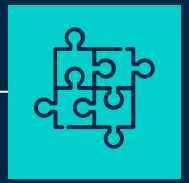
Glitches & Breaches

Vulnerabilities and Threats in the Video Game Industry

Irene Ioannidou
Creative Director – Vongrid

TABLE OF CONTENTS



01

WHY GAMES?

Software is Sowftware but...

02

SECURITY CHALLENGES

From Cheats to Threats...

03

USE CASE

Let’s Exploit...

WHY GAMES?

Software is Software but...

01

GAMING INDUSTRY

- The largest entertainment industry in the world (a market worth more than US$ 197 billion in 2022).
- The pandemic has caused a massive 26% increase in growth in 2019 and 2021
- large and growing industry, where cash and data are exchanged online
- Magnet for malicious actors.

GAMING INDUSTRY

Home > News > Security > Android Minecraft clones with 35M downloads infect users with adware

Android Minecraft clones with 35M downloads infect users with adware

By Bill Toulas

April 27, 2023 03:42 PM 0

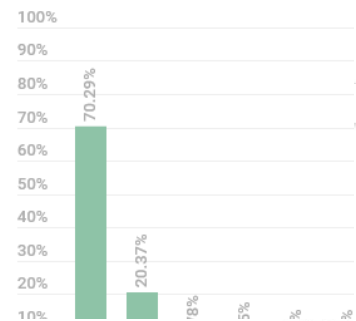
CYBER SECURITY NEWS · 4 MIN READ

Security Breach at Riot Gam
Game Cheats, Source Code
eSport "League of Legends"

SCOTT IKEDA · JANUARY 30, 2023

If you're not familiar with the world of competitive on
be wondering why the leak of game cheats would be n
because the game in question is one of the biggest in t
eSports industry. A security breach at Riot Games has
code for League of Legends, as well as several other ti

Riot says that player personal and financial
information was not compromised in the



ORF OBSERVER RESEARCH FOUNDATION

Ideas · Forums · Leadership · Impact

RESEARCH CENTRES FORUMS EVENTS ABOUT US

Mining Pentagon data

In April 2023, several highly classified documents, some even marked "Top Secret", were leaked on a Discord server, dedicated to "Minecraft", a popular video game. The data later found its way to social media platforms like Twitter and Telegram.

The documents contained sensitive information such as Ukraine's status in its ongoing conflict with Russia, potential problems with Ukrainian ammunition supplies, and the losses sustained by the Russian military. Apart from this, they also provided a strong indication that the United States (US) has been spying on its allies,

ind the leaks remains unclear, but it seems to have

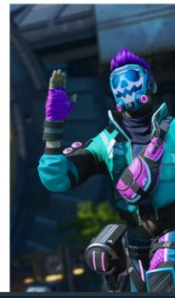
Home

How can w
health and
Find out in The Cli

Apex Le
hack cla

18 March 2024

By Tom Richardson, BE



BBC

Newsweek U.S. World Science Health Life Rankings Opinion Entertainment Fact Check My Turn Education

LIVE Both Sides Deliver Closing Arguments In Trump Hush Money Trial

Science Fortnite Battle Royale

'Fortnite' Free V-Bucks Scam: How to Spot Fake Websites Pushing Hacks, Cheats, In-Game Money

Published Jun 26, 2018 at 8:21 AM EDT | Updated Jun 26, 2018 at 8:55 AM EDT

By Jason Murdock
Reporter
FOLLOW

0

Fortnite players are being targeted by social media scammers who are using websites claiming to offer free in-game currency, known as V-Bucks, to hijack accounts and pilfer personal data.

British authorities said on Monday that they had received 35 reports of *Fortnite*-related fraud between April 1 and March 31, with up to $6,800 (£5,120) being stolen in total. Complaints were lodged by dozens of angry parents who discovered their kids had been exploited by the scams.

In the majority of cases, players are directed to follow links spread across social media platforms like Facebook which claim to offer free in-game money, used to purchase cosmetic items for their character. In reality, fraudsters set up "phishing" websites to log personal information and account details.

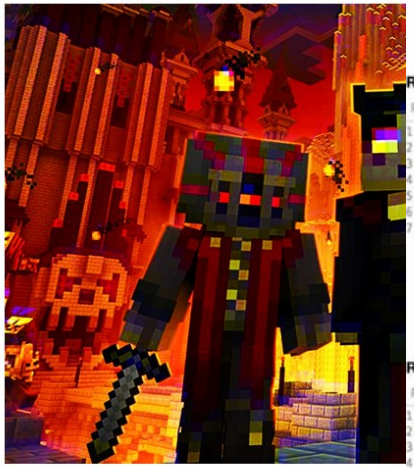
According to Action Fraud, which revealed the scale of the issue, culprits have asked for phone numbers in return for fake V-Bucks which could then be used to sign the victim up to premium rate subscription services. In other cases, scammers sold access to the stolen *Fortnite* accounts. On Tuesday, *Newsweek*

GAMING INDUSTRY

Home > News > Security > Android Minecraft clones with 35M downloa

Android Minecraft clones with 35 adware

By **Bill Toulas**



A set of 38 Minecraft copycat games on Google Play 'HiddenAds' to stealthily load ads in the backgrounc

Minecraft is a popular sandbox game with 140 milli publishers have attempted to recreate.

The Minecraft-like games hiding adware were down worldwide, mainly from the United States, Canada,

Request

```
GET /3.txt HTTP/2
Host: 9c1726648c832281ac953adff5a541574.netlify.app
User-Agent: Dalvik/2.1.0 (Linux; U; Android 12; Pixel 5a Build/SQ3A.220705.003.A1)
Connection: Keep-Alive
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/2 200 OK
Accept-Ranges: bytes
Age: 214346
Cache-Control: public, max-age=0, must-revalidate
Content-Type: text/plain; charset=UTF-8
Date: Sat, 28 Jan 2023 14:19:36 GMT
Etag: "e8ee293a22df4c6e8307f0382cc3fe36-ssl"
Server: Netlify
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
X-Nf-Request-Id: 01GR2RCBGG7FXVFSCW9QAGNYYQ
Content-Length: 119

[{"id":"153d21ab9","id1":"1","id2":"2","id3":"3","init":1,"note":"default","pack":"","pe1":90,
"pe2":150,"status":true}]
```

Request

```
GET /3.txt HTTP/2
Host: c6731f27aeac4c2f979dcf277f5b133b73.netlify.app
User-Agent: Dalvik/2.1.0 (Linux; U; Android 12; Pixel 5a Build/SQ3A.220705.003.A1)
Connection: Keep-Alive
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/2 200 OK
Accept-Ranges: bytes
Age: 68428
Cache-Control: public, max-age=0, must-revalidate
Content-Type: text/plain; charset=UTF-8
Date: Mon, 30 Jan 2023 07:37:04 GMT
Etag: "8db62da800b0e4fe25ce072d41960bca-ssl"
Server: Netlify
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
X-Nf-Request-Id: 01GR2TZK3FZS0P1YHWZYB0Z1WR
Content-Length: 156

[{"id":"142cc1cb9","id1":"ca-app-pub-7647808421428026/8860272654","id2":"2","id3":"3","init":1
,"note":"default","pack":"","pe1":90,"pe2":150,"status":true}]
```

Request

```
GET /3.txt HTTP/2
Host: 3773c6b1e37ec29835d75fe8eb9ee1d8.netlify.app
User-Agent: Dalvik/2.1.0 (Linux; U; Android 12; Pixel 5a Build/SQ3A.220705.003.A1)
Connection: Keep-Alive
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/2 200 OK
Accept-Ranges: bytes
Age: 35627
Cache-Control: public, max-age=0, must-revalidate
Content-Type: text/plain; charset=UTF-8
Date: Mon, 30 Jan 2023 16:44:44 GMT
Etag: "428b0670c67349b6886646a672d9c652-ssl"
Server: Netlify
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
X-Nf-Request-Id: 01GR2V1C0Y2RVNQRWAJ46XC4N3
Content-Length: 156

[{"id":"153d300d9","id1":"ca-app-pub-3020711908526811/8524393014","id2":"2","id3":"3","init":1
,"note":"default","pack":"","pe1":90,"pe2":150,"status":true}]
```

GENSHIN IMPACT – 2020

Vulnerable Anti-Cheat Driver

- Netfilter, FiveSys, and Fire Chili.
- Rootkits usually signed with stolen certificates or falsely validated.
- A legitimate driver was is used as a rootkit.
- mhyprot2.sys, a vulnerable anti-cheat driver for the popular role-playing game Genshin Impact.
- The driver was abused by a ransomware actor to kill antivirus processes and services for mass-deploying ransomware.
- mhyprot2.sys can be integrated into any malware.

KEY CHALLENGES

02

From Cheats to Threats...

KEY CHALLENGES

THREATS

- Cheating and Hacking
- Account Takeovers
- Distributed Denial of Service (DDoS) Attacks
- Ransomware
- Data Breaches

VULNERABILITIES

- Unpatched Software
- Insecure Network Communications:
- Third-Party Plugins and Mods
- User Input Validation
- Social Engineering

CHEATS

SOFT CHEATS

- Bugs and exploits
- Exchanging real money for in-game goods and services

HARD CHEATS

- Bots and other automated tools
- Utilizing secret game data
- Packet modification and replay attacks
- Spoofing

HISTORY OF CHEATING

1985

- Konami Code (up, up, down, down, left, right, left, right, B, A, start)
- added to 1985's Gradius for the NES by Kazuhisa Hashimoto, who found the game to be too difficult during its debugging phase.

HISTORY OF CHEATS

	DATE	REASON	DESCRIPTION
MERCURY	2010	Jupiter	It’s the closest planet to the Sun and the smallest one
MARS	2012	Neptune	Despite being red, Mars is actually a cold place
VENUS	2016	Saturn	It has a nice name and is the second planet from the Sun

ANTI-CHEAT METHODS

SERVER-SIDE METHODS

- checking incoming packets and ensuring that the data and game state are correctly handled on the server

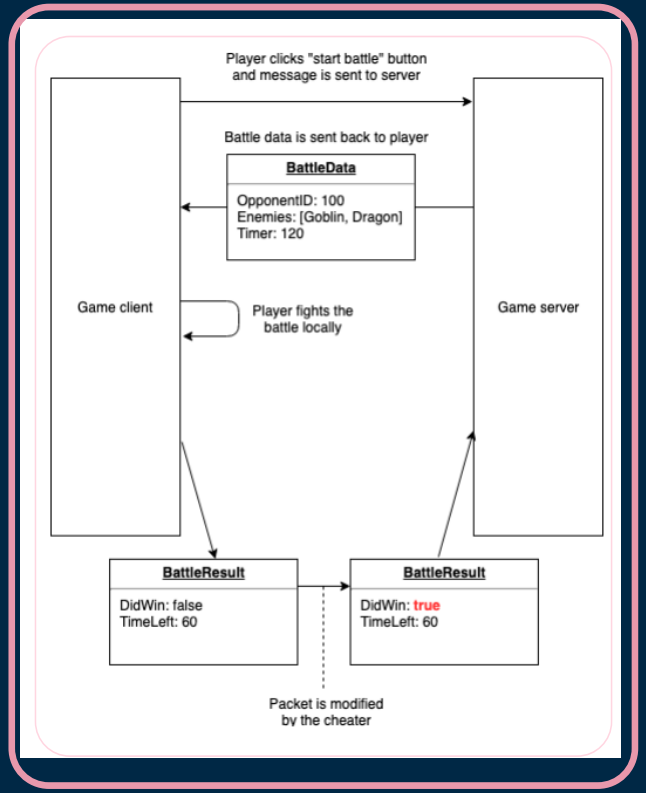
CLIENT-SIDE METHODS

- anti-cheat programs that operate on the client machine and send data back to the server

“DO NOT TRUST THE CLIENT”

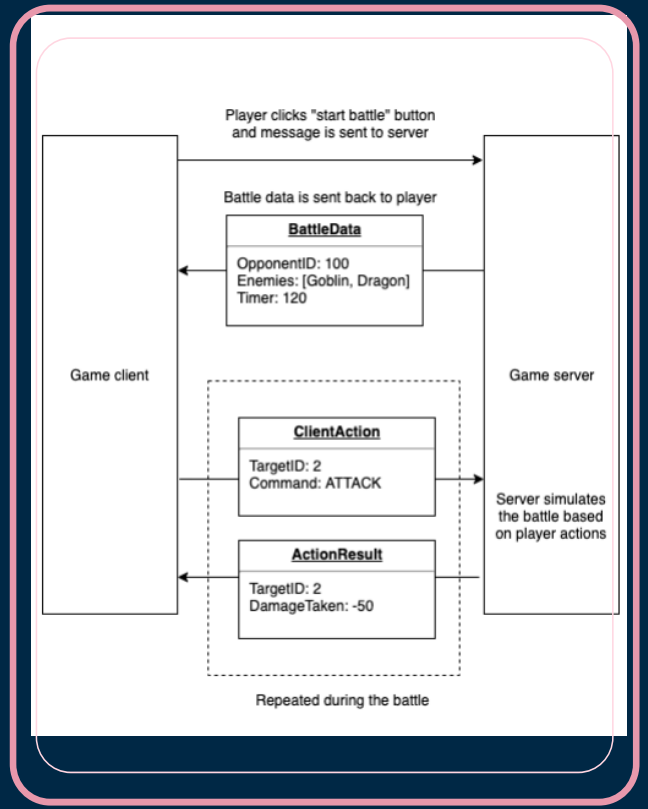
SERVER-SIDE ANTI-CHEAT METHODS

- Eg. Mobile turn-based online strategy has the battles fought on local device and then send the results to the server that blindly trusts the data.
- If the network traffic is not obfuscated, this type attack can be executed just by intercepting the packets and modifying the packet data on the fly without even touching the game client itself.



SERVER-SIDE ANTI-CHEAT METHODS

- Eg. Mobile turn-based online strategy has the battles fought on local device and then send the results to the server that blindly trusts the data.
- If the network traffic is not obfuscated, this type attack can be executed just by intercepting the packets and modifying the packet data on the fly without even touching the game client itself.



EARLY AGE ANTI-CHEATS

2000

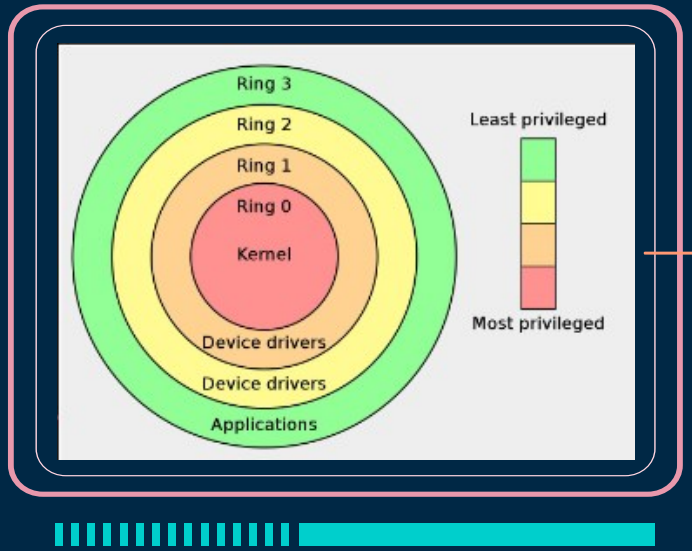
-Scans memory contents of the player's computer while the game is running.
-Monitors the game's files and configuration settings to detect unauthorized modifications.

2002

-Designed for Steam platform games
-Combines signature-based scanning, heuristic analysis, and player behavior monitoring to detect cheats.

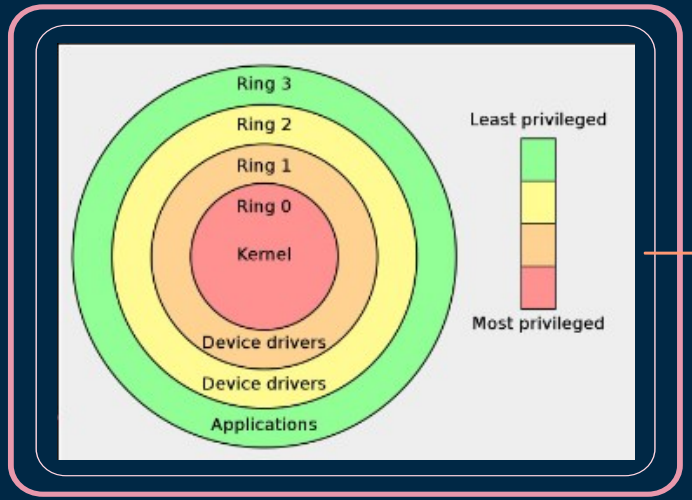
KERNEL LEVEL ANTI-CHEATS

- Kernel loads immediately after the bootloader.
- The kernel’s code has its area in memory and it’s protected from application programs.
- This means the kernel and the apps installed can work in parallel without interference or issues like a browser accessing kernel memory and changing how your operating system works altogether.



KERNEL LEVEL ANTI-CHEATS

- If we were to divide system privileges into four rings, from Ring 0 to Ring 3, the kernel's privileges would belong to Ring 0
- Ring 1 and 2 would be occupied by device drivers
- Apart from the usual anti-cheat client which is active while you play the game and scans what you have running on your computer, the kernel-level driver will load during startup and block certain drivers from loading or running.



KERNEL LEVEL ANTI-CHEATS
[Features]

1. Blocking / stripping of process handles in User Mode
2. Detection of test signing
3. Detection of usermode hooks
4. Detection of injected modules
5. Detection of manually mapped modules
6. Detection of kernel drivers
7. Detecting of traces of manually mapped drivers
8. Detection of virtual machines and emulation

MODERN & POPULAR(?) ANTI-CHEATS

01

WHY GAMES?

Here you could describe the topic of the section

02

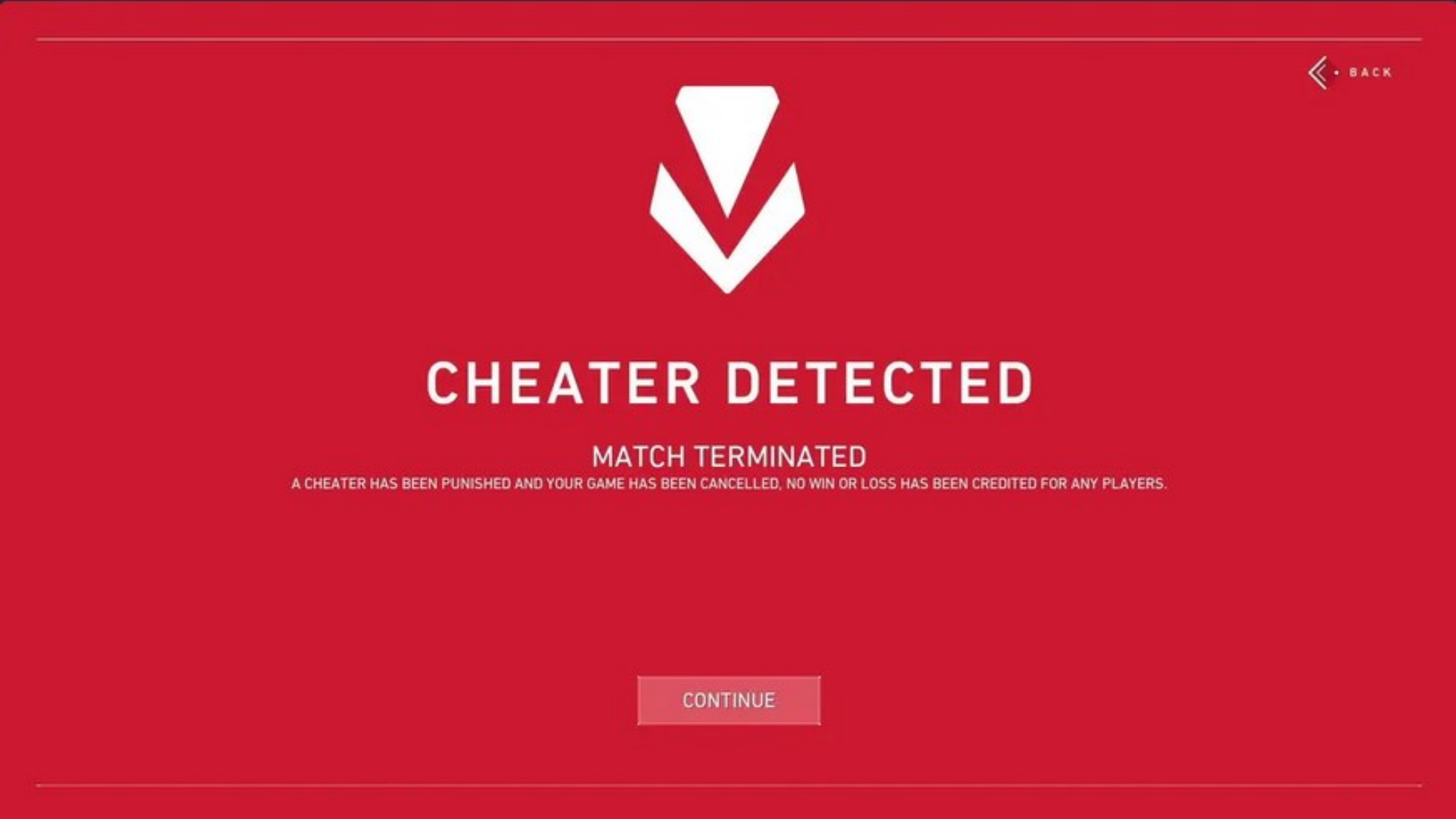
KEY THREATS

Here you could describe the topic of the section

03

DEFENDERS OR MALICIOUS

Here you could describe the topic of the section


BACK
CHEATER DETECTED
MATCH TERMINATED
A CHEATER HAS BEEN PUNISHED AND YOUR GAME HAS BEEN CANCELLED. NO WIN OR LOSS HAS BEEN CREDITED FOR ANY PLAYERS.
CONTINUE

KERNEL LEVEL ANTI-CHEATS
[RISKS]

1. Security Vulnerabilities
2. System Stability
3. Privacy Concerns

KEY CHALLENGES

THREATS

- Cheating and Hacking
- Account Takeovers
- Distributed Denial of Service (DDoS) Attacks
- Ransomware
- Data Breaches

VULNERABILITIES

- Unpatched Software
- Insecure Network Communications:
- Third-Party Plugins and Mods
- User Input Validation
- Social Engineering

USE CASE

Let’s exploit

03

HANDS ON

THANK YOU

"It's all fun and games until your kernel gets compromised"