Minecraft

Guida approfondita su cos'è minecraft dal punto di vista dei controlli

É giusto pensare ai controlli cheats come una branca dell'informatica forense, ma a differenza delle materie come DFIR e indagini varie, i controlli cheats sono legati molto anche al gioco che li ospita in primo luogo. Ecco perché qui vi spiego minecraft da un punto di vista di controlli, insieme ai vari tipi di cheats che ci possiamo aspettare e così via.

Il gioco e Java

Come ben sappiamo, minecraft è scritto in java, questo implica che come processo non esisterà mai un ipotetico "minecraft.exe" o robe del genere, bensì minecraft sarà una semplice task all'interno di un processo della Java Virtual Machine (java.exe o javaw.exe). Il gioco, non essendo appunto scritto in un linguaggio direttamente compilato (c/c++/c#/rust etc..), viene avviato tramite dei launcher. I launcher si occupano semplicemente di tenere un loro log delle attività, di offri alcune peculiarità rispetto a quello default e infine, la cosa più ovvia, scopo stesso dei launcher, è il fatto che hanno il comando loro per avviare il gioco (una java-jar con tanti argomenti in poche parole). I launcher dicono a minecraft anche dove ha la sua cartella radice. Per essere più precisi, minecraft, come tutti i giochi, non ha tutte le informazioni come texture e assets vari all'interno dell'eseguibile, bensì si appoggiano su una cartella radice, con all'interno un sistema di cartelle che ordina i vari file e risorse di cui necessita il gioco. La cartella di minecraft, con l'installazione più vanilla che si può avere, si trova in "C:\Users\{username}\AppData\roaming\.minecraft". Questo non significa che si può trovare esclusivamente li. Un esempio può essere MultiMC, un launcher usato da modders e player tecnici di minecraft, che ha come peculiarità quella che ogni versione di minecraft creata, crea una cartella di minecraft separata dalle altre e unica per quella versione, cosa molto comoda per i modders e tenere ordinate tutti i loro mod pack vari, ma ci indica come sia possibile che la cartella radice di minecraft si trovi in un posto diverso dalla posizione vanilla. Per accedere alla cartella di minecraft giusta, si consiglia di andare sul gioco > impostazioni > pacchetti risorse (resource packs) > apri cartella pacchetti risorse. Questa cosa aprirà la cartella resource packs sul disco, che ha come cartella parente, la cartella radice di minecraft.

I tipi cheats

I cheater con minecraft hanno a disposizione forse una tra le più vaste gamme di cheat rispetto a qualsiasi altro gioco, questo tutto per alcune peculiarità del gioco (foreshadowing: java). Prima di partire a scheggia su come trovare i cheats etc.., direi che è meglio avere una base teorica su cosa ci dobbiamo aspettare, cosa dobbiamo trovare in quanto staffer, sul pc del player. I client si dividono in quattro categorie principali, che poi analizzeremo per bene:

- Ghost clients
- Injection clients
- External clients
- Autoclickers

Ora i prossimi paragrafi saranno dedicati esclusivamente alla spiegazione nel dettaglio di questi client e di alcune cose fondamentali da sapere, non che metodi vari.

Ghost clients

I ghost clients, sono forse i client più semplici da trovare, per la quantità di prove che lasciano alla loro esecuzione, ma anche i più sottovalutati. Per definizione i ghost client possono essere delle versioni, delle mod o delle librerie, che vanno a modificare il gioco in modo che il player ha dei vantaggi sleali. Sono delle versioni perché molti tra i ghost client più famosi, sono delle vere e proprie versioni di minecraft che si scaricano e si mettono nella cartella minecraft/version, e si avvia quella specifica versione. Possono essere delle mod, perché tramite le mod noi possiamo implementare delle feature malevole nel gioco, senza andare ad intaccare però la versione originale del gioco. Possono infine essere delle librerie di minecraft, questa è una cosa meno vista in giro, solo un client particolarmente famoso usava questa tecnica, la Serenity. Le librerie sono tutti quei file esterni che contengono codice fondamentale per permettere a minecraft di essere eseguito. Se siete proprio bravi, avete notato un pattern particolare tra questi tipi di ghost clients, il loro obbiettivo è eseguire codice direttamente all'interno di minecraft, che poi sia tramite versione o tramite mod o tramite libreria conta poco, quello che conta è che il loro scopo è modificare il codice del gioco, dall'interno, sfruttando punti di accesso di minecraft, quali la possibilità di avere mods, librerie personalizzate o client custom. Una proprietà fondamentale di questi client, è che per la loro natura, non si possono trovare fuori dalla cartella radice di minecraft. Per finire, essendo accedendo internamente al codice di minecraft, si possono trovare tracce di essi nella memoria del processo di minecraft.

Injection clients

I ghost clients sono stati la prima tipologia di cheats ad essere inventati, ma presto gli anticheat diventarono migliori, come anche le persone che controllavano. Ci voleva qualcosa di nuovo e quel qualcosa si è rivelato essere gli Injection clients. Questi clients riescono ad accedere internamente al gioco, rimanendo però un eseguibile qualunque e non quindi una versione, libreria o mod. Questo li rendeva molto più difficili da trovare ma per capirci qualcosa forse è meglio capire a prescindere il loro funzionamento. Come detto all'inizio di questo capitolo, il gioco di minecraft è scritto in java, e java stesso ci fornisce dei tool con cui noi possiamo interfacciarci con la Java Virtual Machine, ed andare ad implementare le nostre funzioni scritte in linguaggio nativo (c/c++). Queste librerie sono JNI e JvmTI, rispettivamente Java Native Interface e Java Virtual Machine Tool Interface. Non mi soffermerò troppo su jvmti, ma vi basta sapere che è la versione aggiornata e più memory safe di JNI, che è invece molto vecchia come interfaccia. Tralasciando tutto questo, gli injection clients sono delle librerie dinamiche (.dll), che si attaccano al processo di minecraft, si iniettano al suo interno e grazie all'interfaccia fornita dalle librerie JNI.h e jvmti.h, riescono a modificare il codice del gioco a loro piacimento. É fondamentale capire che gli injection client sono solo e soltanto delle DLL. I cheat maker però per rendere l'utilizzo del cheat più user friendly, hanno creato dei semplici eseguibili che si occupano di injectare la dll, che è l'effettivo cheat, all'interno del processo di minecraft. Modificando il codice del gioco dall'interno, si possono trovare tracce di questi client nel processo di minecraft, ma è più difficile trovare altre tracce perché non sono limitati alla cartella radice di minecraft. Un tempo, si usava dire che gli injection client erano tali, perché avevano la GUI all'interno della finestra di minecraft. Col tempo è stata totalmente smentita questa cosa ma vorrei approfondire e dare un po' di crediti a questa vecchia "definizione". Non è del tutto sbagliata, ma per capire bene cosa intendo dobbiamo sempre guardare tutto dal lato del programmatore. Quando io vado a creare una gui interna al gioco, è perforza una modifica del codice originale di minecraft, perché tutti i rendering dei vari elementi grafici sono gestiti dal gioco stesso. Anche le più semplici overlay si attaccano internamente, anche se in modo differente, al gioco, e sono quindi

possibilmente individuabili nella memoria del processo. Una GUI esterna però non implica che sia un external client, questo perché come ho spiegato, il cheat in se per se è un .dll, che viene iniettato nel processo del gioco, ma il programmatore potrebbe non avere voglia di fare una gui interna al gioco, così sfrutta l'eseguibile che usa per iniettare la libreria .dll come GUI, quindi interfaccia per il cheat. Questo breve chiarimento lo volevo fare per sottolineare quanto gli argomenti dei controlli e della programmazione sono intrinsechi, perché alla fine sono tutti modi diversi di approcciare lo studio del computer e dei sistemi operativi. Come breve riassunto, voi potete dare come definizione la seguente: L'injection client è un client che agisce direttamente sulla memoria del gioco, modificando classi, il che lo rende individuabile all'interno della memoria del processo.

External clients

Come ultimi (ma non ultimi davvero spoiler) abbiamo gli External clients. La principale differenza e innovazione rispetto ai precedenti injection client, è il fatto che loro accedono in modo diverso alla memoria del gioco. Se prima i ghost e gli injection si riuscivano ad interfacciarsi internamente col gioco, quindi modificando classi e quindi costrutti di alto livello, gli external client agiscono su costrutti di basso livello, sui valori singoli della memoria. Non c'è la necessità che si iniettino all'interno di un processo, perché, almeno parlando di windows, la windows API fornisce funzioni per modificare i valori della memoria dato un indirizzo valido e l'Handle di un processo. Chiaramente non significa però che gli external client sono solo eseguibili. Agendo su valori singoli della memoria, è virtualmente impossibile per noi staffer capire se un player ha usato o no un external client se ci basiamo sulla memoria del processo di minecraft. Come definizione generale si può dire la seguente: Gli external clients sono dei client che agiscono su valori singoli della memoria. Per concludere, questo fatto di poter agire su valori invece che costrutti di alto livello, li limita in funzionalità.

Autoclickers

Gli autoclickers, non sono perforza legati a minecraft in se per se. Essi esistono da molto più tempo, e sono molto facili da nascondere. Interagiscono poco e niente con il processo di minecraft la maggiorparte delle volte, e sfruttano invece le API del rispettivo sistema operativo per simulare i vari click. Non essendo trovabili nella memoria del processo di minecraft, assumono un pattern di ricerca nel pc simile a quello applicato agli external clients, ma bisogna stare attenti, perché gli external possono essere solo degli eseguibili, ma gli autoclickers possono essere scritti in molteplici linguaggi (java, python e così via), il che aumenta la quantità di artefatti da controllare e casistiche possibili. Come sotto categoria degli autoclickers, verrei parlare un po' delle macro e del debounce time. Le macro sono molto semplici come concetto, sono delle istruzioni che si assegnano ad un tasto tramite un software esterno o dedicato al mouse stesso, e si utilizzano, almeno su minecraft, per aumentare la velocità di click del player. Il debounce time invece è un argomento caldo sulla quale discutere, ma da chad jitterclicker, vorrei chiarire un po' sulla posizione del debounce time come un cheat. Il debounce time è una feature dei mouse che è stata implementata tanto tempo fa, per prevenire un problema con gli switch dei mouse, ovvero essendo essenzialmente una molla, quando cliccati rischiavano di rimbalzare ed inviare al computer un secondo, terzo, quarto click e così via, senza però che l'utente stesse cliccando appunto tutte quelle volte. Il debounce time, è il tempo in cui il software del mouse, aspetta prima di inviare un altro segnale di click. Quando un click viene registrato, parte un timer che dura tot ms (generalmente 10 o 16 millisecondi), e che evita qualsiasi tipo di multiple click accidentale da parte del mouse. Questa feature su alcuni mouse è modificabile o totalmente assente, e che permette al player di cliccare a velocità assurde, facendo utilizzo di particolari metodi che triggherano un double click, tutte sotto la categoria di mouse abuse. Su alcuni server, il debounce time sotto a 10ms è bannabile, proprio perché viene considerato un vantaggio sleale nei confronti del player medio, che ha un mouse dei cinesi e fa al massimo 10 cps non per il

debounce time ma per la qualità dello switch palesemente indonesiano. Apparte tutto, su determinati server viene considerato cheating il fare uso di click sotto la categoria mouse abuse, quando si è in possesso, a prescindere dalle impostazioni del mouse, un mouse della roccat o bloody, perché questi due, come poi anche altre marche, non sono riuscite ad implementare per bene il debounce timer, rendendo il tutto molto sleale per il player che si trova contro la persona con tale mouse. Detto questo il debounce time si può modificare solo esclusivamente dal software del mouse, se esso lo permette in primo luogo. Non esistono software esterni, anche perché il firmware di ogni mouse è unico oltre che proprietario della società che lo produce.

Conclusioni

Abbiamo visto in modo si generale, ma anche approfondito, quali sono i possibili cheats che dobbiamo cercare su minecraft, e come riconoscerli, le loro caratteristiche e tanto altro. Nelle prossime parti vedremmo invece robe più correlate al sistema operativo, e quindi informatica forense in generale. Grazie della lettura e buon proseguimento.