Guida controlli multi-account

Una guida sui controlli multiaccount, da Bestemmie per voi

Premessa

Questa guida è pensata solo per i sistemi Windows. Inoltre il journal è disponibile da Windows 10 in su. Su altri sistemi operativi le cose potrebbero essere organizzate in modo diverso e funzionare in modo differente da quello spiegato qua. Nel caso incontraste un utente con macOS o linux, vi consiglio di fare riferimento ad uno staff ss verified.

Introduzione

I controlli multi-account mirano a verificare che un utente stia utilizzando altri account per: evadere una sanzione, boosting, etc… In questa guida imparerete passo passo alcune tecniche base per fare i controlli multiaccount, che sono necessarie per procedere.

Primo step | tipo di client

Bisogna controllare quale tipologia di client il player sta utilizzando. Alcuni client facili da riconoscere e molto utilizzati sono i seguenti:

- Minecraft default
- Forge
- Fabric
- Badlion client
- Lunar client
- Feather client
- Salwyrr client
- etc…

Per renderci la vita facile, suddividiamo i client in due grandi categorie:

- Client vanilla
- Lunar client

Il lunar client è l'unico client che ha un modo differente per trovare le informazioni che noi desideriamo cercare, almeno questo è l'unico di cui siamo a conoscenza al momento. Detto questo possiamo procedere.

Secondo step | controllare i logs di sessione

Ogni volta che utilizziamo minecraft, il gioco salva in un file con estensione “.log”, tutte le informazioni riguardo allo stato del gioco nel tempo, una copia della chat e altre informazioni. Il file dell’ultima sessione viene nominato “latest.log” mentre gli altri vengono marcati con la data e compressi in una cartella compressa di tipo tarball (.tar.gz). Per analizzare tutti questi file in modo efficiente e funzionale, procediamo nel seguente modo:

Secondo step | metodo per i Client vanilla

1. Aprire la cartella seguendo questi step: *dentro il gioco* > ESC > Opzioni > Pacchetti risorse > Apri cartella pacchetti risorse (Option > Resource packs > Open pack folder);

2. Andare indietro di una cartella (cartella parente), e ci troviamo all’interno della cartella radice del gioco di minecraft;

3. Andate successivamente nella cartella logs ed aprirla con WinRAR;

4. Filtrare tutti i logs (estensione .tar.gz + il latest.log) e usare il cerca (find) su WinRAR per filtrare con la seguente parola chiave: "setting user:";

5. Se la cartella di minecraft ha come parente della cartella parente una cartella di nome instances, allora entrare dentro instances e procedere ad entrare su ogni cartella e la cartella “.minecraft” di ognuna, per poi ripetere dallo step 3 per ognuna di esse.

Secondo step | metodo per il Lunar client

1. "ESC" > Disconnetti > Esci > e si controlla la lista degli account passando con il mouse sopra l'iconcina dell'account in alto a sinistra

2. Nel caso sembri apparentemente pulito cercare il lunar client, poi aprire la sezione “about” e la cartella “logs”, andare indietro nella cartella parente di nome ".lunarclient" e aprire la cartella offline > multiver

3. Andare successivamente nella cartella logs e aprirla all'interno di winrar

4. Filtrare tutti i logs (estensione .tar.gz + il latest.log) e usare il cerca (find) su winrar per filtrare con la seguente parola chiave: "[LC Accounts] Loaded content for"

Terzo step | macchine virtuali

L'utilizzo delle macchine virtuali è sanzionabile come se si stesse utilizzando un cheat. Detto ciò, una domanda sorge spontanea: "Come riconosco una macchina virtuale?".

Le macchine virtuali si possono riconoscere tramite semplici controlli, come il nome di dispositivi (es. L'harddisk o il storage device utilizzato dal sistema). Possiamo trovare queste informazioni su gestione dispositivi (da pannello di controllo > sistema e sicurezza > strumenti di windows > gestione computer > gestione dispositivi || cerchi gestione dispositivi su windows search). Se all'interno del nome parole come VM, virtual harddisk e cose che vagamente fanno riferimento a macchine virtuali, bisogna controllare. Molte macchine virtuali hanno dei pacchetti di integrazione con il sistema, quindi individuare nella sezione dell'esplora file, possibili cd drive con nomi tipo: "VirtualBox extensions pack" o "Vmware drivers" o cose simili. Consiglio di provare in prima persona la creazione di macchine virtuali per trovare tutti i modi veloci per provare il loro utilizzo ed eventualmente conoscere più a fondo l'argomento.

Quarto step | journal

Quando un file viene eliminato, modificato, rinominato, etc.... il sistema ne tiene traccia, tramite una serie di meccanismi, tra cui ritroviamo l'USNJournal. Questo contiene ogni singolo cambiamento al filesystem (il nostro disco), con tanto di informazioni su cosa è stato fatto, dove l'azione ha avuto luogo e quali file ha interessato.

Per accedere alle informazioni del journal dobbiamo:

1. Avviare il prompt dei comandi come AMMINISTRATORE

2. utilizzare il tool fsutil.

Quarto step | funzionamento del comando fsutil

La composizione del comando generico per leggere il journal è il seguente:

$ fsutil usn readjournal c: csv | .....

- usn → utilizziamo il toolkit fornito per la sezione USN (fondamentale);

- readjournal → come indica lo stesso, serve a leggere le informazioni contenute nel journal di un particolare disco;

- c: → il disco che dobbiamo analizzare. Esso deve essere formattato come ntfs per essere leggibile da questo tool, quindi chiavette con fat32/16 non funzioneranno, e se contengono informazioni che servirebbero a provare che il player non è legit, allora va bannato perchè utilizza dispositivi non consentiti. Generalmente si controlla il disco c:, ma se vogliamo controllare qualsiasi altra cosa, mettiamo la lettera del drive associata;

- csv →il formato in cui le informazioni vengono gestite. (si usa generalmente questo, consigliato non modificarlo);

- | → tutti i risultati verranno mandati come input al prossimo comando che vedremo. se invece si vuole visualizzare tutto il journal così, magari per controllarne semplicemente la sua integrità, si toglie il | e si preme invio senza aggiungere altro.

Quarto step | funzionamento del comando findstr

Dopo il pipe ("|"), il comando in questione è “findstr”, che serve per filtrare l'input secondo regole che gli diamo. Esempio di comando.

- primo esempio: $ fsutil usn readjournal c: csv | findstr /i /C:"Eliminazione"

Possiamo spezzare il comando aggiunto in due parti:

- /i → indica che vogliamo filtrare
- /c:"filtro" → è l'effettivo filtro che vogliamo usare, che è contenuto nelle virgolette

Questo comando quà sopra filtra ogni record dove è avvenuta un eliminazione.

- secondo esempio: $ fsutil usn readjournal c: csv | findstr /i /C:"0x00008000" | findstr /i /R /C:".exe"

In questo secondo esempio, notiamo che filtriamo per una particolare stringa (0x00008000) e successivamente l'output di quel comando lo passiamo ad un altro filtro, che cerca tutti i ".exe", ma con una peculiarità.

- /R → serve per rendere il filtro case-sensitive, ovvero deve matchare oltre che le lettere, il fatto di essere o meno maiuscole o minuscole.

Conclusione

Dopo la lettura intera di questa guida e forse una parlata con qualche staff ss verified, allora potrete iniziare a fare controlli assistiti. Buona fortuna a tutti voi.

- *Bestemmie*