



ForuM Club

KeyMac

Anti-Cheat Steam para la Comunidad de SNET





¿Qué es KeyMac?





KeyMac

KeyMac es un proyecto que tiene como objetivo brindar un servicio de Anti-Cheat para la comunidad de SNET. Siendo un producto libre y compatible entre toda la comunidad, fácil de montar y administrar. El cual le dará solución a muchos problemas con respecto al tema “Parcheros” en los diferentes servicios o juegos que la red provee.



Características

- Detecta procesos maliciosos y mouses con bloody.
- Gestión de cuentas y acceso a servicios.
- Recopila información y capturas del cliente.
- Whitelist/Blacklist de procesos y mouses.
- Integración con Steam u otros sistemas vía API.
- Lista de Servidores disponibles.
- Sistema altamente configurable y adaptativo.



¿Por qué surgió?





Surgimiento

A medida que la red crece, muchos servicios se están consolidando. Y cada día se montan diferentes juegos/servicios sin protección ya que los administradores no poseen el grupo de trabajo necesario para desarrollar un sistema propio de alta calidad. Por eso surgió esta idea, crear un Anti-Cheat lo mas Escalable, Robusto y Adaptable posible sin costo para la comunidad de SNET.



Funcionamiento



KeyMac



Procesos y
dispositivos HID



Acceso al
Sistema



Filtrados por
Whitelist/Blacklist



Firewall



Detectar Procesos sospechosos

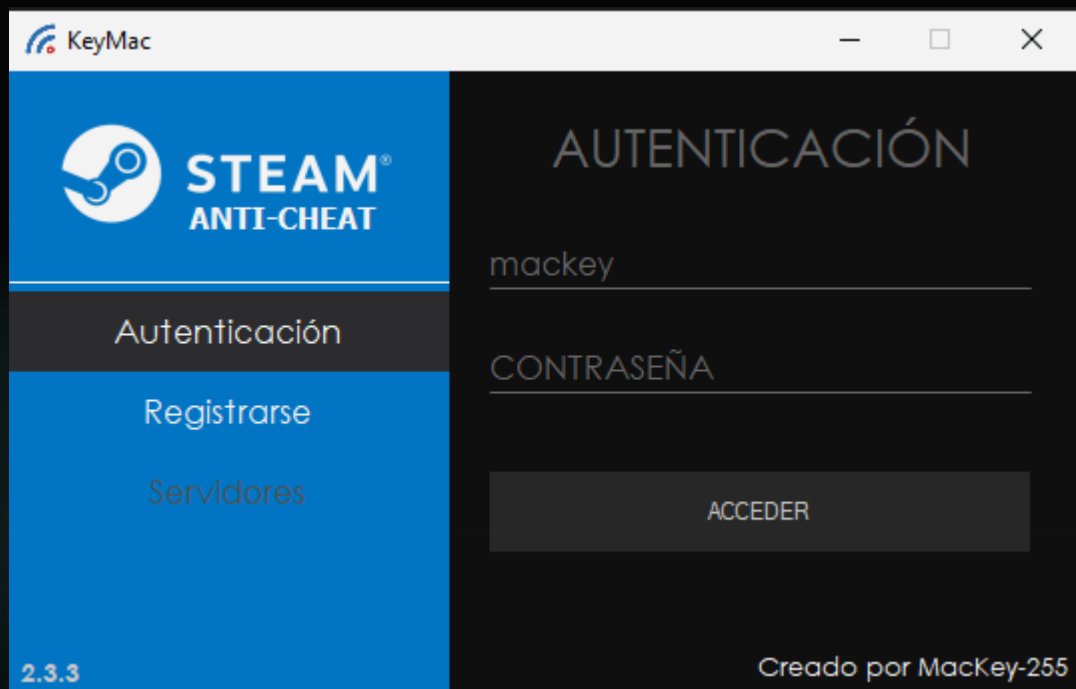


Instalación

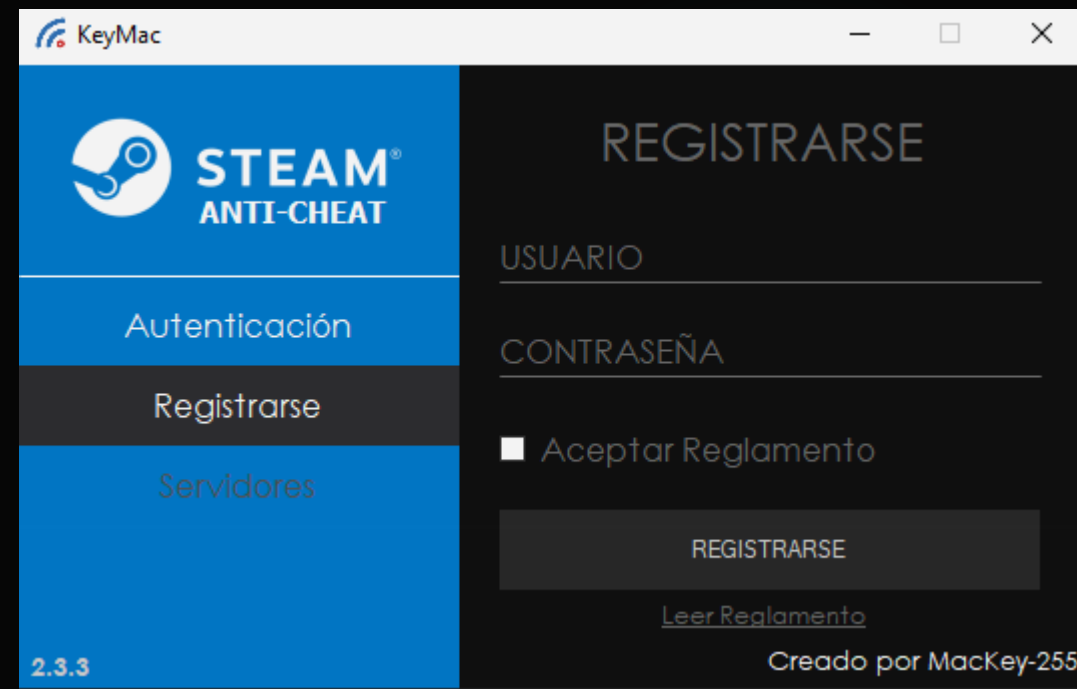
1. Creamos una carpeta con el KeyMac Server dentro.
2. Activamos el Firewall de Windows con las reglas de bloqueo activadas.
3. Abrimos el KeyMac Server y configuramos todo desde el panel.
4. El cliente lo abrimos y lo configuramos con el IP y puerto de nuestro server.
5. Listo!! A disfrutar.



Secciones del Cliente



Autenticación



Registro



Autenticar

- Dado usuario y contraseña el sistema autentica al usuario según el registro. Si esta activada el API utilizara el mismo para autenticar.
- El Cliente se auto autentica cada vez que inicia, una ventaja para que el usuario no este constantemente realizando esta tarea.

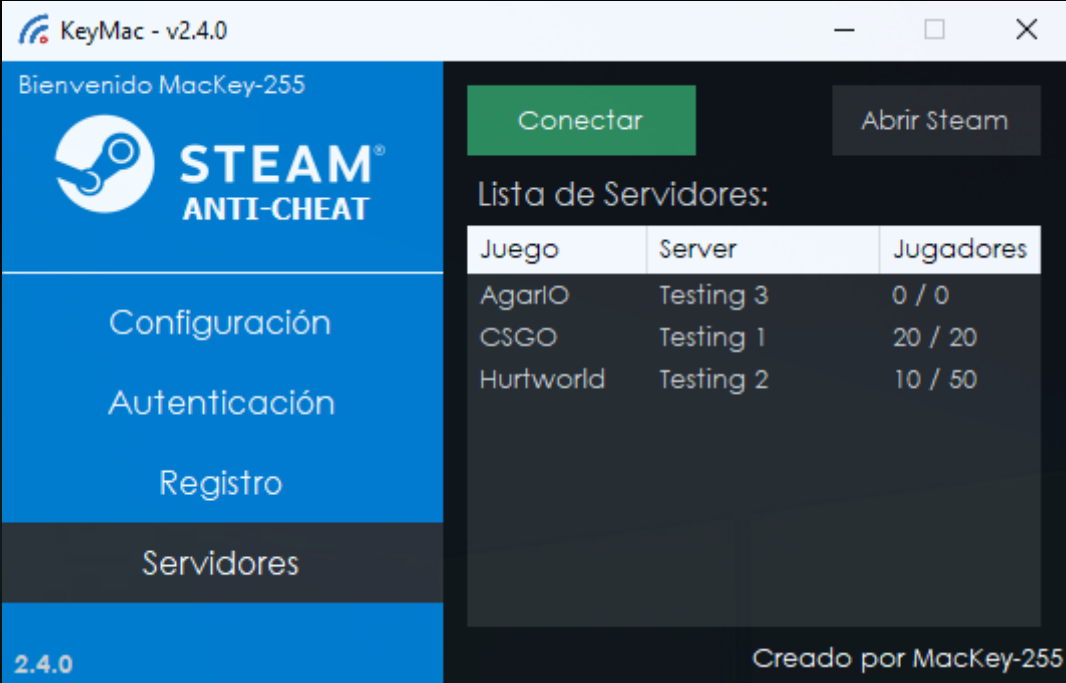


Registro

- El registro esta habilitado por defecto, a menos que sea deshabilitado mediante el API. Si esta integrado con el Steam, hasta que el Steam no reconozca al usuario nuevo no podrá surgir efecto el registro.
- El usuario registrado debe estar en minúscula y la contraseña como mínimo 8 caracteres.



Secciones del Cliente



Lista de Servidores



Configuración



Servidores

- El usuario observará una lista de servidores que están disponibles en el Steam. Si implementan un API pueden agregar otros servidores como Agar.io, Xnova u otros.
- Una vez conectado el usuario, este es agregado al Firewall y tendrá acceso a todos los puertos bloqueados (Puertos de juegos protegidos por el Anti-Cheat).

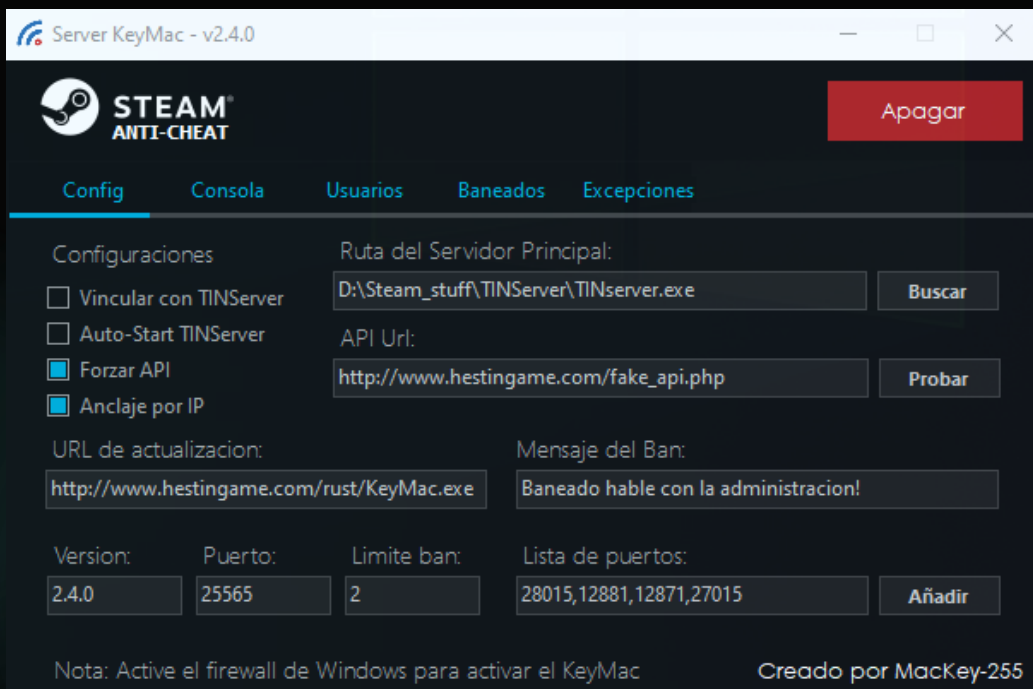


Configuración

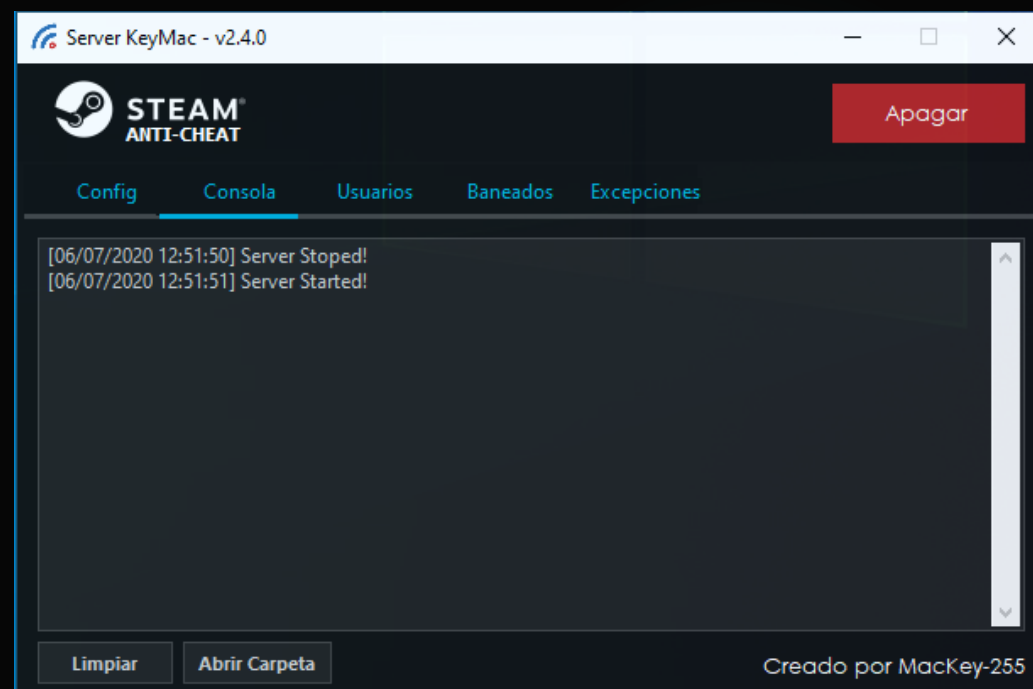
- El usuario puede cambiar el servidor y puerto del Anti-Cheat cuando crea conveniente. Permitiendo utilizar el mismo Cliente para diferentes servidores.
- Esta permitido utilizar IP o URL para acceder a un servidor. El sistema DNS funciona sin conflictos.



Secciones del Servidor



Configuración



Consola de
información

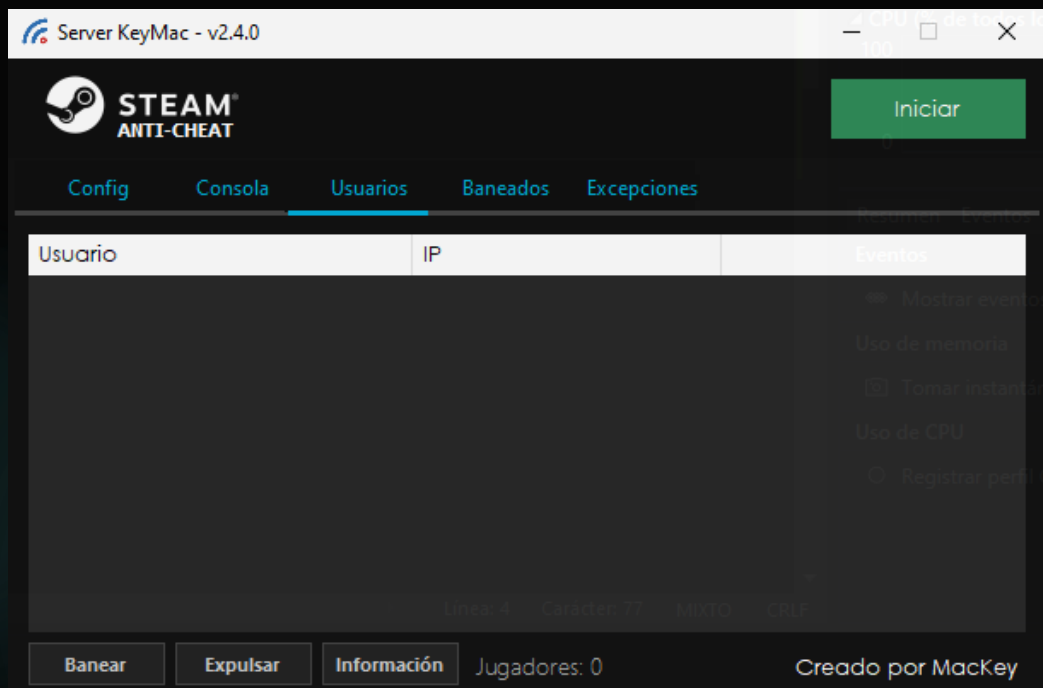


Config y Consola

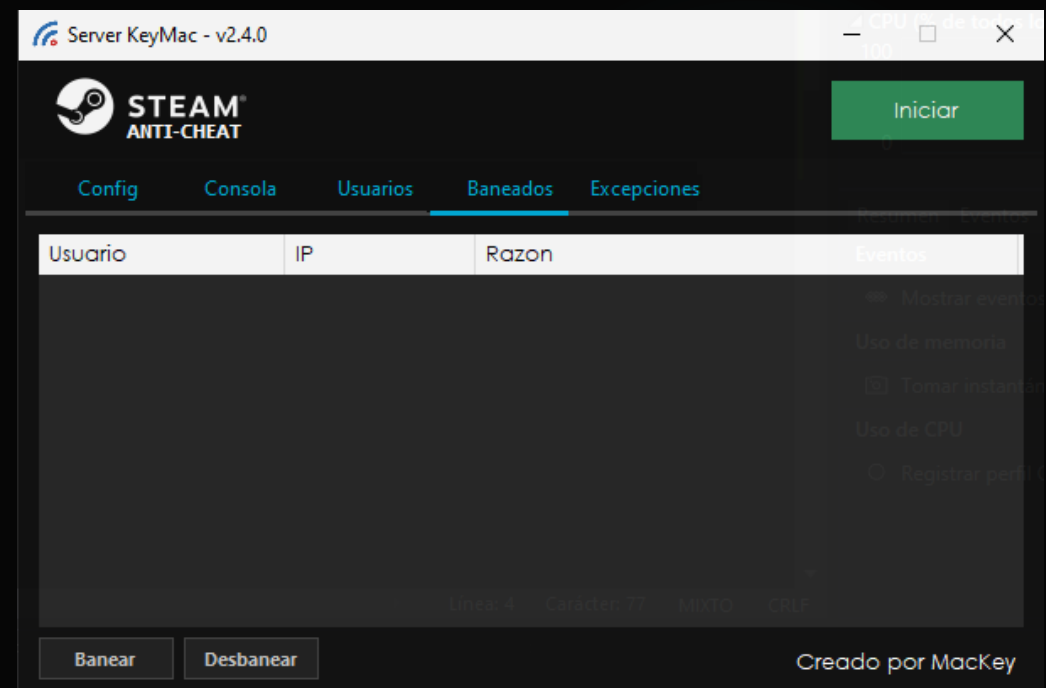
- En las configuraciones esta la integración con el Steam o con el API y la lista de puertos bloqueados por el Anti-Cheat. Además de otras opciones de bastante interés como el Anclaje por IP.
- La consola muestra todo lo que el sistema este haciendo, tanto acciones del usuario como procesos internos del sistema.



Secciones del Servidor



Lista de usuarios
conectados



Lista de usuarios
baneados




Lista de usuarios

- Tenemos la lista de usuarios conectados donde podemos pedirle información sensible (Procesos, programas ejecutados/instalados, dispositivos HID y capturas), expulsarlo o banearlo del sistema.
- La lista de baneados muestra el usuario, el ip y la razón del baneo. Pueden desbanear o banear nuevos usuarios.



Secciones del Servidor

Server KeyMac - v2.4.0

 **STEAM**
ANTI-CHEAT

Iniciar

ConfigConsolaUsuariosBaneadosExcepciones

AgregarProgramsWhitelist

Valor	Descripcion
AChat	First Data Whitelist
AutoKMS	First Data Whitelist
AutoRun Pro Enterprise	First Data Whitelist
BattleNet_Nordrassil	First Data Whitelist
Dukto	First Data Whitelist
EasyAntiCheat	First Data Whitelist
Everything	First Data Whitelist
glDriverquery64	First Data Whitelist

Eliminar

Creado por MacKey

Whitelist/Blacklist

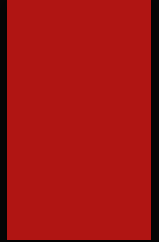


Whitelist/Blacklist

- El corazón del Anti-Cheat, nos permite detectar procesos maliciosos utilizando el detector + blacklist previamente definida.
- Muchos procesos poseen código igual o semejante al de procesos malignos por lo que pueden ser reconocidos como maligno, para ello esta la whitelist que ya viene con algunas excepciones previas.



Whitelist/Blacklist



Los procesos detectados como “Sospechosos” nos saldrá en la consola de esta forma:

```
ProductName | FilePath | FileOriginalName | WindowsTitle | FileDescription | FileVersion |  
CompanyName | FileSize | LastModified | LegalCopyright | Checksum | Detected
```

Tenemos en el Whitelist varios parámetros, agregamos el que encaja y listo. Casi siempre intentamos agregar el CompanyName para asegurar todos los procesos de esa compañía. Si es algo muy específico agregar el Checksum.



¿Qué errores puede haber?





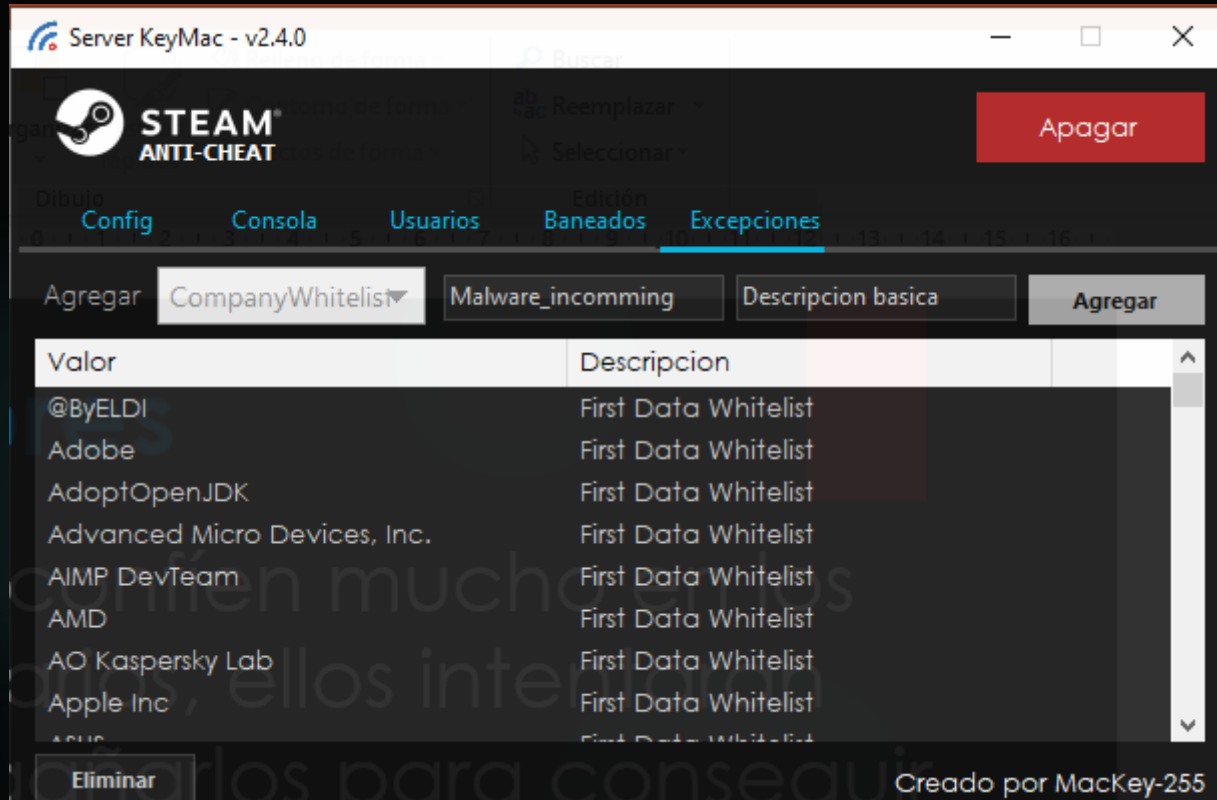
Errores Blacklist

Muchas veces el Anti-Cheat no detecta los procesos maliciosos o los mouses bloody, ya que muchas veces se comete el error de agregar algún mouse/proceso en la Whitelist permitiendo el uso de este, siendo realmente malicioso. Para evitar esto es aconsejable buscar información del mouse/proceso.

[USB ID Database::Vendor ID and Product ID list - the sz development](#)



Errores Whitelist



No confíen mucho en los usuarios, intentaran engañarlos para utilizar Hacks. Revisen que mouses/procesos tienen permitidos en el listado. De esto pende la seguridad de sus servicios.



Errores Vincular Steam

client	30/06/2020 12:59	Carpeta de archivos	
data	02/07/2020 8:33	Carpeta de archivos	
log	30/06/2020 12:01	Carpeta de archivos	
plugins	30/06/2020 12:19	Carpeta de archivos	
tools	30/06/2020 12:43	Carpeta de archivos	
_run_me_first.cmd	19/09/2017 9:55	Script de comand...	1 KB
client.zip	30/06/2020 13:00	Archivo WinRAR Z...	7.469 KB
Readme.txt	23/02/2019 8:51	Archivo TXT	4 KB
TINserver.exe	01/07/2019 11:30	Aplicación	7.575 KB
TINserver.ini	02/07/2020 11:58	Opciones de confi...	4 KB
TINserver.users.db3	02/07/2020 4:59	Archivo DB3	12 KB
TINserver.users.db3-shm	02/07/2020 12:48	Archivo DB3-SHM	32 KB
TINserver.users.db3-wal	02/07/2020 10:48	Archivo DB3-WAL	9 KB
TINserver.users.ini	02/07/2020 11:16	Opciones de confi...	0 KB
TINserverlauncher.exe	30/01/2020 3:36	Aplicación	6.956 KB
updateApplInfo.cmd	17/02/2017 12:31	Script de comand...	1 KB
updateClient.cmd	16/12/2014 3:18	Script de comand...	1 KB

Si posees un TINServer puedes vincularlo con el Anti-Cheat. Debes asegurarte de que la carpeta “data” sea la de configuraciones del Steam y que la base de datos de users sea: TINserver.users.db3



Errores Vincular Steam

ApplInfo	30/06/2020 11:54	Carpeta de archivos	
Certificates	30/06/2020 13:00	Carpeta de archivos	
ClientCrash	02/07/2020 12:28	Carpeta de archivos	
ClientLauncher	30/06/2020 11:54	Carpeta de archivos	
ClientServices	30/06/2020 11:54	Carpeta de archivos	
ClientUpdates	30/06/2020 11:54	Carpeta de archivos	
ConfigServer	15/04/2020 3:16	Carpeta de archivos	
Content	30/06/2020 13:02	Carpeta de archivos	
DrmFileServer	30/06/2020 11:54	Carpeta de archivos	
Emoticons	30/06/2020 12:10	Carpeta de archivos	
EmoticonsLarge	22/04/2020 10:21	Carpeta de archivos	
GamePatches	30/06/2020 12:10	Carpeta de archivos	
GameStats	15/04/2020 3:16	Carpeta de archivos	
Inventory	30/06/2020 11:54	Carpeta de archivos	
Parental	22/04/2020 10:24	Carpeta de archivos	
SteamCloud	30/06/2020 13:05	Carpeta de archivos	
SteamWeb	30/06/2020 11:54	Carpeta de archivos	
ClientLauncher.zip	30/06/2020 13:05	Archivo WinRAR Z...	7.469 KB
loginKeys.blob	02/07/2020 12:28	Archivo BLOB	1 KB
TINserver.cmserver.db3	02/07/2020 4:59	Archivo DB3	252 KB
TINserver.cmserver.db3-shm	02/07/2020 12:48	Archivo DB3-SHM	32 KB
TINserver.cmserver.db3-wal	02/07/2020 12:48	Archivo DB3-WAL	1.027 KB
TINserver.content3server.db3	02/07/2020 12:48	Archivo DB3	2.780 KB
TINserver.content3server.db3-shm	02/07/2020 12:48	Archivo DB3-SHM	32 KB
TINserver.content3server.db3-wal	02/07/2020 12:48	Archivo DB3-WAL	5.657 KB

Asegúrate de que en la carpeta “data” tengas la base de datos llamada:
TINserver.cmserver.db3
Sino puede dar errores durante la ejecución del servidor Anti-Cheat.



Errores Vincular Steam

CEGDownloader	02/07/2020 11:26
ClientUpdateDownloader	30/06/2020 13:14
CreamAPI	30/06/2020 13:28
Dedicated Server List - Help	30/06/2020 12:22
DepotDownloader	22/04/2020 10:48
GameCoordinator	23/04/2020 6:22
PICSdownloader	30/06/2020 12:09
RinGameCoordinator	30/06/2020 12:12
Steam.Content.Packager.v3.0	30/06/2020 13:26
SteamCMD	02/07/2020 9:12
SteamEmu	30/06/2020 12:43
SteamFileEditor	22/04/2020 10:56
steamGuardKeygen	02/07/2020 9:10
Steamless	23/04/2020 3:44
TINcft	02/07/2020 12:33
TINServerClient for Servers	04/07/2020 11:51

Verifica que tengas todas las herramientas del TINServer para poder trabajar cómodamente con él.



Funcionando con TINServer

0 | Testing

7/4/2020 3:50:41 PM [EAC Server] [Info] [Initialize] ServerName: 'Hurtworld.Server' RegisterTimeout: 30.
7/4/2020 3:50:41 PM [EAC Server] [Verbose] [Cerberus] [Initialize] Called.
7/4/2020 3:50:41 PM [EAC Server] [Info] [Cerberus] [RegisterEvent] EventID: 1h EventName: 'game_round_start' Parameters: { map_name (string) }.
7/4/2020 3:50:41 PM [EAC Server] [Info] [Cerberus] [RegisterEvent] EventID: 2h EventName: 'game_round_end' Parameters: { winning_team_id (uint32) }.
Listening on port 12871.
Loading level nullius...
Level load complete. Loaded level `nullius.win64.map` (Build 278 from SDK version 0.2.0.0) in 28.8358413 seconds
Loading localization stuff BaseContentLocalization
Loading localization stuff BaseArtLocalization
Processed 210592 objects and resolved 4085 proxy references in 0.51 seconds.
No game mode found in level, defaulting to survival
Loading server state from file [redacted]/steamCMD/steamapps/common/hurtworld_server/autosave_nullius.hwb
Saved with version 1.0.0.6
World Load Complete: 0 Players, 5 Items, 0 Constructions. Created: 04/01/2020 09:05:29 NextWipe: 04/01/2020 09:05:28
initializing painter grid with 60,0.75
Destroying 5 orphaned items
IP address from Steam query: 192.168.0.188
Server version is: 1.0.0.6
Starting game save to file [redacted]/steamCMD/steamapps/common/hurtworld_server/autosave_nullius.hwb
Weather System Blizzard(Clone) couldn't find a mapping for BlizzardBiome (HurtBiome), adding to grid dictionary
Starting game save to file [redacted]/steamCMD/steamapps/common/hurtworld_server/autosave_nullius.hwb
Starting game save to file [redacted]/steamCMD/steamapps/common/hurtworld_server/autosave_nullius.hwb

Testing 3204fps, 24m09s
0/50 players 0b/s in, 0b/s out
2:20 am, nullius Oxide.Hurtworld 2.0.4084

KeyMac - v2.4.0

Bienvenido mackey

Desconectar

Abrir Steam

Lista de Servidores:

Juego	Server	Jugadores
hurworld	Testing	0 / 50

Creado por MacKey-255

Server KeyMac - v2.4.0

Apagar

Config

Consola

Usuarios

Baneados

Excepciones

[04/07/2020 12:11:04] Loading config ...
[04/07/2020 12:11:04] Loading firewall ...
[04/07/2020 12:11:04] Loading database ...
[04/07/2020 12:11:05] Server Started!
[04/07/2020 12:11:06] USER mackey LOGIN [192.168.0.188 - [redacted]]
[04/07/2020 12:13:36] WHITELIST ADD [192.168.0.188 - [redacted]] DEVICES CONNECTED =>
Genius 4D Scroll Mouse (VID 458, PID 56, version 0.0)
[04/07/2020 12:13:44] SCREENSHOT [192.168.0.188]

Limpiar

Abrir Carpeta

Creado por MacKey-255



Errores de Puertos

En ocasiones introducimos mal los parámetros por lo que puede dar error el sistema. La lista de puertos son los puertos de los servicios/juegos que están protegidos por el Anti-Cheat es importante agregarlos todos y bien.

Lista de puertos:

28015,12881,12871,27015,adasd

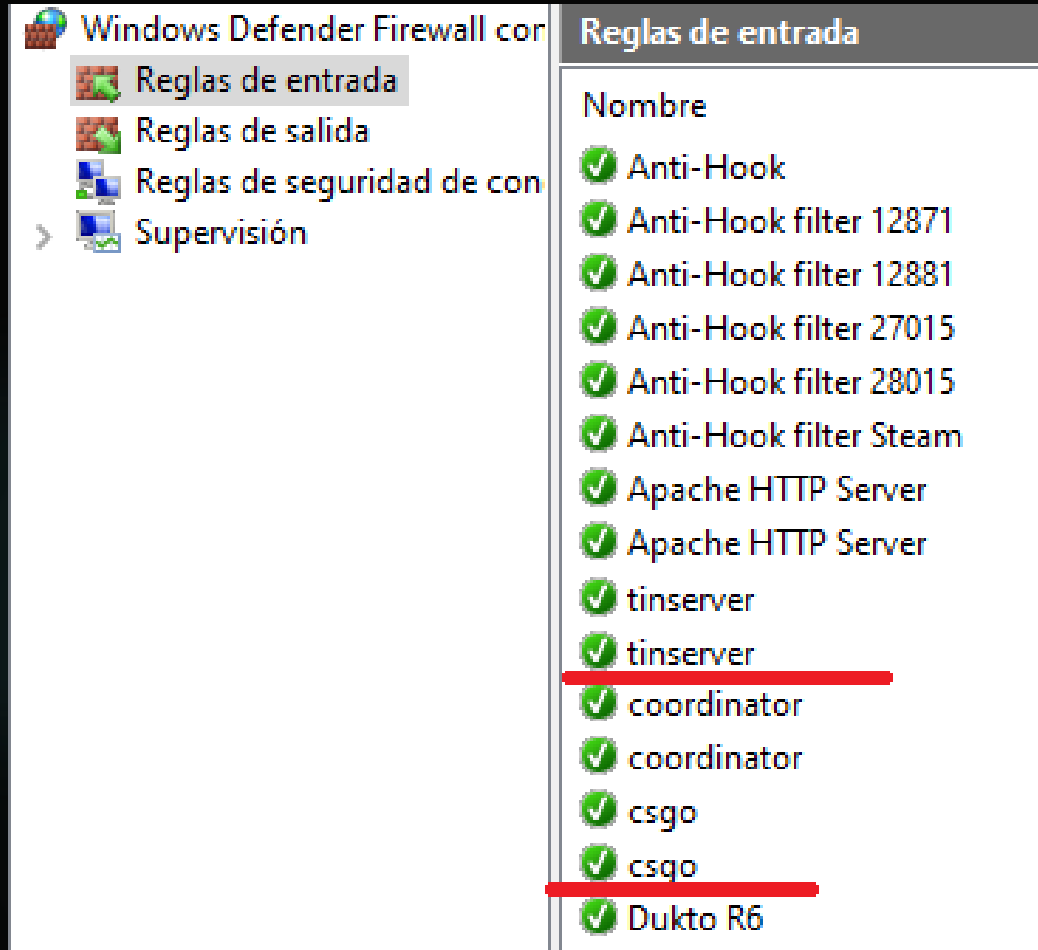
Añadir

ar el KeyMac

Creado por MacKey-255



Errores Firewall



A veces cuando iniciamos un programa, el firewall de Windows lo añade como permitido/denegado, por lo que puede o no acceder sin tener abierto el Anti-Cheat. Comprueben y arreglen este grave fallo.



Errores Firewall

```
L 07/04/2020 - 11:46:08: server_cvar: "mp_freezetime" "12"  
L 07/04/2020 - 11:46:08: server_cvar: "mp_limitteams" "0"  
L 07/04/2020 - 11:46:08: server_cvar: "sv_contact" "0"  
L 07/04/2020 - 11:46:08: server_cvar: "sv  
L 07/04/2020 - 11:46:08: server_cvar: "sv  
L 07/04/2020 - 11:46:08: server_cvar: "sv  
L 07/04/2020 - 11:46:08: server_cvar: "sv
```

```
sv_pure value unchanged (current value is
```

```
-----  
CHostage::Precache: missing hostage model  
PrecacheScriptSound 'Snowball.Bounce' fai  
PrecacheScriptSound 'Survival.VO.Taunt4a'  
PrecacheScriptSound 'balkan_epic_blank' f  
Commentary: Could not find commentary dat  
Error parsing BotProfile.db - unknown att  
Error parsing BotProfile.db - unknown att  
Error parsing BotProfile.db - unknown att  
Error parsing BotProfile.db - unknown att  
Error parsing BotProfile.db - unknown att  
Error parsing BotProfile.db - unknown att  
Error parsing BotProfile.db - unknown att  
Error parsing BotProfile.db - unknown att  
Initializing Steam libraries for secure I  
*****  
* Unable to load Steam support library.  
* This server will operate in LAN mode only.  
*****
```



Alerta de seguridad de Windows



Firewall de Windows Defender bloqueó algunas características de esta aplicación

Firewall de Windows Defender bloqueó algunas características de srcds.exe en todas las redes públicas y privadas.



Nombre: srcds.exe
Editor: Desconocido
Ruta de acceso: D:\steam_stuff\steamcmd\steamapps\common\csgo_server\srcds.exe

Permitir que srcds.exe se comuniquen en estas redes:

- ☐ Redes privadas, como las domésticas o del trabajo
- ☒ Redes públicas, como las de aeropuertos y cafeterías (no se recomienda porque estas redes públicas suelen tener poca seguridad o carecer de ella)

[¿Cuál es el riesgo de permitir que una aplicación pase a través de un firewall?](#)



Permitir acceso

Cancelar



Errores Firewall



Lo arreglamos desde el panel de control: Firewall > Cambiar la config. de notificaciones.

Deshabilitando las notificaciones del firewall de nuevas aplicaciones. Y eliminando las reglas de entrada de los servicios.



Errores de Consola

A veces interpretamos mal los datos de la consola y vemos un programa como malicioso cuando no lo es. Podemos agregarlo si tenemos prueba de que no lo es. El orden del proceso es:

ProductName | FilePath | FileOriginalName | WindowsTitle | FileDescription | FileVersion |
CompanyName | FileSize | LastModified | LegalCopyright | Checksum | Detected

```
[06/07/2020 13:07:09] Server Started!  
[06/07/2020 13:07:09] BANNED TRY CONNECT [192.168.0.188] KICKED!  
[06/07/2020 13:07:33] USER mackey LOGIN [192.168.0.188 - 1C:1B:0D:61:ED:CB]  
[06/07/2020 13:07:42] USER WARNING [192.168.0.188] => GitKraken|C:\Users\MacKey\AppData\Local  
\gitkraken\app-6.1.3\gitkraken.exe|GitKraken.exe|GitKraken|6.1.3|Axosoft, LLC|Copyright (C) Axosoft,  
LLC|5e45d6d47ffdc7bd198b9dee76064b2e|Injector
```




Errores de Conexión

Es necesario tener una buena conexión con el servidor de Anti-Cheat ya que este consume mucha red. Debido al constante envío de imágenes al servidor y el volumen de conexiones. Puedes ver en las opciones del servidor si desea enviar constantemente imágenes (Para servicios pequeños) o deshabilitar esta función. Cuando revisas a un usuarios sospechoso igual te enviará la imagen.



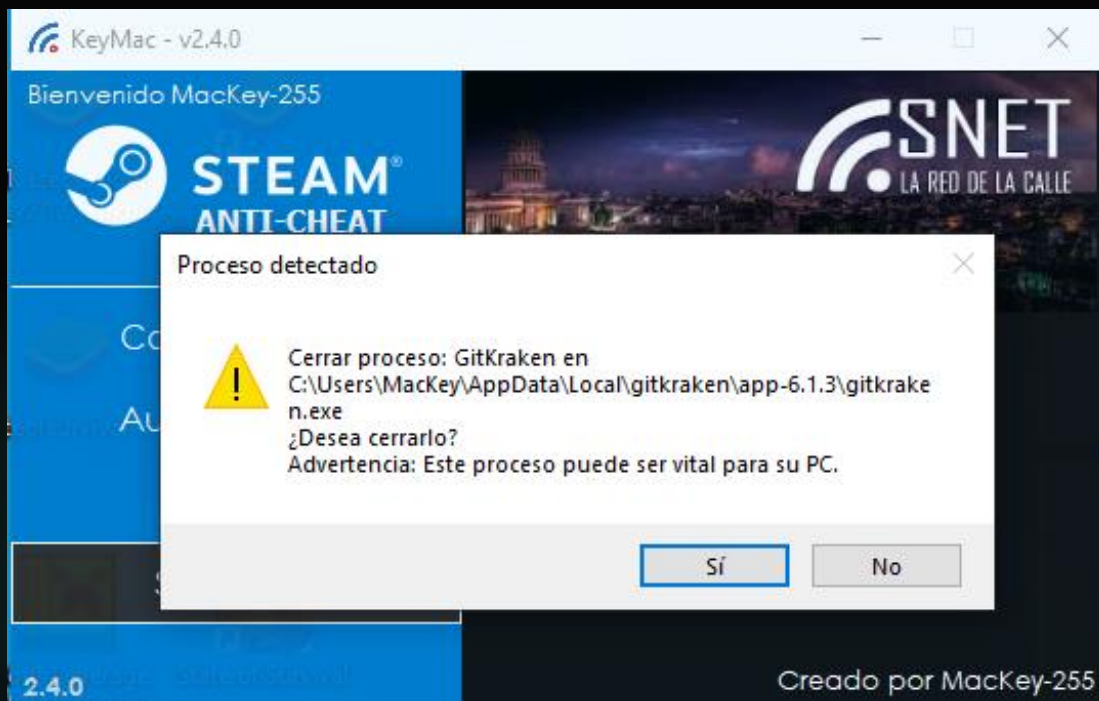
Errores Inesperados

A veces el Anticheat no esta totalmente testeado y puede conllevar a varios errores que serán almacenados en una carpeta llamada errors. Súbelos como un Issues en Github para darle solución, o puedes contactarme directamente vía TeamSpeak. En el próximo release estará arreglado.

Nombre	Fecha de modificación	Tipo	Tamaño
 error_07_09_2020	08/08/2020 16:30	Archivo TXT	2 KB



Errores inconscientes



Obliga a los usuarios a cerrar todos los programas que realmente no necesitan tener abiertos para disfrutar del servicio. Así tendrás menos problemas tú como el usuario.



Conclusiones

Este Anti-Cheat te ayudará a mantener a los “Parcheros” a raya, el resto esta en tus manos, estar todo el tiempo revisando y monitoreando a los usuarios. Es tediosa pero peor es tener un servicio lleno de jugadores tramposos y que el resto dejen de consumir tú servicio por ello. Yo soy MacKey-255 y te deseo suerte 😊

Dudas o sugerencias por correo: <https://github.com/MacKey-255>



ForuénClub



SNET

LA RED DE LA CALLE

KeyMac

Anti-Cheat Steam para la Comunidad de SNET

