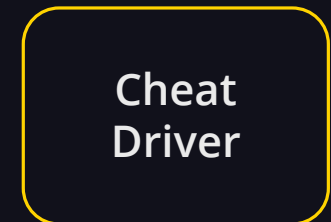
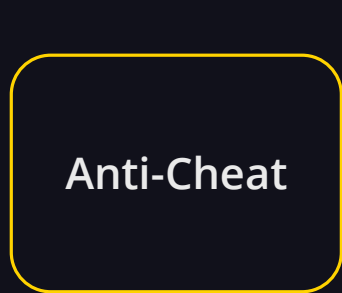


Bypassing Anti-Cheats & Hacking Competitive Games

Windows



User level



Kernel level
~~(signed by MS)~~

Let's Try to Get Banned: BYVOD

BRATISLAVA, PRAGUE — January 11, 2022 — ESET Research has released an in-depth blogpost offering an in-depth look into the abuse of vulnerable kernel drivers. Vulnerabilities in signed drivers are mostly utilized by game cheat developers to circumvent anti-cheat mechanisms, but they have also been observed being used by several APT groups and in commodity malware. The blogpost discusses the types of

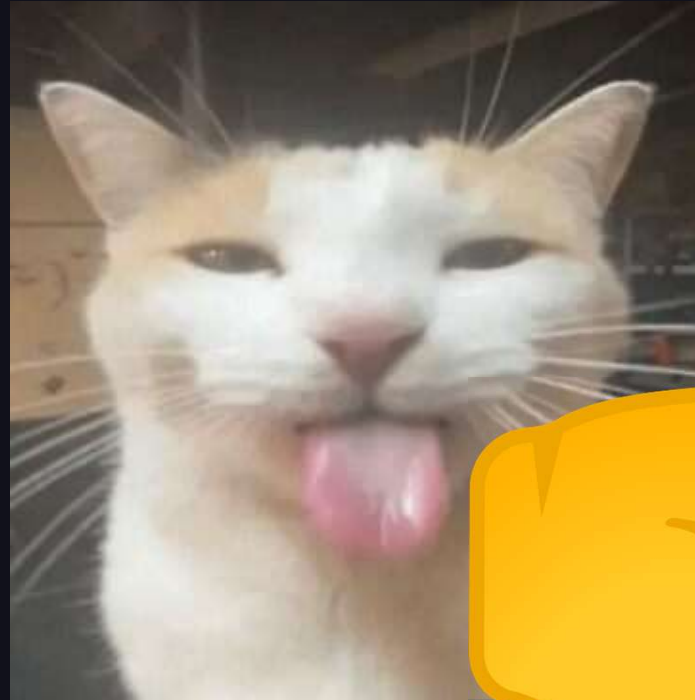


Let's Try to Get Banned: BYVOD

Driver does not load!

Hooked .sys load function.

Drivers unloaded.



Windows



User level



Hypervisor

Domain Expansion – Hypervisor Based Debugging



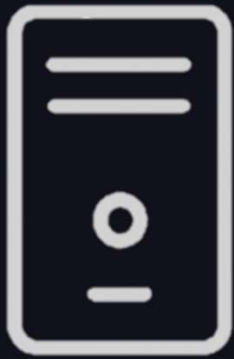
Hardware



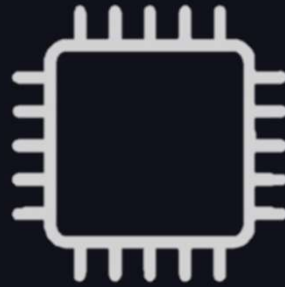
OS

We usually debug here → Kernel
Usermode

Domain Expansion – Hypervisor Based Debugging



Hardware



Hypervisor

↑
We now debug here



Virtual OS

Kernel
Usermode

Domain Expansion – Hypervisor Based Debugging

Let's try a hypervisor-based debugger!

```
C:\Tools\BreakingThings\Release\hyperdbg-cli.exe
HyperDbg Debugger [version: v0.13.2, build: 20250604.1052]
Please visit https://docs.hyperdbg.org for more information...
HyperDbg is released under the GNU Public License v3 (GPLv3).

HyperDbg> .connect local
local debugging (vmi-mode)

HyperDbg> load vmm
loading the vmm driver
err, failed loading driver
it's because either the driver signature enforcement is enabled or HVCI prevents the driver from loading
you should disable the driver signature enforcement by attaching WinDbg or from the boot menu
if the driver signature enforcement is disabled, HVCI might prevent the driver from loading
HyperDbg is not compatible with Virtualization Based Security (VBS)
please follow the instructions from: https://docs.hyperdbg.org/getting-started/build-and-install
unable to install VMM driver
failed to install or load the driver
```

Driver Signature Enforcement stops us loading our hypervisor 😞

Side Quest- Disable DSE

- Windows DSE relies on the function `CiValidateImageHeader` to check signatures
- Using a signed vulnerable driver we can read/write kernel memory
- Let's patch that to always return true instead 😊

```
[+] CI.dll base address: 0xFFFFF80423000000
[+] Found CiValidateImageHeader at 0xfffff80423050280
[+] Found PTE base as 0xffff860000000000
[+] Found CiValidateImageHeader PTE 0xFFFFF867C02118280, value 0x100000004650121
[+] Patched CiValidateImageHeader PTE
[+] Patched CiValidateImageHeader
```

Domain Expansion – Hypervisor Based Debugging

Let's try a hypervisor-based debugger again...

```
HyperDbg> load vmm  
loading the vmm driver  
current processor vendor is : GenuineIntel  
virtualization technology is vt-x  
vmx operation is supported by your processor  
vmm module is running...  
interpreting symbols and creating symbol maps
```

Hypervisor loaded! Let's run a game and do some debugging

Domain Expansion – Hypervisor Based Debugging

Easy Anti Cheat

Battleeye



Your device ran into a problem and needs to restart. We're just collecting some error info, and then we'll restart for you.

0% complete

Vanguard



Your device ran into a problem and needs to restart. We're just collecting some error info, and then we'll restart for you.

0% complete



Your device ran into a problem and needs to restart. We're just collecting some error info, and then we'll restart for you.

Please Ban Us!



Your cheat attempts
are pathetic. You
are not worthy of
our ban.

Road Map

1: Intro and not getting banned

- Game cheats and anti-cheats
- Methods that don't lead to a ban

3: Staying Banned

- Account vs Hardware Bans
- How Hardware Bans work
- How to spoof hardware serials/IDs

2: Getting Banned

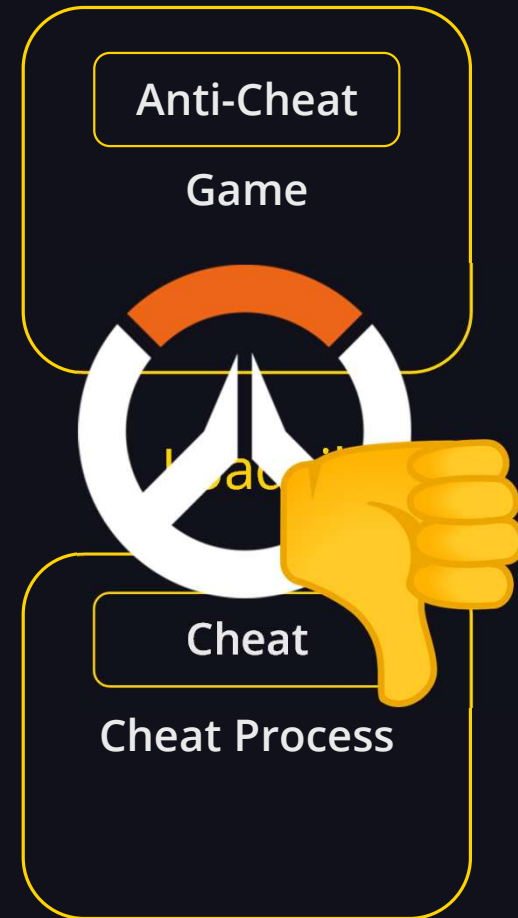
- What gets you banned from various big titles
- How to do it with style

4: Getting Others Banned

- Get someone else banned
- Make any Malware Worse!
- Make your friends go and play outside.

User Mode Injection ft. Overwatch 2

- We want to run some custom code in the target game process
- Usually we'd use something like
`LoadLibrary("1337hax.dll");`
- All anti-cheats will hook/block common API calls like `LoadLibrary(A)` and `CreateRemoteThread`, ruining our day



User Mode Injection ft. Overwatch 2

- To avoid API calls we use a process called **manual mapping**
- This boils down to **replicating LoadLibrary ourselves**
 1. Allocate some executable space
 2. Copy PE sections into memory
 3. Resolve imports
 4. Call DLL entry (thread hijack optional)



User Mode Injection ft. Overwatch 2

NOTICE OF ACCOUNT CLOSURE

Greetings,

Account: [REDACTED]

Account Action: Account Closure - Overwatch Account

Offense: Unauthorized Cheat Programs ("hacks")

Recent activity on this account shows the use of an unauthorized cheat program, also known as a "hack", which harms the intended player experience.

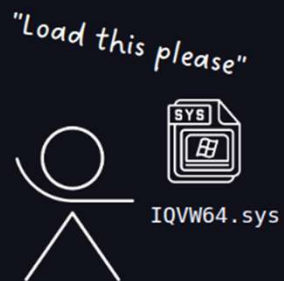


- Our first ban \o/
- Where a kernel anti-cheat can block us, OW2 is in usermode so can only crash or deliver a ban

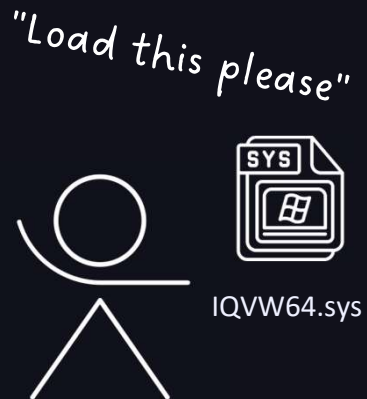
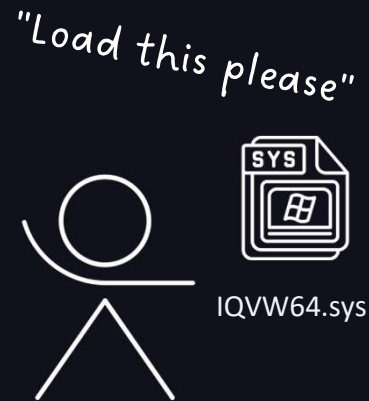
BYOVD++ ft. Rainbow 6

Let's Try to Get Banned: BYVOD

BRATISLAVA, PRAGUE — January 11, 2022 — ESET Research has released an in-depth blogpost offering an in-depth look into the abuse of vulnerable kernel drivers. Vulnerabilities in signed drivers are mostly utilized by game cheat developers to circumvent anti-cheat mechanisms, but they have also been observed being used by several APT groups and in commodity malware. The blogpost discusses the types of



BYOVD++ ft. Rainbow 6



BYOVD++ ft. Rainbow 6

Account Alert for horseman740 - 8 Jul, 2025

You've been permanently banned in Tom Clancy's Rainbow Six® Siege X by the game's developers.

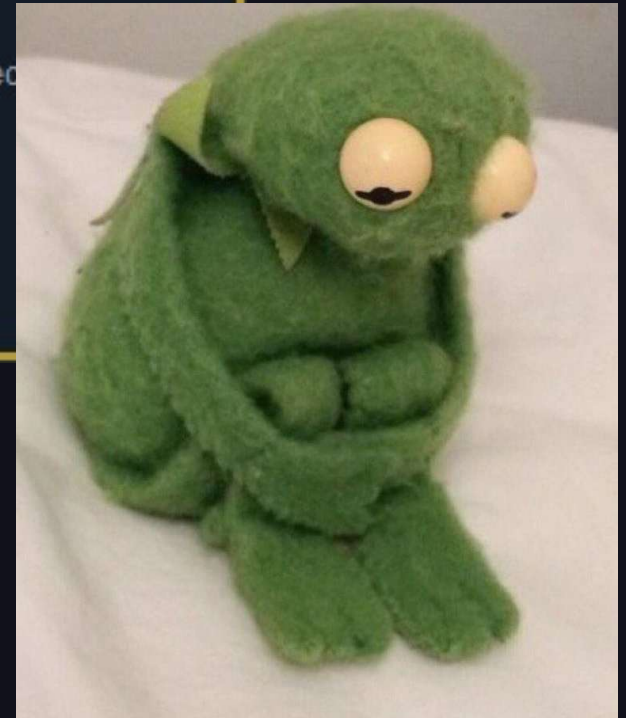
You can view your Steam account status by visiting your [ban history](#).

Please see our [In-Game Ban](#) page for more details.

BANNED FOR CHEATING



You have been permanently banned from the Rainbow Six Siege servers for multiple cheating offenses.

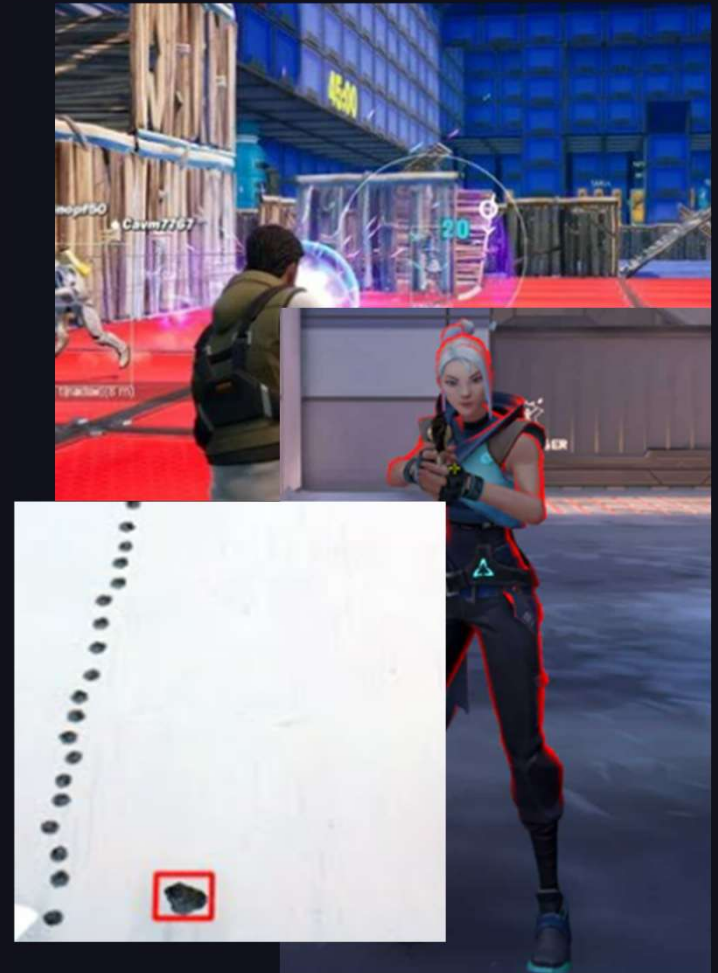


Some Mousey Cheats

Aimbots – Aim for you, can shoot for you, achieved simulated inputs

Pixelbots – Shoot for you on a color change via simulated clicks

Macros – Shoot or move for you in specific patterns e.g. to reduce recoil



Keyboard++ ft. Apex Legends

Cheats may simulate inputs. Can usual inputs get us banned?

The keyboard problem:

- Modern keyboards are too small and lack soul
- We prefer to compose our movement more tastefully
- Presenting... keyboard++



Keyboard++ ft. Apex Legends



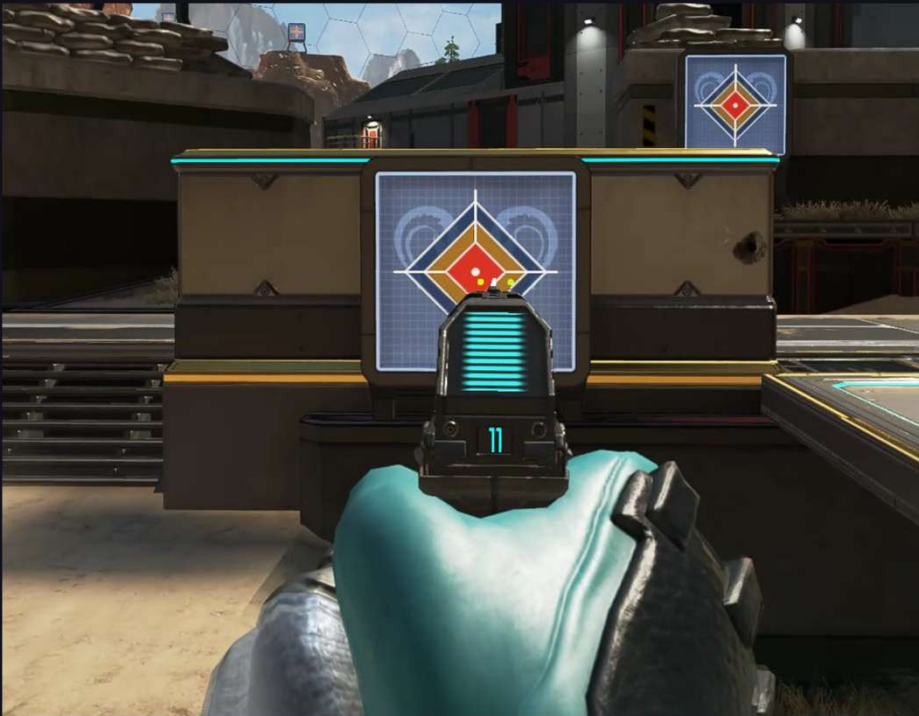
Keyboard++ ft. Apex Legends

Log in the next day – unfortunately, we can still play!

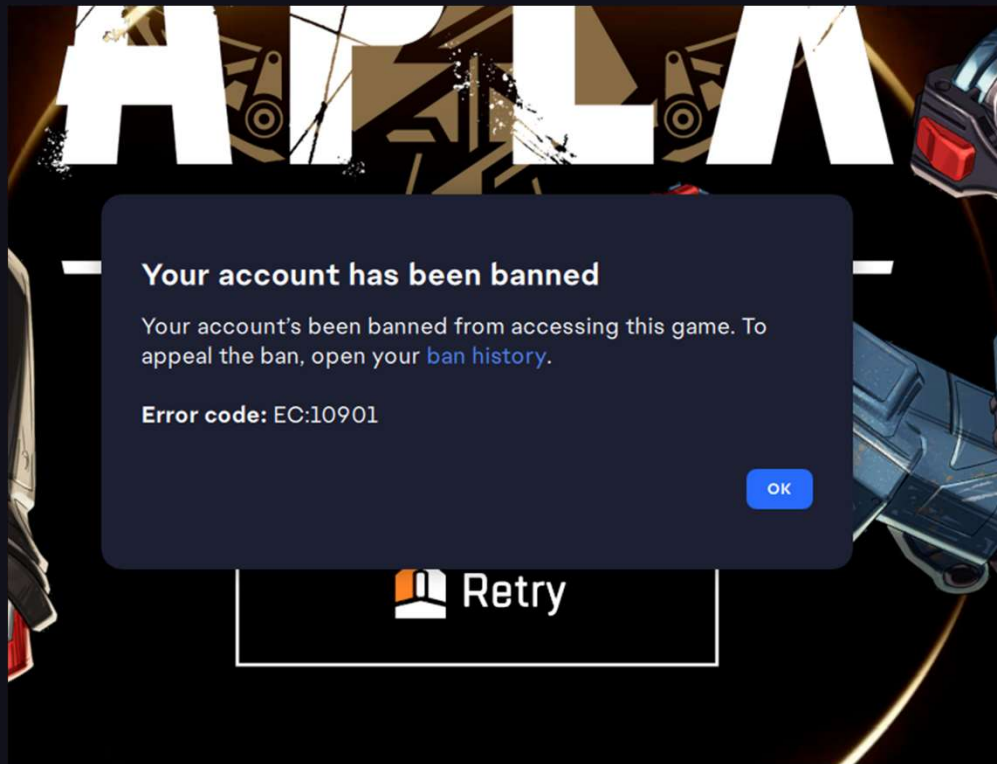


Keyboard++ ft. Apex Legends

A dramatic pause it great, but the input is too slow! Let's improve that.



Keyboard++ ft. Apex Legends



So what happened?

- a) EA hates classy music?
- b) We've run into one or more anti-cheat measures

Two Likely Possibilities:

1. Macro Detection
2. Aimbot or Pixelbot Detection

Keyboard++ ft. Apex Legends

	Macro	Aimbot	Pixelbot
Timing Checks	✓	✓	✓
Screen Capture Detection	✗	✗	✓
Input Source Analysis	✓	✓	✓
Memory Read Detection	✗	✓	✗

Trigger 1 – Third Party Software creating synthetic inputs

Trigger 2 – Inhuman click timing e.g. exactly 10ms between each input

Extra Sensory Perception

Wallhacks – Show player overlays through walls, a classic

Radars – Show players or loot on a minimap

Other – Any game state info you shouldn't know, reloads, aiming, line-of-sight



Crosshair++ ft. Fortnite

ESPs show enemy locations overlayed onto the game. Can this get us banned?

The crosshair problem:

- Most crosshairs are boring and uninformative
- My attention span is too cooked to pay attention to most crosshairs
- Presenting... crosshair++



Crosshair++ ft. Fortnite



Crosshair++ ft. Fortnite



This account has been banned.

Due to recent actions on your account, you have been banned
for:
Exploiting

Crosshair++ ft. Fortnite

What's the problem Epic?

- a) The meme format hit a little close to the bone?
- b) Our overlay has triggered anti-cheat measures

Trigger 1 – No-click window in front of the game process and...



Two Likely Possibilities:

1. General Overlay Detection
2. Specific Wallhack Detection

Trigger 2 – Image is being constantly updated (pointing hand)

Memory Injection++ ft. Valorant

APIs Suck:

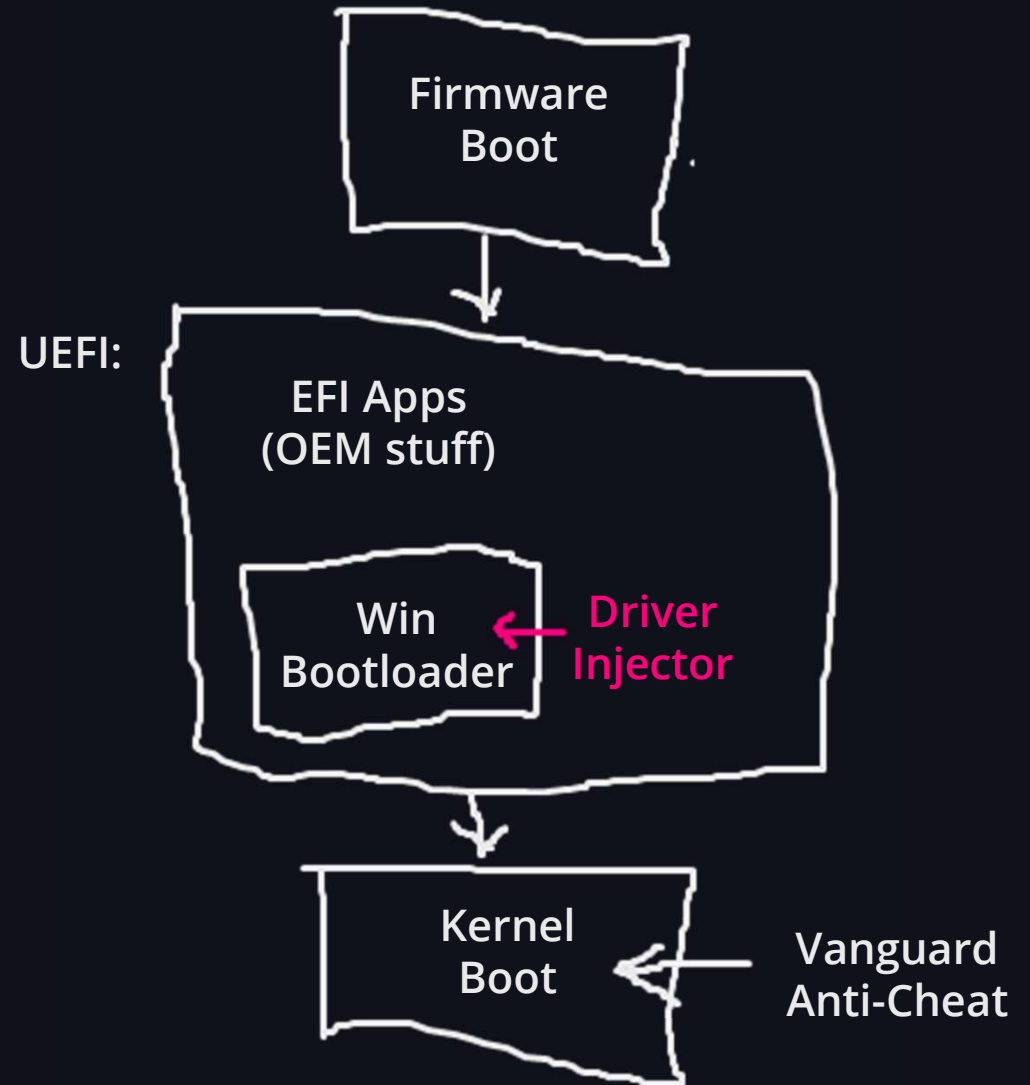
- Loading a driver normally is too easy to prevent
- We can't just load before the game starts as Vanguard runs from boot
- What if we could get our code into the kernel without the help of a vulnerable driver?



Memory Injection++ ft. Valorant – Variant 1: UEFI

EFI:

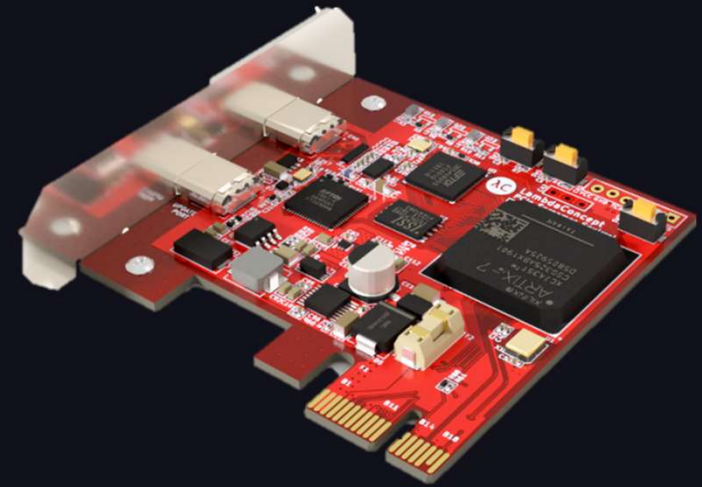
- We disable secure boot
- Run our injector from the UEFI/BIOS boot environment
- Write our own code into the boot cycle
- Map our mischievous driver before/as windows is loaded



Memory Injection++ ft. Valorant – Variant 2: DMA

Direct Memory Access (DMA):

- A separate PCI card which circumvents the CPU entirely
- Camouflaged as a legitimate device if required
- We can then stealthily map our code into the kernel



Memory Injection++ ft. Valorant

ACCOUNT LOCKED

This is an automated message that this VALORANT account has been permanently suspended. Once you close this message, you'll return to the login screen.

Player reports and an automated gameplay review show that this account used prohibited third party tools to gain an unfair advantage, which breaks our user rules (Section 7 in our Terms of Service) and ruins the game for other players.

True competition can't exist without fair play and you'll never know how good you really are until it's just you and the game. Always give both other players and yourself an honest shot. If you have

I Understand

So what happened?

- Vanguard hooks into the windows page fault handler
- Using this trick they can catch unsigned kernel code executing
- It doesn't matter how the code got there!

Road Map

1: Intro and not getting banned

- Game cheats and anti-cheats
- Methods that don't lead to a ban

3: Staying Banned

- Account vs Hardware Bans
- How Hardware Bans work
- How to spoof hardware serials/IDs

2: Getting Banned

- What gets you banned from various big titles
- How to do it with style

4: Getting Others Banned

- Get someone else banned
- Make any Malware Worse!
- Make your friends go and play outside.

Account Vs Hardware Ban

- Rewind to 2015...
- You've been banned from Rainbow 6 Siege
- **No Problem!**
- Make a new account, get back to cheating
- Do it again...
- ...and again



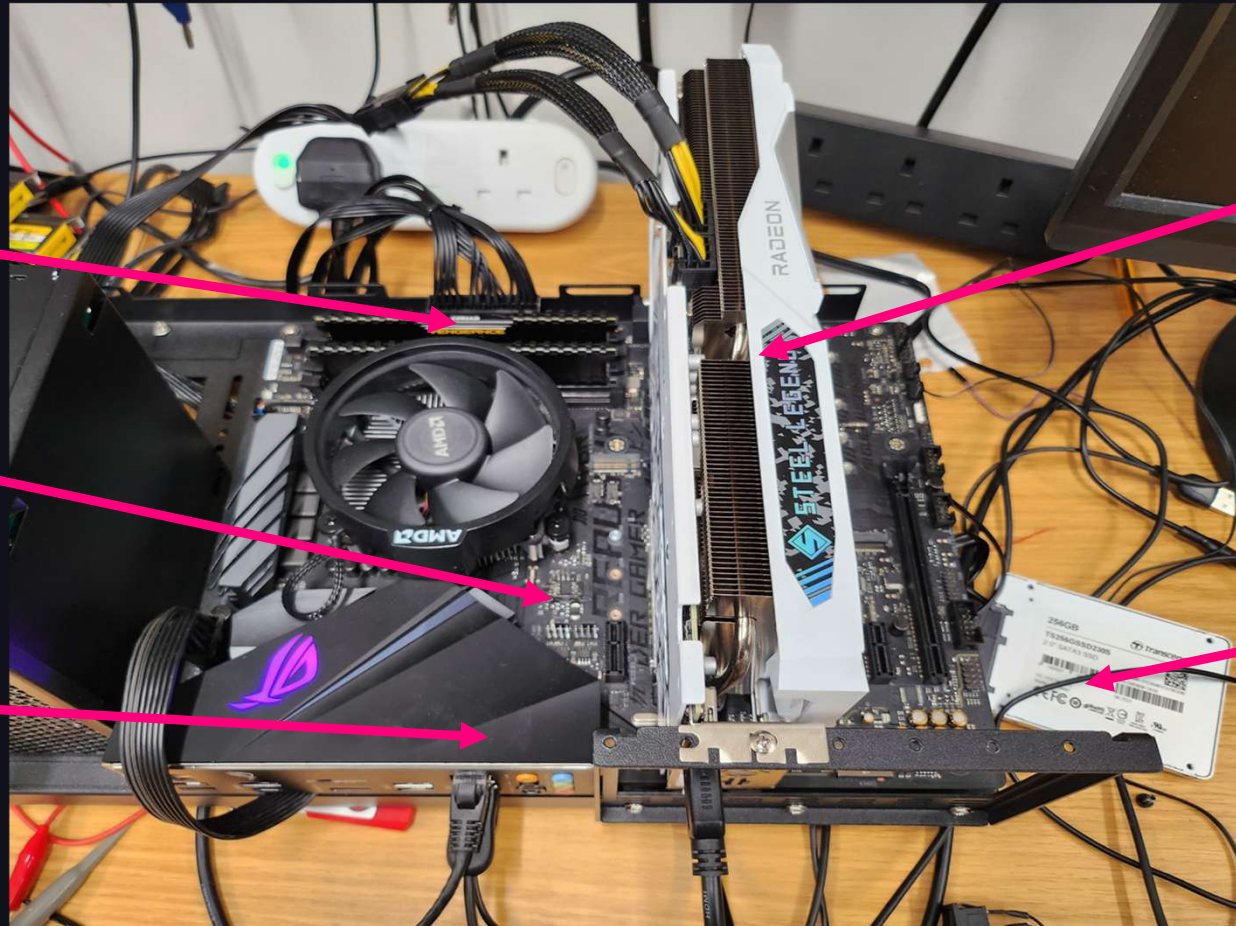
The answer? Hardware ID Bans

Some Hardware IDs

DIMM Memory
Serials

Motherboard
Serials + IDs

Internal or
External NIC



GPU
Serials

Volume Serials
and OS Info

Dumping out the Hardware IDs

```
Getting HWIDs...

Motherboard Serial Number:
SerialNumber
NBQDS1100214302E253400

System UUID:
UUID
19B01C4D-5F35-EC11-80E2-088FC3258920

Memory Chip Serial Numbers:
SerialNumber
A2C851E9
A4C85218

GPU(s):
Name                                PNPDeviceID
Intel(R) UHD Graphics               PCI\VEN_8086&DEV_9A60&SUBSYS_15401025&REV_01\3&11583659&0&10
NVIDIA GeForce RTX 3070 Laptop GPU  PCI\VEN_10DE&DEV_249D&SUBSYS_15401025&REV_A1\4&6CEB2C9&0&0008

Main Network Adapter MAC Address:
0A:00:27:00:00:0C

Done.
```

*example IDs are already banned on some titles

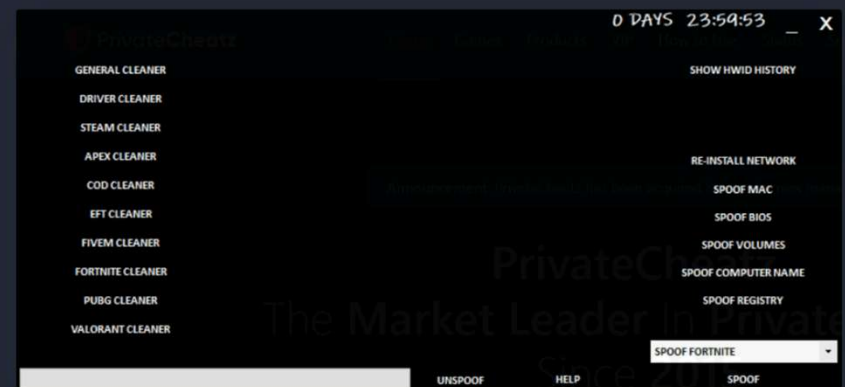
Hardware ID Spoofer

- You can buy hardware ID spoofers from game cheat websites
- Most spoof the reporting of the IDs to software
- So can be detected by anti-cheats.
- Can we directly change the hardware?

HWID Spoofer By PC V2

By Zack Zwiezen – Last Updated: May 1st 2023

Anti-cheat companies are gradually becoming more creative when it comes to how they intend to ban cheaters from their games more permanently, especially due to the rising prevalence of free to play games. The PC V2 [HWID spoofer](#) can help prevent you from getting your whole machine hardware banned if you ever get caught hacking.



1-Day Access

\$4.99

7-Days Access

\$19.00

30-Days Access

\$49.00

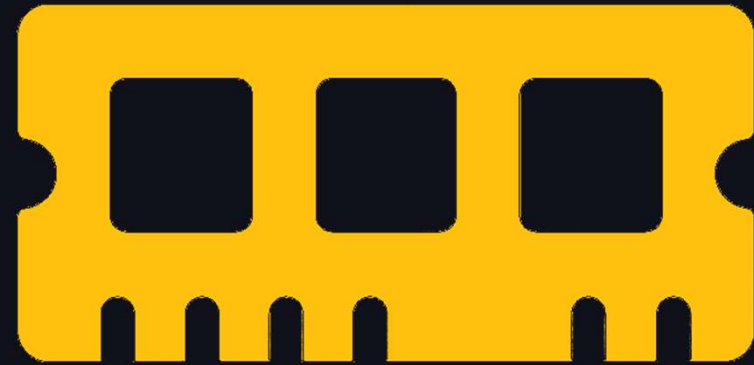
Examples

There is too much hardware to cover in one talk!

Focuses:



Motherboard



RAM

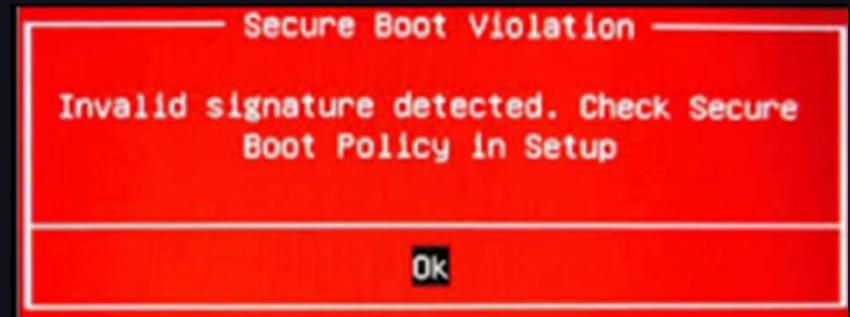
Motherboard Shenanigans

Attempt 1

- Load AMI Firmware Update software onto USB
- Boot into EFI shell
- Change IDs for the current power cycle

Issues

- Volatile (resets on power cycle)
- Limited functionality
- Violates secure boot ☹️



Motherboard Shenanigans

Attempt 1 2

- Boot machine into MSDOS
- Using AFUDOS utility, dump the BIOS
- Scan for and change desired serials – incl. inbuild MAC on some boards
- Using AFUDOS utility, flash the edited BIOS

**BIOS WRITE
PROTECTIONS!**

Problem Solved

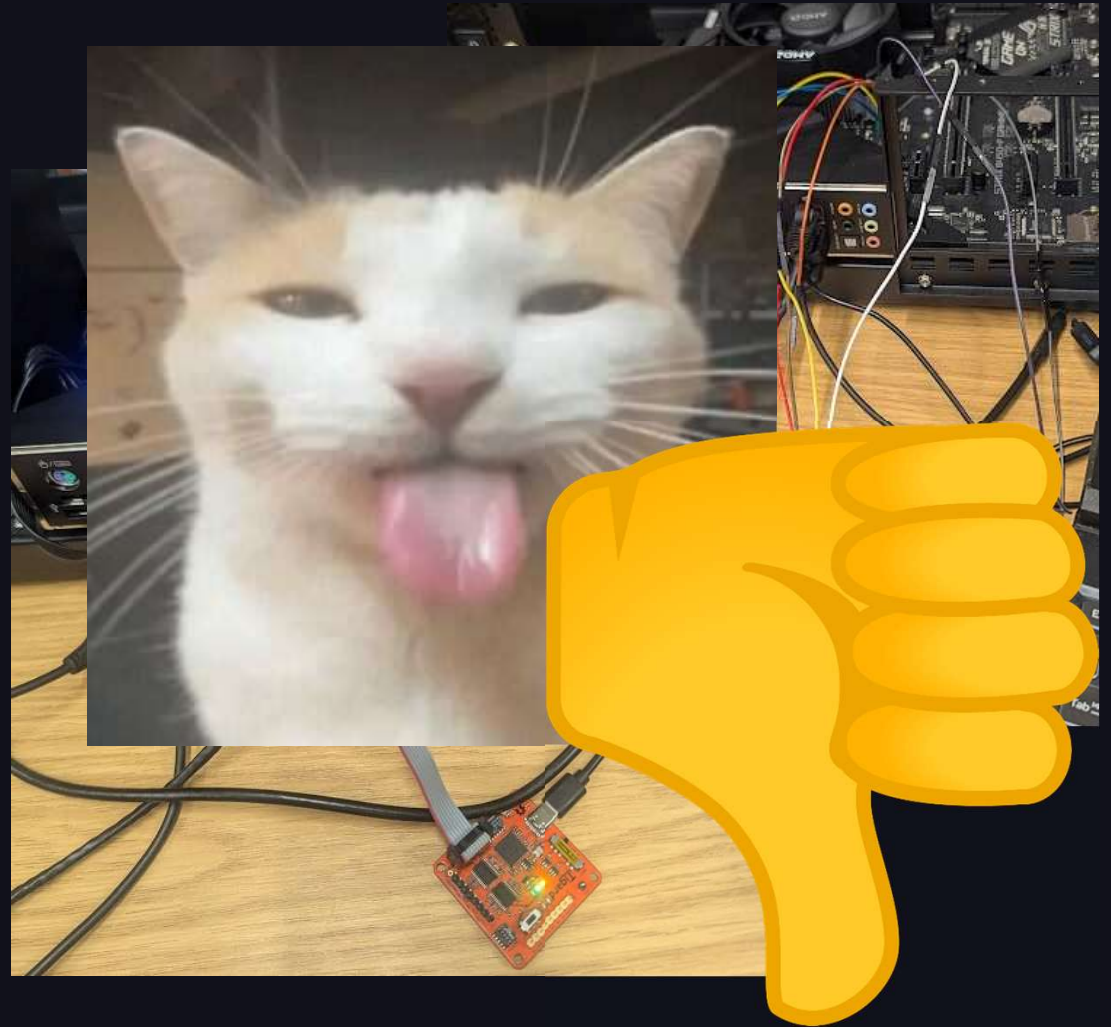
- Non-volatile
- Bypasses secure boot
- YIPPEE?



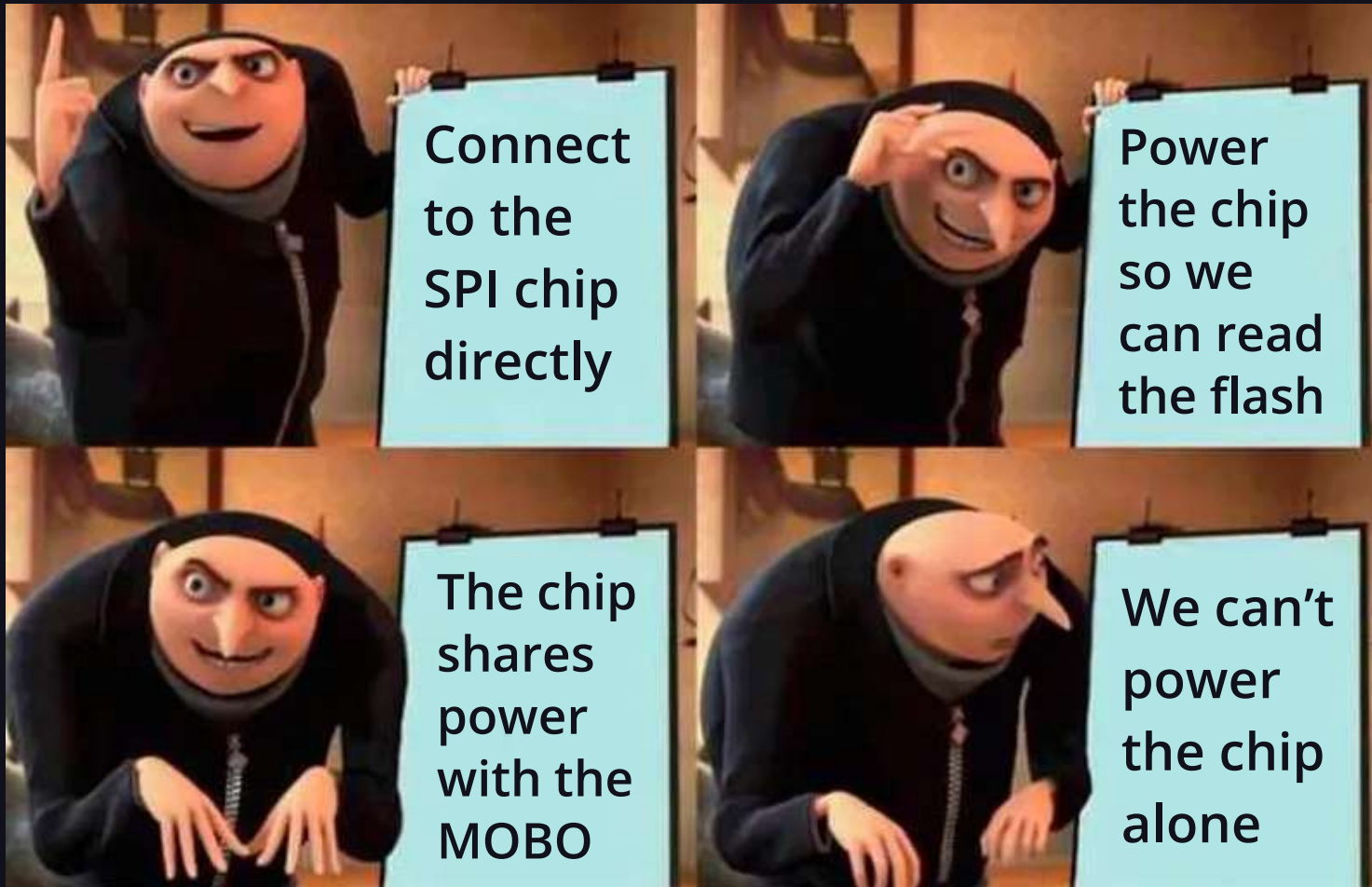
Motherboard Shenanigans

Attempt 1 2 3

- Connect to the onboard SPI chip (EEPROM) directly
- Interface from a separate machine using flashrom
- Dump, edit, and then reflash the BIOS
- Profit?



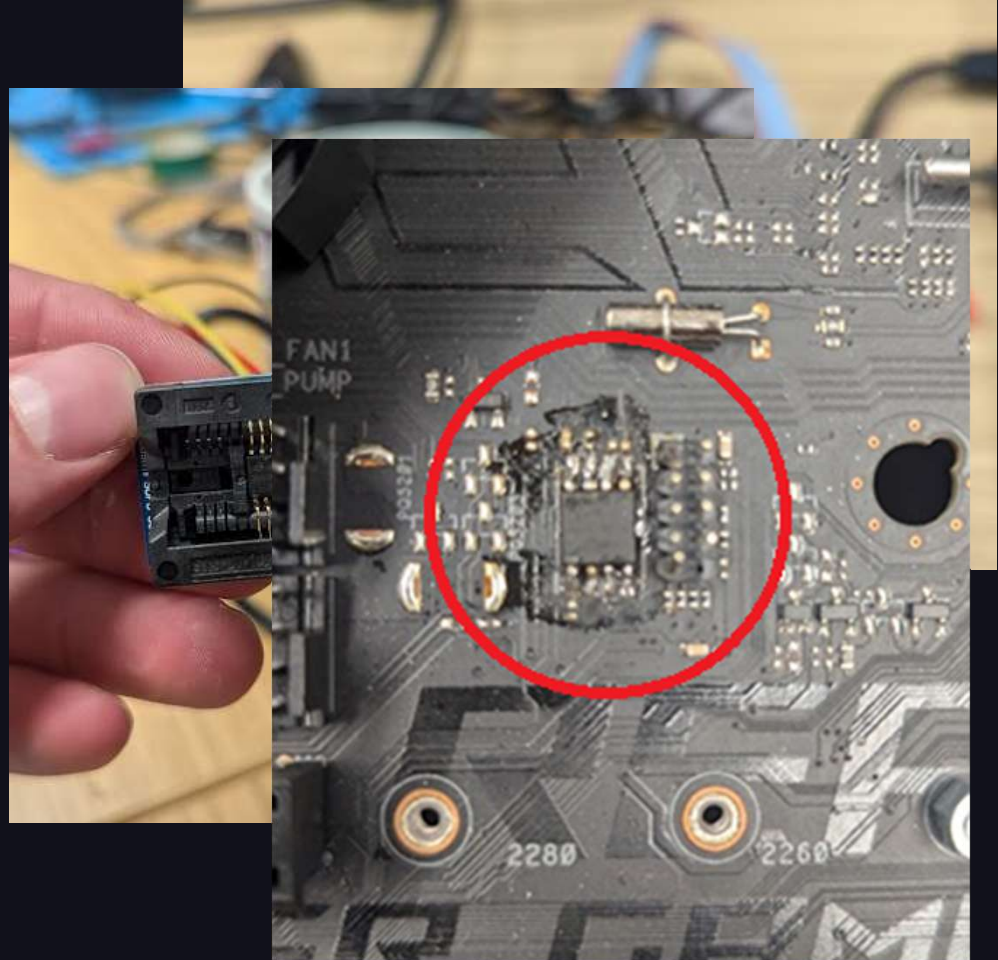
Motherboard Shenanigans



Motherboard Shenanigans

Attempt 1 2 3 4

- Desolder the SPI chip from the motherboard
- Connect to adapter then interface via flashrom
- Flash edited BIOS
- Resolder SPI chip to motherboard



Motherboard Shenanigans

Before

Manufacturer	Product	SerialNumber	Version
ASUSTeK COMPUTER INC.	ROG STRIX B450-F GAMING	230215316500238	Rev 1.xx



After

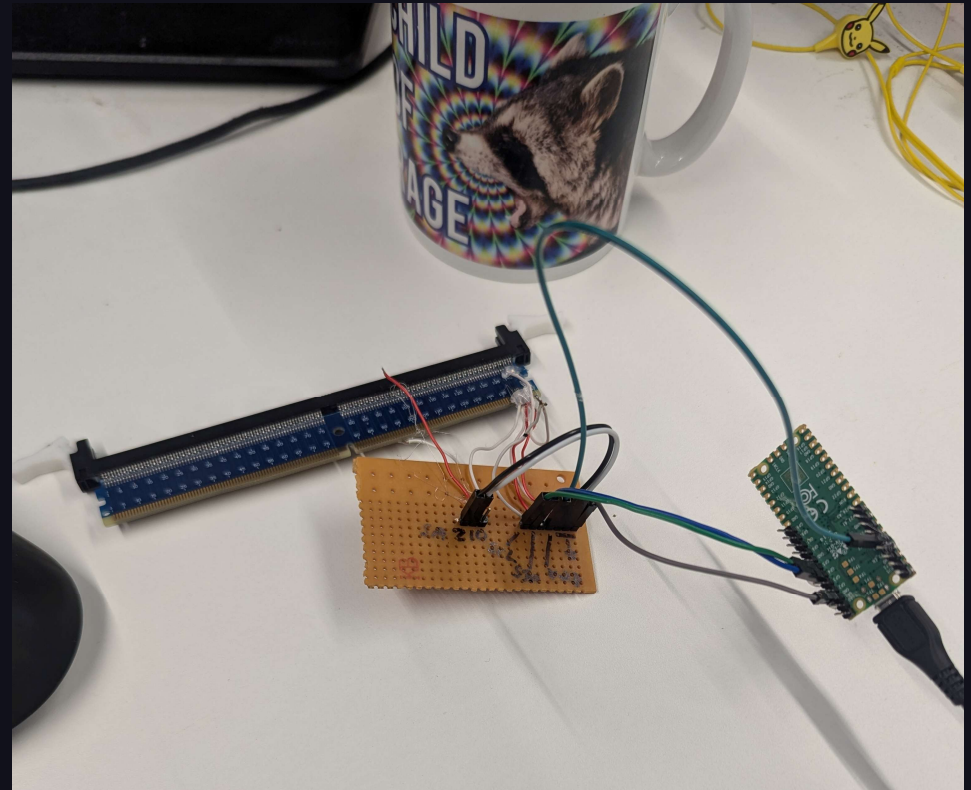
Manufacturer	Product	SerialNumber	Version
Incog Tek Inc.	Inconspicuous Mobo	19095855110421	Rev 1.xx

Spoofing RAM

RAM is traditionally difficult to spoof from hardware due to:

- lack of software tools
- no SPI interface
- write protected chips

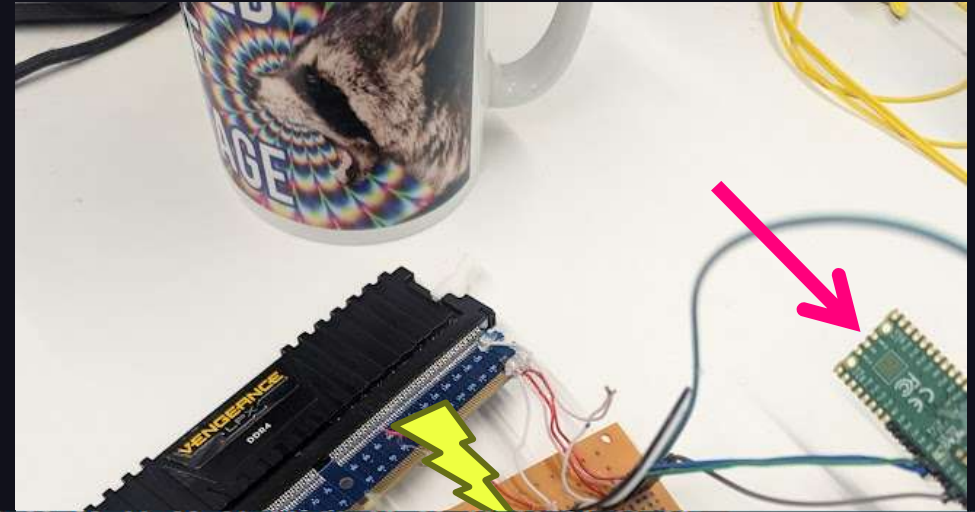
The adapter setup required to overcome this is a little messy



*thanks to the BADRAM project

Spoofing RAM – The Process

1. Connect DIMM adapter to a Pi Pico
2. Dump SPD chip (EEPROM) data
3. Hex edit the serials to desired ID values
4. Kill write protection on the chip
 - Send 7V down pin 139
 - Issue CWP command to 0x33
5. Write edited SPD dump back to the chip and profit



```
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 B6 58
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
9E 00 00 00 1F 23 BB E8 43 4D 4B 33 32 47 58
4D 32 41 32 36 36 36 43 31 36 00 00 00 80 2C
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
4A 05 20 00 00 00 00 94 00 00 06 FF FF 03
60 6C 6C 10 D1 3E 30 11 F0 0A 20 08 00 B0 1E
00 00 00 00 00 00 00 00 00 00 F6 F6 F6 F6 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA
```

```
.....x
.....
.....
.....
.P...#CMK32GX
4M2A2666C16...Ç,
.....
.J.....ö
`ll.τ>0.=...
0.....÷÷÷÷
```

Road Map

1: Intro and not getting banned

- Game cheats and anti-cheats
- Methods that don't lead to a ban

3: Staying Banned

- Account vs Hardware Bans
- How Hardware Bans work
- How to spoof hardware serials/IDs

2: Getting Banned

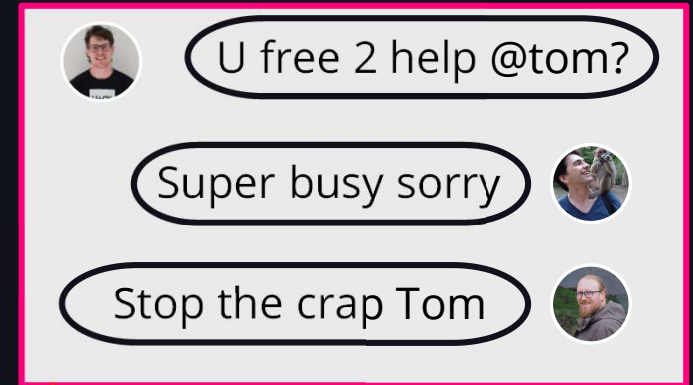
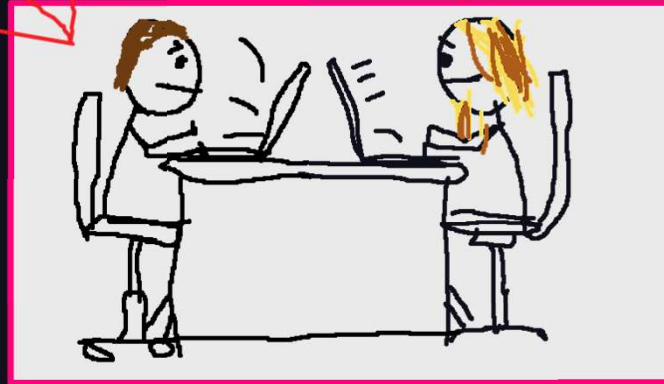
- What gets you banned from various big titles
- How to do it with style

4: Getting Others Banned

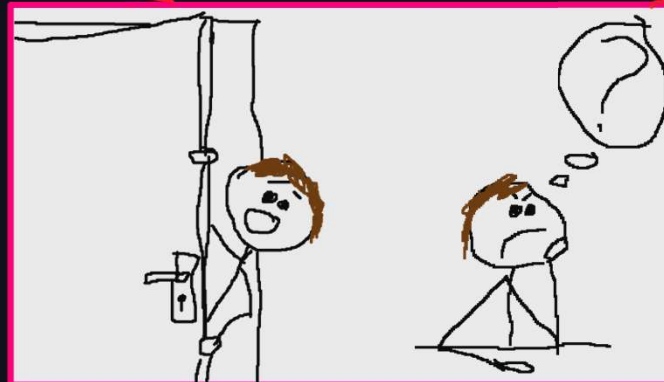
- Get someone else banned
- Make any Malware Worse!
- Make your friends go and play outside

A Supervision Issue

April 1st 2025...
Twas the night before
the BHUSA deadline –
Sam and Marius were
hard at work...



Meanwhile...



A devious prank is
imagined to save
future PhD students

A Week Later...

- I come into work.
- Select All + Delete my emails
- Settle in for a morning playing Valorant

....

NOOOOOOOO!

CONNECTION ERROR

A review detected that actions of an account playing on this device violated the User Rules (Section 7) of our Terms of Service. This device is now restricted from access. Fair play and respecting the integrity of a match are essential to be a team that wins together. We encourage you to reflect on your behavior to be a respectful player in future games. You can visit our Terms of Service to learn more, including your right to appeal.

Error Code: VAN 152

QUIT

What Happened?

- Sam ran a script on Tom's machine to dump out the hardware IDs.
- Sam faked those hardware IDs on his machine.
- Sam got his machine (with Tom's hardware IDs) banned.
- The next day Tom logs into the game, the anti-cheat sees banned hardware IDs and bans Tom's account.
- Result: Tom has to do some work on the damned slides.

This Could Make Any Malware Much Worse

Grandoreiro : Banking Malware that steals money

PowerGhost : Mines Crypto using your machine

Stuxnet : Disable nuclear centrifuges

This Could Make Any Malware Much Worse

Grandoreiro++: Banking Malware that steals money and gets you banned from Rainbow 6.

PowerGhost++: Mines Crypto using your machine and gets you banned from Valorant.

Stuxnet++: Disable nuclear centrifuges and stop nuclear engineers playing Fortnite. No more victory royales.

Game Bans as an Attack

- This is not a problem for weaker anti-cheats (like VAC) that do not hardware ban
- Getting innocent people banned in games is a real attack that works in practice
- Any attempt to mitigate this attack would make hardware banning much weaker

Road Map

1: Intro and not getting banned

- Game cheats and anti-cheats
- Methods that don't lead to a ban

3: Staying Banned

- Account vs Hardware Bans
- How Hardware Bans work
- How to spoof hardware serials/IDs

2: Getting Banned

- What gets you banned from various big titles
- How to do it with style

4: Getting Others Banned

- Get someone else banned
- Make any Malware Worse!
- Make your friends go and play outside

Summary of Cheat Technique, Bans and Games

- **Basic techniques blocked but no ban**
 - Common cheat tools, opening process, reading/writing memory, loading vulnerable drivers.
- **Mapping code into the game process - ban on Overwatch.**
- **Mapping code into the kernel - ban on Rainbow 6.**
- **Simulate inputs - ban on Apex Legends.**
- **Add a video overload - ban on Fortnite.**
- **Load our own driver sneakily - ban on Valorant**

Conclusion

- Modern anti-cheats shrug off many traditional cheat attempts
- Properly getting banned can be very easy or very hard
- Modifying hardware is the king of spoofing
- The touchgrassm8™ and StreamerBan3000© available now in your town



<https://game-research.github.io/>