

Guía Básica de Screenshare (SS) para Detección de Cheats en Minecraft

Introducción

El Screenshare (SS) es un proceso de revisión directa en el sistema de un jugador, destinado a identificar programas o configuraciones que proporcionan ventajas desleales en juegos en línea, como hacks o cheats. Comúnmente utilizado en entornos de Minecraft, el SS busca detectar archivos o comportamientos que sugieran el uso de programas externos o modificaciones que den ventajas injustas en el juego.

La revisión mediante SS permite un análisis en tiempo real del sistema, garantizando que los jugadores cumplan con las reglas y ofreciendo una experiencia de juego justa para todos.

Indicadores de Baneo Inmediato

Durante un SS, ciertos indicios resultan en baneo automático, ya que representan intentos directos de ocultar o interferir con la revisión. Entre ellos se encuentran:

- **Uso de grabadores o software de captura de pantalla:** Grabar o compartir la pantalla mientras se realiza una SS está estrictamente prohibido, ya que puede utilizarse para ocultar actividad o procesos sospechosos.
- **Archivos eliminados o modificados:** Alterar o eliminar archivos durante el proceso de SS es un intento claro de interferencia y será motivo de baneo.
- **Detención de Servicios del Sistema:** Algunos servicios deben permanecer activos durante la SS. Detener servicios críticos como `dps`, `dusmsvc` o `BITS` indica que el usuario está tratando de ocultar procesos maliciosos o sospechosos.
- **Cierre del Launcher de Minecraft:** Interrumpir el launcher durante el SS impide revisar ciertos datos importantes y resulta en baneo inmediato.
- **Reinicio de ProcessHacker:** ProcessHacker es una herramienta avanzada de monitoreo de procesos. Si ha sido reiniciada o manipulada durante el SS, el usuario será baneado automáticamente.

Conceptos Clave en el Screenshare (SS)

Cheats Internos: Estos hacks o cheats se alojan dentro de la carpeta de instalación de Minecraft (`.minecraft`) y pueden ser detectados revisando el contenido de esta carpeta.

Cheats Externos: Son hacks o cheats que se ejecutan fuera del directorio de Minecraft. Pueden estar ubicados en cualquier otra parte del sistema, por lo que su detección puede requerir un análisis exhaustivo de los procesos activos y del historial de actividad.

USN Journal: El USN (Update Sequence Number) Journal es un registro detallado de cambios en el sistema de archivos NTFS, útil para rastrear modificaciones, creaciones o eliminaciones de archivos.

Prefetch: La carpeta Prefetch de Windows almacena registros de los ejecutables que han sido abiertos recientemente, permitiendo verificar actividad sospechosa y rastrear archivos ejecutables utilizados en las últimas horas.

Herramientas Esenciales para el Screenshare

- ProcessHacker: Monitorea los procesos activos en el sistema en detalle. Es útil para identificar procesos ocultos, inusuales o que interactúan de forma sospechosa con el sistema.
- ShellBags: Permite visualizar el historial de carpetas a las que el usuario ha accedido, detectando ubicaciones sospechosas o fuera de lo común.
- WinPrefetch: Similar al Prefetch de Windows, con funciones avanzadas para búsqueda y organización de registros de ejecutables, ayudando a identificar aplicaciones que se han ejecutado recientemente.
- MyLastActivityView: Muestra una línea de tiempo de la actividad reciente del usuario, lo cual es útil para rastrear acciones, accesos y ejecuciones de archivos o programas.
- Luyten: Herramienta para descompilar archivos `.jar`, utilizada para verificar el código y la estructura interna de archivos en Minecraft y detectar modificaciones o cheats internos.

Proceso Completo de Screenshare (SS)

Verificación Inicial de la Versión de Minecraft

Identificación de la Versión:

- Verifica la versión en el cliente de Minecraft con `F3`.
- Si el usuario está utilizando una versión con Forge, se debe revisar la carpeta `.minecraft` para buscar cheats internos.
- Si está utilizando Vanilla u otro cliente sin Forge, se procede a buscar cheats externos en otros lugares del sistema.

Análisis Detallado en ProcessHacker

Verificación de Reinicio: En `explorer.exe`, selecciona `Properties` > `General` y confirma la hora de inicio. Si se observa que el proceso se ha reiniciado después del inicio de la SS, esto justifica un baneo inmediato.

Análisis de Memoria: En `explorer.exe`, accede a `Memory` > `Options` > `Strings` y usa la siguiente configuración:

- Longitud mínima (Minimum Length): 5
- Activa las opciones Private, Detect Unicode, Extend Unicode y Mapped

Realiza una búsqueda de cadenas sospechosas (strings), como "AutoClicker", "file:\\", o "c:\\users\\". La presencia de términos relacionados con cheats no garantiza un baneo inmediato, pero indica que se necesita un análisis más profundo.

Herramientas Adicionales para Inspección

- ShellBags: Verifica el historial de carpetas a las que el usuario ha accedido, permitiendo rastrear ubicaciones sospechosas que el jugador pudo haber explorado.
- WinPrefetch: Revisa los registros de ejecutables para detectar actividad reciente que indique la ejecución de cheats externos.
- MyLastActivityView: Proporciona una cronología detallada de las acciones recientes del usuario, incluyendo archivos abiertos, programas ejecutados y otros eventos.
- Luyten: Permite la descompilación de archivos `.jar`, facilitando el análisis del contenido y código interno de los mods en Minecraft.

Consejos para una SS Completa y Efectiva

- Registro Detallado de Hallazgos: Documenta cada paso y hallazgo sospechoso para mantener un registro completo y transparente.
- Mantén el Entorno Controlado: Asegúrate de que el usuario no cierre aplicaciones ni manipule el sistema mientras se realiza la SS.
- Mantén las Herramientas Actualizadas: Utiliza versiones recientes de las herramientas para garantizar una detección precisa y eficaz de cheats y modificaciones.

Conclusión

Esta guía de Screenshare (SS) es una base para detectar cheats y asegurar una experiencia de juego justa en entornos de Minecraft. Aplicando estas prácticas, los servidores pueden mantener la integridad de sus comunidades, garantizando que todos los jugadores compitan en igualdad de condiciones.