Introduzione ai controlli

Introduzione alla guida dei controlli – stilata da bestemmie, 22/02/2023 – 07/06/2023

Un caldo benvenuto da parte mia e da tutta la community SS a chiunque tu sia, che hai deciso di leggere questa guida. Prima di iniziare ci tengo a precisare due cose:

- Questa guida è stata pensata per essere completa, non per forza semplice o intuitiva. Pur coprendo la maggior parte degli aspetti dei controlli e alcuni dello studio dell'informatica forense, questa non è una guida che favorisce chiunque. Se si decide di leggere questa guida bisogna avere una mente libera da ogni preconcetto sentito sui controlli, oltre ad essere aperta all'imparare nuove cose, ad accettare nuovi concetti ma saper usare anche lo spirito critico e valutare anche degli eventuali errori, perché si, pur essendo questa opera di dimensioni mai viste e grandi attenzioni e cure sono state portate alla stesura di questo testo (eccetto l'italiano corretto maybe ._.), non tutte le nozioni fornite possono essere precise. Io sono aperto a commenti costruttivi sulla guida etc.., li potete dare tutti sulla sezione del gruppo FearGames | SS Chat, o li comunicate agli scrittori (per ora solo io, @bestemmies).
- Questa guida è stata scritta interamente dal sottoscritto (aka Bestemmie), ogni nozione fornita qua è puramente scritta in da me e solo da me, non significa che le cose imparate le ho inventate io, ci mancherebbe, ma sicuramente non sono stati altri a scriverle così, men che meno a insegnarle in questo modo. É una carta destinata al pubblico e deve essere, di conseguenza, di pubblico dominio. Ogni cosa presa da qua può essere reinterpretata e riutilizzata, affinché ci siano almeno crediti all'autore. Non è vietato copiare / prendere ispirazione, ma per favore come impegno comune .. siate onesti con me, con gli altri e con voi stessi.

Detto questo, Buona lettura …..

Controllo, definizione ed overview generale

Il controllo hack, anche conosciuto come screenshare in inglese, è una pratica che gli staffer utilizzano per dimostrare che un player sta utilizzando o meno dei cheats. Per avere un minimo di knowledge base su alcuni termini dei controlli partirei proprio da uno dei punti dolenti: il bypass. La definizione comune di bypass è la seguente: "Il bypass avviene quando lo staffer non riesce a trovare i cheats ad un player, nonostante lui li stava utilizzando. Questa è una cosa molto generica e secondo me è soltanto fonte di dibattito inutile. Come prima cosa, molte persone hanno diversi significati di "trovare i cheats", ma io penso che non esista una cosa generica come trovare i cheats. Intanto ci possono essere due tipi di server, i server che bannano per possesso e quelli che non lo fanno. Se parliamo di server che bannano per il possesso, trovare un cheat si limita a trovare delle tracce dell'esistenza di un cheat qualsiasi in un arco di tempo stabilito dal regolamento. Non ci si dovrebbe preoccupare più di tanto degli orari di esecuzione etc.. più che altro perché sono le prove dell'esistenza dei cheat in primo luogo a contare nella prova per il ban. Pochi server però decidono di bannare ancora con questi criteri, e qui entriamo nella categoria principale per la maggior parte di voi: La dimostrazione dell'esecuzione. Essendo questa una introduzione non mi soffermerò su tutti i modi di dimostrare l'esecuzione di un programma (chiaramente), bensì ci terrò a precisare due cose in croce. Bisogna in questi casi, avere prove che un cheat (.exe, .jar, .py, etc ...) o una libreria

(.dll e così via), sia stato eseguito e non solo. Bisogna avere un timestamp se si vuole essere precisi, perché un cheat eseguito può essere considerato in due modi: fuori istanza e dentro. Per istanza si intende il processo di minecraft attuale, quindi bisogna confrontare l'esecuzione del cheat, con il timestamp di avvio del processo di minecraft. Ban fatti in altro modo sarebbero imprecisi e/o senza abbastanza prove. Tutto dipende, alla fine della giornata, dalle regole del server, ma è necessario in primo luogo, avere una conoscenza base delle casistiche in cui si banna e in cui no. Detto questo per ricollegarci al concetto dei bypass, un ban è valido finché rispetta le regole del server, non quelle inventate dalla "community". Questo lo specifico perché nel tempo si sono avuti molti episodi di flame altamente inutile tra staffer e bypasser, che si linciano perché uno che ha bypassato e che è stato "false bannato" mentre il povero staff cerca di fare il possibile per difendersi. Assumendo che lo staffer in questione abbia seguito alla lettera il suo regolamento e le prove che ha fornito sono necessarie, un bypasser non ha motivo neanche di parlare, se non per spawnare flame a random, ma una cosa è sicura, lo staffer in questione non è stato bypassato. Altra casistica invece, quando lo staffer non trova niente, il bypasser dice di aver usato un "client privato" e lo staffer si sente come giustificato a non aver trovato niente. Non funziona così, nelle varie tecniche per fare controlli ci sono infiniti metodi per dimostrare che un artefatto sia effettivamente un cheat, quindi lo staffer non è giustificato se il bypasser ha usato un "client privato". Come ultima cosa, farsi bypassare succede, va bene ogni tanto il flame da npc, ma alla fine sono solo esperienze costruttive, che ti insegnano cosa hai sbagliato, e quindi indicano cosa dovrai fare in un altro modo. Gli staffer non dovrebbero bannare per paura di essere bypassati, ne avere questa paura a prescindere. Si praticano i controlli per eliminare i cheater, non per costruire una reputazione. Alla fine tanto è solo un gioco.

Tool vari

I controlli non si fanno di certo evocando demoni pagani o leggendo nella mente del player, dei tool vengono utilizzati per praticare lo screenshare e quindi voglio fare anche qui un po' di chiarezza per chi è nuovo. I tool li possiamo dividere in 3 categorie (2 principali, una di queste sarebbe una sottocategoria, ma fa lo stesso):

- Tool per la condivisione schermo
- Tool per la ricerca di cheats:
    - Tool automatici
    - Tool manuali

Partendo dalla prima, i tool per la condivisione schermo penso siano i più ovvi; in questa categoria fanno parte programmi come Anydesk, Teamviewer e anche discord a volte. É preferibile che uno staffer abbia la possibilità di utilizzare mouse e tastiera del pc appartenente al player, quindi l'utilizzo di anydesk o teamviewer dovrebbe essere un must. In alcune casistiche si può usare discord ma è rara come occasione nonché comunque molto inefficace.
I tool per la ricerca dei cheats, sono tutti quei programmi e command line utilities (programmi per riga di comando), che utilizziamo per effettivamente dimostrare che il player è in possesso ed eventualmente utilizzo di cheats. Ci sono i tool manuali, che ci permettono di visualizzare una vasta gamma di artefatti più o meno tradotti in campi che possiamo capire e quindi interpretare. Manuali quindi perché richiedono la nostra interpretazione. Ci sono poi i tool automatici per controlli, come

echo, avenge, ssdetector e tanti altri, che controllano automaticamente vari artefatti, e confrontano le prove con i loro metodi per verificare se un player ha utilizzato cheats. Questi tool sono tanto affidabili quanto non. É sempre meglio avere una conoscenza avanzata dei controlli prima di affidarsi a ss tools automatici, dato che si rendono veloce il controllo di tanto, ma allo stesso tempo bisogna stare attenti nei casi in cui non segnala niente, o segnala un cheat che sembra strano o non coincide con le condizioni del player in quel momento. Ci sono tante cose da prendere in considerazione perciò sconsiglio l'uso dei tool automatici ai principianti.

Il viaggio è appena iniziato

Nelle successive guide troverete più nello specifico gli argomenti, spiegati per bene e in modo sopratutto completo. Vi auguro un buon proseguimento e mi raccomando rimanete aggiornati e curiosi.