SS GUIDE EasyMC

Malware - Indepressed (malware#0104 -) (Head SS)

WARNING: Questa SS Guide è in continuo aggiornamento...

Questa guida è composta dalle seguenti sezioni »»

Background

Ecco come vedere tutti i programmi in background:

»» Esegui (Win + R)

»» explorer.exe shell:::{05d7b0f4-2121-4eff-bf6b-ed3f69b894d9}

Nota Bene »»» Copiate tutta la stringa completa e inseritela nell'esegui, se in caso non andasse allora provate a mettere solo questa stringa

»» shell:::{05d7b0f4-2121-4eff-bf6b-ed3f69b894d9}

Elementi Nascosti

Una volta aperta la cartella .minecraft dovremo abilitare gli elementi nascosti:

»» Visualizza

»» Elementi nascosti

poi

»» Modifica opzioni

»» Visualizzazione

»» Nascondi file protetti da sistema (consigliato)

»» Applica

»» Ok

Nota Bene »»» Se l'utente sta usando Windows 7, bisognerà cercare sulla barra di ricerca "cambia le opzioni di ricerca di file di cartelle".

Libraries

Client come la Serenity (ghost client) si nascondono all'interno della cartella "Libraries".

Per trovarla bisogna andare su:

»» .Minecraft

»» Libraries

»» Io

Nota Bene »»» In questa cartella, controlliamo la presenza di cartelle non nella norma come "GitHub" e proviamo a rinominarla.
(all'interno troveremo il percorso della Serenity.)

Client come Optifine XIV (ghost client) anche esso si trova all'interno della cartella "Libraries".
Per trovarlo bisogna andare su
»» .Minecraft
»» Libraries
»» Commons
»» Client XIV 1.1-DEVELOPMENT
»» "XIV-1.1-DEVELOPMENT.jar"
Nota Bene »»» Non dobbiamo bannare l'utente, prima dobbiamo verificare se questo file è in utilizzo (basterà spostarlo o provare a rinominarlo)

Logs

Per controllare il log del minecraft che sta utilizzando bisogna recarsi su:
»» .Minecraft
»» Logs
»» Latest
Nota Bene »»» Ora apriamo il blocco note, così avremo i logs del minecraft corrente.
»» In caso l'utente stia utilizzando il Lunar Client troveremo i suoi logs qui:
»» C:\Users\%Username%\.lunarclient\offline

»» In caso l'utente stia utilizzando il BadLion Client troveremo i suoi logs qui:
»»
C:\Users\%USERNAME%\AppData\Roaming\.minecraft\logs\blclient

Nota Bene »»» I file presenti oltre al "Latest" sono risalenti ai logs precedenti, possiamo usarli per verificare ban evading e altro.

Mods

Tutte le mod hanno un peso quindi per prima cosa dovremo confrontare i pesi delle sue mod con i pesi delle mod legit.

Una volta fatto, bisogna decompilare le mod con Luyten.

»» Apriamo Luyten

»» Trasciniamo la mod al suo interno

»» Controlliamo le Classi della mod e cerchiamo scritte come "Max Cps: / Min Cps :" oppure "A u t o c l i c k e r" oppure "Reach" "Aimbot "Triggerbot" o altro.

Nota Bene »»» Se troviamo qualcosa del genere, allora siamo davanti ad un ghost client.

Nota Bene »»» Se l'utente sta usando Forge e ispezionando una mod troviamo le classi "unlegit" spiegate prima, possiamo bannarlo.

In seguito analizziamo il "Mcmod.info" (sempre con luyten) per vedere il creatore della mod

»» Mcmod.info

»» authorList

»» Incolliamo su google il nome della mod + il nome dell'autore

»» Facciamo una breve ricerca per vedere se si tratti di una mod unlegit.

Nota Bene »»» In questo caso banniamo l'utente solo se troviamo nella nostra ricerca una mod Unlegit con lo stesso identico nome di quella che si trova nella cartella

e siamo veramente sicuri che si tratti di essa (possiamo provare a scaricarla e vedere se è uguale).

Mods Pesi

Alla fine di questo file txt vi ho inserito moltissime mod con il loro corrispettivo peso.

Mods Unloadate

E' possibile chiudere una mod in utilizzo in modo tale da poterla spostare o eliminare nella directory nonostante sia in utilizzo, dunque le Mod Unloadate sono quelle mod "rimosse" dal processo di minecraft (javaw.exe), per fare ciò bisogna andare su Process Hacker.

»» Andiamo nel processo javaw.exe

»» Properties

»» Handles

»» Selezioniamo la mod che ci interessa e premiamo su "close"

Nota Bene »»» Per verificare se una mod è stata "chiusa" dovremo incollare su Process Hacker la directory della mod, sempre nel processo "Javaw.exe":

»» Process Hacker

»» javaw.exe

»» Properties

»» Memory

»» Togliamo la spunta su "hide free regions"

»» Selezioniamo "4" al posto di "10"

»» Attiviamo la spunta su Image e Mapped

»» Filter

»» Contains (case-insensitive)

»» Incolliamo la directory delle mod (esempio: C:\Users\Christian Quartuccio\AppData\Roaming\.minecraft\mods)

Nota Bene »»» Troveremo nei risultati tutte le mod presenti nella cartella (comprese quelle unloadate) e dovremo bannare l'utente solo se nei risultati del Process Hacker
troviamo una mod che non è presente nella cartella Mods.

Mod Offuscate

Le mod offuscate sono quelle mod con codici non capibili. Apriamo luyten, decompiliamo una mod, se non potremo capire il codice poichè usciranno tutti simboli strani incomprensibili allora siamo davanti ad una mod offuscata.

Nota Bene »»» Se in un controllo ti ritrovi davanti ad una mod offuscata in uso, banna l'utente.

Java Edit

Per "java edit" si intende una versione java modificata che può contenere un cheat all'interno.
Un tool per trovare un java edit è HashMyFiles che ci permette di calcolare gli hash MD5 e SHA1 (funzioni crittografiche) di uno o più file nel sistema.
Noi dovremmo fare riferimento al codice "Sha-256"

Nota Bene »»» Alla fine di questo file txt ho rilasciato praticamente tutte le versioni possibili e le loro corrispettive Sha-256.

Lo utilizzeremo per verificare dei possibili java edit. Per esempio la versione 1.7.10 ha un codice SHA-256 diverso dalla 1.16.5 ma il codice SHA-256 della 1.7.10 sarà

uguale per ogni versione 1.7.10 scaricata dal minecraft launcher, quindi per verificare che questa 1.7.10 non sia diversa da una vostra versione legit, vi basterà trascinare la vostra versione legit nel programma e vedere se il codice risulta diverso da quello della versione 1.7.10 dell'utente (possibile unlegit)
Possiamo fare questa cosa anche con le mod, ma dobbiamo stare molto attenti che si tratti della stessa mod precisa e non ad esempio una versione aggiornata.

Nota Bene »»» Possiamo bannare l'utente solo se siamo sicuri di aver comparato la versione giusta con la versione dell'utente e troviamo un codice SHA-256 diverso.

Cestino

Per vedere se un utente ha cancellato qualcosa prima del controllo bisogna controllare la modifica del cestino.

»» Win + R oppure cerchiamo nella barra di ricerca "Esegui"
»» C:\$Recycle.bin
»» Attiviamo gli elementi nascosti nel modo che vi ho spiegato all'inizio del file
»» Poi ritorniamo sul cestino e facciamo un click destro e clicchiamo su AGGIORNA
»» Controlliamo l'ultima modifica

Nota Bene »»» Se l'ultima modifica risale a pochi minuti prima del controllo allora possiamo bannare l'utente.

Shell:recent

Il shell:recent serve a controllare gli elementi recenti.
»» Win + R oppure cerchiamo nella barra di ricerca "Esegui"

»» shell:recent

Una volta fatto ciò, ci ritroveremo nella cartella dei file recenti, controlliamo la cronologia e vediamo se appare l'ultima modifica di un ipotetico cheat.

Nota Bene »»» Banniamo l'utente solo se troviamo file espliciti (esempio: 7clicker) con data di ultima modifica maggiore all'avvio del pc.

%temp%

La cartella Temp di Windows contiene file temporanei generici creati dal sistema operativo, per aprirla apriamo "Esegui" (Win + R) e digitiamo %temp%

Usiamo il %temp% per controllare che l'utente non abbia aperto un autoclicker con estensione .jar poichè quasi tutti questi autoclicker rilasciano nel %temp% un file chiamato JNativeHook quindi per controllare se l'utente abbia utilizzato un autoclicker .jar nel %temp% dobbiamo scrivere JNativeHook

»» %temp%

»» JNativeHook

»» Controlliamo l'ultima modifica del file chiamato JNativeHook in modo da capirne l'orario di avvio.

Nota Bene »»» L'utente potrebbe aver eliminato il file bypassando il cestino, in svariati modi, quindi rechiamoci su Process Hacker

»» ProcessHacker

»» explorer

»» Properties

»» Memory

»» Togliamo la spunta su "hide free regions"

»» Selezioniamo "4" al posto di "10"

»» Attiviamo la spunta su Image e Mapped

»» Filter

»» Contains (case-insensitive)

»» JNativeHook

Nota Bene »»» Se troveremo dei risultati come "JNativeHook, JNativeHookD", NON dobbiamo bannare l'utente poichè quelli sono risultati ricerca nel %temp%, quindi
dovremo prendere in considerazione solo le stringhe come JNativeHook-4576956031440593786.dll

Nota Bene »»» Banniamo l'utente solo se troviamo un JNativeHook con data e orario di ultima modifica maggiore a data e orario di avvio del computer.

Per controllare che l'utente non abbia aperto un cheat all'interno di un archivio WinRar:

»» %temp%

»» Rar$Exa

»» Controliamo all'interno della cartella Rar$Exa tutti i file avviati dentro un archivio WinRar

Nota Bene »»» Se troviamo una cartella con data e orario di ultima modifica maggiore dell'avvio del computer, verifichiamo che ci sia effettivamente un cheat
all'interno prima di bannare l'utente, ovviamente il contenuto potrebbe essere stato modificato (spiegherò più avanti come verificarlo).

»» %temp%

»» clicks_tmp.mp3

»» Yagami.exe autoclicker / grape.exe autoclicker (trovi gli autoclicker che all'interno hano file audio, dato che ha un file audio lascia tracce nel %temp%)

controllare nel csrss i file .exe avviati

LastActivityView

Un programma che può aiutarci a controllare gli elementi recenti è LastActivityView che raccoglie informazioni da varie fonti sul sistema in esecuzione e visualizza un registro delle azioni eseguite dall'utente e degli eventi verificatisi sul suo computer.

Una volta aperto clicchiamo su "Action Time" e selezioniamo l'ultima modifica, in modo da vedere tutto in ordine.

Qui controlliamo tutti i programmi avviati dopo l'avvio del computer, cliccando su Full Path potremmo copia incollare la directory del programma.

Mettiamo caso che troviamo un presunto cheat chiamato "Vape Lite.exe" avviato dopo l'avvio di minecraft, ci basterà copia incollare la directory su "esegui" (Win + R) e verificare che si apra il cheat.

(In caso non potremo aprire il file, ritrovandoci davanti ad un "errore", l'utente lo ha sicuramente eliminato o spostato per cercare di bypassare il controllo)

Nota Bene »»» LastActivityView è collegato al prefetch. Per bypassare LastActivityView si deve cancellare il prefetch.

Prefetch

Il prefetch è una cartella di sistema apribile con Win + R e scrivendo Prefetch, dove all'interno ci saranno i log dell'esecuzione di file .exe e serve a far si che l'avvio viene sollevato dal file di sistema esempio: apposta di 1s di avvio, il prefetch fa si che lo avvii in 0.5s, quindi ne garantisci l'avvio migliore, il prefetch si può disabilitare, per farlo bisogna cambiare il parametro sul regedit che di norma è 3, tramite una regedit key possiamo vedere se il valore da 3 è 0, se è 0 allora

è unlegit e per capire se prima del controllo ha aperto il prefetch, quando entriamo nell'anydesk dell'utente e apriamo il prefetch, ci dovrà chiedere l'avvio come amministratore, se quando entriamo nell anydesk dell'utente non ci chiederà l'avvio come amministratore, allora lo ha già aperto. Ogni volta che si esegue un applicazione
nel sistema, il sistema operativo windows crea un file prefetch che contiene informazioni sul file caricati dell'applicazione nella cartella "Prefetch"

Se per esempio avviamo Chrome, esso rilascerà nel prefetch un file chiamato "CHROME.exe-D999B1C2.pf"

Quando apriamo il prefetch, dobbiamo controllare i file avviati dopo l'avvio del minecraft
esempio avvio mc: MINECRAFTLAUNCHER.EXE-0B3AF558.pf
Molto probabilmente l'utente avrà rinominato il cheat con un nome di un file legit quindi facciamo molta attenzione, ma se troviamo ad esempio una vape_lite.exe.pf
avviata recentemente o comunque dopo l'avvio di mincraft, possiamo già bannare senza perdere tempo.

Nota Bene »»» Banniamo l'utente solo se troviamo un file esplicito come un Autoclicker.pf con data e orario di ultima modifica maggiore a data e orario dell'avvio del pc,
nel caso troviamo dei file sospetti verifichiamoli con i metodi che spiegherò più avanti.

Nota Bene »»» Per tradurre i file del prefetch si usa un tool chiamato LastActivityView poichè è collegato ad esso. Per bypassare LastActivityView si deve cancellare il prefetch.

Nota Bene »»» Firma digitale = garanzia dell'autenticità del prodotto, per vedere firma digitale, tasto destro proprieta' e firma digitale

Prefetch Solo Lettura

Un metodo di bypass al prefetch, consiste nel mettere la sola lettura a un file del cheat in modo tale da non far aggiornare la sua ultima modifica quando andiamo ad avviare il cheat stesso, in questo modo quando avviamo il cheat, non si creerà il file del prefetch.

Per verificare ciò andiamo su Esegui (Win + R)

»» CMD

»» cd C:\Windows\Prefetch

»» Dir /Ar

Nota Bene »»» In questo modo vedremo tutti i file che hanno la sola lettura nel prefetch

Nota Bene »»» Nessun file del prefetch dovrebbe avere la sola lettura perciò se ne troviamo anche solo 1 di file in sola lettura, possiamo bannare l'utente

Prefetch Disabilitato

Un altro metodo di bypass al prefetch, è quello di disabilitarlo dal regedit in modo da non far apparire i .pf di un client nel Prefetch stesso.

Come vi ho spiegato sopra, per vedere se il prefetch è disabilitato bisogna controllare i suoi parametri dal regedit.

»» Esegui (Win + R)

»» regedit

»» HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters

»» EnablePrefetcher

»» Se il valore è "0" il prefetch è stato disabilitato, se il valore è 3 allora è abilitato

»» EnablePrefetcher, Clicchiamo e guardiamo i Dati Valore

»» Controlliamo che ci sia 3 e non 0

Nota Bene »»» Se il prefetch non si aggiorna e il valore è 0 allora il prefetch è stato disabilitato e quindi possiamo bannare l'utente.

Winprefetchview

»» E' un programma che controlla il Prefetch e che legge i file del Prefetch archiviati nel sistema e visualizza le informazioni in essi archiviate. Guardando in questi file è possibile apprendere quali file vengono utilizzati da ogni applicazione e quali file vengono caricati all'avvio di Windows.

»» Per prima cosa una volta aperto il programma premiamo su "Modified Time" e selezioniamo l'ultima modifica in modo da vedere tutto in ordine.

»» Ora cerchiamo "Conhost" (Stiamo attenti a data e orario per non sbagliarci) poi clicchiamo sopra il .pf e nella seconda parte in basso possiamo notare tutti gli eventuali cheat che aprono il cmd al loro avvio. (Ovviamente se troviamo file espliciti come Vape_Lite.exe possiamo già bannare l'utente).

»» Ora cerchiamo "Javaw" (Stiamo attenti a data e orario per non sbagliarci) poi clicchiamo sopra il .pf e nella seconda parte in basso possiamo notare tutti

gli eventuali autoclicker.jar avviati con tanto di file JNativeHook. (Ovviamente se troviamo file espliciti come 7Clicker.jar possiamo già bannare l'utente).

»» Ora cerchiamo "Taskhost" (Stiamo attenti a data e orario per non sbagliarci) poi clicchiamo sopra il .pf e nella seconda parte in basso possiamo notare tutti gli eventuali cheat avviati tramite il Task Manager ovvero Gestione Attività. (Ovviamente se troviamo file espliciti come Koid.exe possiamo già bannare l'utente).

Nota Bene »»» Una volta trovato un file sospetto facciamo doppio click su di esso e spostiamoci nella sua directory, mi raccomando non apriamo subito il file finchè non siamo sicuri che l'utente lo abbia avviato, fatto ciò verifichiamo che sia un cheat con i metodi spiegati più avanti poi proviamo ad aprirlo per vedere se si apre un cheat come ultima conferma, in caso il file è stato spostato/eliminato dalla sua directory ci troveremo davanti ad un errore.

Regedit

Il regedit o registro di sistema, ci indica la base di dati in cui sono custoditi le opzioni e le impostazioni di un sistema operativo di tipo Microsoft Windows e di tutte le applicazioni installate, quindi potrebbe rilevarsi utile in un controllo hack, vediamo come:

»» Esegui (Win + R)

»» regedit

Nota Bene »»» Le directory o "stringhe" che vi darò più avanti bisogna metterle nella barra di ricerca in alto.

Regedit Store

Ora controlliamo lo store del regedit, da cui possiamo visualizzare una lista di tutti gli eseguibili installati dall'utente o dai software, inseriamo questa directory:

»» Esegui (Win + R)

»» regedit

»» Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility Assistant\Store

»» in questo modo appunto, si aprirà una lista di tutti gli eseguibili installati dall'utente o dai software presenti nel pc.

Modifica al Regedit

Per controllare se è stata effettuata una modifica al regedit ad esempio l'eliminazione di un risultato nella cartella "Store" facciamo questo procedimento

(che vale per ogni cartella)

»» click destro su store

»» esporta

»» desktop

»» inseriamo un nome a piacere

»» mettiamo .txt

»» salva

»» Ora apriamo il file di testo e vediamo l'orario di ultima scrittura in alto.

Nota Bene »»» Possiamo bannare l'utente in caso abbia effettuato una modifica pochi minuti prima di essere entrati su anydesk.

Archivi WinRar

Un metodo comune di bypass consiste nell'avviare un client da un archivio WinRAR, ecco come visualizzare gli archivi WinRAR aperti dal regedit.

»» Esegui (Win + R)

»» regedit

»» Computer\HKEY_CURRENT_USER\SOFTWARE\WinRAR\ArcHistory

»» Qui troveremo una lista degli archivi WinRAR aperti sul pc. Copiamo la directory e vediamo cosa contengono.

Nota Bene »»» Non è per forza detto che siano stati visitati oggi, quindi una volta controllato che all'interno dell'archivio WinRAR ci sia un cheat, verifichiamo
che sia stato effettivamente avviato oggi, tramite i metodi che spiegherò più avanti, prima di bannare l'utente.

Estensioni

Ora controlliamo eventuali cheat presenti nel pc.

»» Esegui (Win + R)

»» regedit

»» HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU\

Nota Bene »»» In questa directory sono presenti delle cartelle, denominate con nomi di varie estensioni, ogni volta che avviamo un presunto cheat con un estensione,
si creerà un numeruni nella cartella dell'estensione con cui è stata avviata, quindi:

»» Clicchiamo sul numerino

»» Scendiamo in basso

»» Troviamo il nome con cui è stato avviato il cheat

Ad esempio: Avvio un Christian4CCIO.exe, nella cartella "exe" si creerà un numerino, che conterrà al suo interno il nome Christian4CCIO.exe

Nota Bene »»» Anche qui non è detto che il file sia stato avviato in questa sessione di gioco, ma può essere comunque un buono spunto per il nostro controllo hack, andando a verificare poi con i metodi più avanti che vi spiegherò.

Directory Regedit

Ecco a voi una lista di molte directory che potrete usare durante un controllo hack.

»» *Prefetch Disabilitato*

»»
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters

»» *Store*

»»
Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\AppCompatFlags\Compatibility Assistant\Store

»» *Archivi WinRAR*

»» Computer\HKEY_CURRENT_USER\SOFTWARE\WinRAR\ArcHistory

»» *Estensioni*

»»
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU

»» *Wmic - Estensioni spooffate - exe eseguiti*

»»
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings

»» *Vedere ultima data di modifica + nome file --->> esporta e salva come .txt*

»»
HKEY_CURRENT_USER\Software\Microsoft/Windows/CurrentVersion/Explorer/ComDlg32/OpenSavePidIMRU/dll

»» *Per visualizzare i tasti corrispondenti ai driver del mouse*
»» **Computer\HKEY_CURRENT_USER\Control Panel\Mouse**

»» *Per verificare le voci dentro la cartella MuiCache*
»»
HKEY_USERS\S-1-5-21-3588730549-3518937415-2257010710-1001\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache

»» *Per vedere tutti i dispositivi usb collegati al pc*
»» **HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\USB**

»» *Per vedere programmi aperti recentemente*
»»
HKEY_CURRENT_USER\Software\Microsoft\DirectInput\MostRecentApplication

»» *per vedere le cartelle visitate (e file aperti all'interno di esse)*
»»
KEY_CLASSES_ROOT/LocalSettings/Software/Microsoft/Windows/Shell/MuiChace

»» *Per trovare file injectati .dll .exe ecc*
»»
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU*

»» *Per controllare se è stato injectato qualcosa tramite ProcessHacker*
»» *Se si trova in una delle due cartelle di questa stringa il nome ProcessHacker.exe significa che e' stato injectato qualcosa tramite ProcessHacker*

»»
Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.dll

»» *Per controllare* **S-1-5-21-3588730549-3518937415-2257010710-1001** *E le voci DeviceHarddiskVolume***4**
»»
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRU

»» *Per controllare le voci all'interno della cartella LastVisitedPidlMRU*
»»
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32

»» *Aggiungi \dll per vedere se ci sono file dll injectati*
»»
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU

Eventvwr

E' lo strumento di diagnostica più potente di Windows. Il suo utilizzo risulta di fondamentale importanza per monitorare l'integrità del sistema perché fornisce informazioni dettagliate su tutti gli eventi che si verificano nel PC. Un evento è un fenomeno che accade dentro il sistema e viene comunicato all'esterno, ovvero all'utente o ad altri programmi, e corrisponde solitamente a uno stato o a una modifica della configurazione. In ambito SS, Con l'EventVWR possiamo controllare se l'utente ha effettuato un cambio d'orario e molto altro.

Nota Bene »»» Per vedere la directory dei logs dell'eventvwr facciamo:

»» Esegui (Win + R)
»» %SystemRoot%\System32\Winevt\Logs

EventVWR | Ereditarietà Regedit

Alcuni utenti provano a bypassare disabilitando l'ereditarietà di una cartella del Regedit, per far si che quando essa non si possa modificare. Esempio = tolgo l'ereditarietà alla cartella estensioni così quando avvio un client .dll non si creerà più la cartella relativa all'estensione Dll.

Nota Bene »»» Per detectarla bisogna fare:
»» Esegui (Win + R)
»» EventVWR
»» Registri di Windows
»» Sicurezza
»» Filtro registro corrente
»» Tutti gli id
»» 4798

Nota Bene »»» Qui ci troveremo davanti a una lista di risultati di cui la maggior parte saranno false flag, a noi interessa solo un risultato che abbia informazioni generali " nome : C:\Windows\Regedit", se troviamo un risultato del genere allora l'utente ha disabilitato l'ereditarietà.

Nota Bene »»» Se troviamo un risultato del genere in questa sessione di gioco possiamo bannare l'utente.

EventVWR | Cambio d'orario

Alcuni utenti provano a bypassare un controllo cambiando l'orario del pc all'avvio del cheat, in questo modo l'avvio del cheat risulterà a un orario diverso da quello reale.

Per detectarlo bisogna fare:

»» Esegui (Win + R)

»» EventVWR

»» Registri di Windows

»» Sicurezza

»» Filtro registro corrente

»» Tutti gli id

»» 4616

Nota Bene »»» In questo modo possiamo vedere tutti i registri relativi a un cambio orario cliccando su "dettagli" troveremo sia l'orario precedente che l'orario impostato.

Alcuni dei risultati che troveremo saranno risalenti a cambi d'ora effettuati in automatico dal sistema, e quindi false flag vediamo ora come distinguerli aiutandoci con 2 esempi.

Nota Bene »»» 1 Caso

Nel primo caso vediamo un cambio di orario effettuato da un utente con il comando "Time set" dal cmd: l'orario varierà di ore e minuti e il suo "Process Name" sarà "C:\Windows\System32\cmd.exe"

Nota Bene »»» 2 Caso

Nel secondo caso vediamo un false flag: l'orario varierà di pochi secondi (in alcuni casi potrebbe anche non variare) e il suo "Process Name" sarà "C:\Windows\System32\Svchost.exe"

Nota Bene »»» In caso troviamo un cambio d'ora non effettuato dal sistema possiamo bannare l'utente.

EventVWR | Eliminazione Eventi / Registri

Alcuni utenti cercano di bypassare un controllo eliminando i registri del visualizzatore eventi, relativi ad azioni sospette come ad esempio un cambio d'orario.

Per visualizzare l'eliminazione di un registro del EventVWR rechiamoci su:

»» Esegui (Win + R)

»» EventVWR

»» Registri di Windows

»» Sicurezza

»» Filtro registro corrente

»» Tutti gli id

»» 1102

Nota Bene »»» Qui possiamo vedere tutti gli eventi relativi all'eliminazione di un registro con tanto di data e orario.

Nota Bene »»» Se troviamo un registro eliminato in questa sessione di gioco possiamo bannare l'utente

EventVWR | Eliminazione Journal

Alcuni utenti provano a bypassare un controllo eliminando i risultati del Journal, in modo tale da non farci trovare nulla con i metodi precedentemente spiegati.

Possiamo vedere l'eliminazione dei risultati del Journal recandoci su:

»» Esegui (Win + R)

»» EventVWR

»» Registri di Windows

»» Applicazione

»» Filtro registro corrente

»» Tutti gli id

»» 3079

Nota Bene »»» Qui troveremo un errore relativo all'eliminazione dei risultati del journal, con tanto di data e orario.

Nota Bene »»» Se troviamo una eliminazione del journal fatta durante questa sessione di gioco possiamo bannare l'utente

ExecutedProgramsList

Questo programma visualizza per ogni programma la data di creazione e la modifica del file .exe + le informazioni sulla versione corrente del programma

»» Clicchiamo su File last modified

»» Per vedere tutti i risultati in ordine

RecentFilesView

Questo programma vi mostrerà l'elenco di tutti i file aperti di recente, può mostrarci anche l'avvio di un cheat che non abbia nome e estensione.

ShellBagsView

Questo programma visualizza l'elenco di tutte le cartelle visitate dall'utente, questo è possibile poichè ogni volta che apriamo una cartella in Esplora risorse,

Windows salva automaticamente le impostazioni di questa cartella nel Registro di sistema.

Possiamo utilizzarlo quindi per vedere le cartelle aperte dall'utente e verificare se ha aperto qualche cartella sospetta o anche per vedere se ha aperto

qualche cartella per eliminare tracce di Ban Evading, ad esempio la cartella Logs.

Nota Bene »»» Anche qui bisogna selezionare Last Modified Time per visualizzare tutto in modo ordinato.

USBDeview

Questo programma elenca tutti i dispositivi USB attualmente collegati al computer, nonchè tutti i dispositivi USB utilizzati in precedenza.

Aprendolo troveremo una lista di tutti i dispositivi che sono collegati o sono stati collegati in precedenza.

»» Registry 1 = orario in cui è stato collegato un dispositivo
»» Registry 2 = orario in cui è stato scollegato un dispositivo

Nota Bene »»» Quelli evidenziati in verde sono i dispositivi al momento collegati.

Nota Bene »»» Possiamo utilizzarlo per vedere se l'utente ha scollegato un mouse (magari contenente una macro) o una chiavetta prima del controllo,
oppure se utilizza due mouse per "Mouse Abusare"

Nota Bene »»» Se un utente ha staccato una chiavetta o un mouse prima del controllo, banniamolo.

HotKeysList

E' uno strumento per windows che visualizza l'elenco di tasti di scelta rapida attualmente registrati sul sistema.
E' possibile utilizzare questo strumento per determinare facilmente quali tasti di scelta rapida sul sistema sono disponibili per l'uso.

Nota Bene »»» Possiamo utilizzarlo anche per vedere tutti i programmi di registrazione in background o autoclicker non chiusi che hanno degli shortcut.

Macro

Per macro si intende assegnare una funzione specifica ad un pulsante del mouse o della tastiera, che solitamente dà notevoli vantaggi in gioco come ad esempio il doppio o triplo click, che ci permettono di cliccare più velocemente.

»» C:\Users\%username%\AppData\Local\Razer\Synapse3\Log
»» Razer Synapse 3.log

»» C:/ProgramData/Razer/Synapse/Accounts
»» Macro

»» C:\Users\%username%\AppData\Local\Logitech\Logitech Gaming Software
»» settings

»» C:\Users\%username%\AppData\Local\LGHUB
»» settings

»» C:\Users\%USERNAME%\Documents\M711 Gaming Mouse
»» MacroDB

»» C:\Users/%username%\AppData\Roaming\ROCCAT\SWARM\macro
»» custom_macro_list

Nota Bene »»» Bisogna controllare l'ultima modifica.

Verificare un Cheat

Ogni volta che troviamo una directory sospetta dobbiamo verificare che si tratti effettivamente di un cheat. Per farlo selezioniamo la directory che ci interessa e in basso a destra premiamo "Copy" e incolliamo la directory su Esegui (Win + R), quando la incolliamo eliminiamo tutti i caratteri presenti prima del C:\ e togliamo alla fine il nome del file, in modo tale da spostarci solo nella cartella in cui si trova e non aprirlo direttamente.

Fatto ciò per prima cosa controlliamo le "Proprietà" e vediamo la data di ultima modifica e quella di ultimo accesso, in modo tale da avere una maggiore conferma del fatto che quel file sia stato avviato e solo dopo fatto ciò proviamo ad aprirlo per vedere se si tratta di un cheat.

Mettiamo caso che il file non si apra e vogliamo un ulteriore conferma che esso sia unlegit allora rechiamoci su process hacker e controlliamo se ha degli imports che potrebbero risalire a un client generico, ecco come:

»» Aprire ProcessHacker2
»» Tools
»» Inspect executable file
»» Selezionare il file
»» Apri
»» Imports

controlliamo la presenza di alcuni imports che potrebbero essere unlegit:

»» Mouse_Event = Risalibile a un Autoclicker
»» SendMessage = Risalibile a un Autoclicker
»» RegDelValue = Risalibile al Self Destruct di un client
»» WriteProcessMemory = Risalibile a una Memory Hacking (Reach ecc ecc)
»» GetKeyState = Risalibile a un Keybinding per stoppare o avviare il clicker

»» GetAsyncKeyState = Risalibile a un Keybinding per stoppare o avviare il clicker

Nota Bene »»» Se troviamo solo uno dei seguenti imports elencati prima, non è detto che sia un cheat perciò prima di bannare l'utente
assicuriamoci che c'è ne siano almeno più di 1 o 2.

Nota Bene »»» Mouse_Event e WriteProcessMemory invece sono abbastanza sicuri e possiamo bannare se un programma ha anche solo 1 dei due imports appena elencati

Data di creazione Spoffata

Alcuni utenti si divertono a cambiare la data di creazione o di ultima modifica per bypassare metodi precedentemente spiegati. Per trovare questo
metodo di bypass ci sono due metodi.
Il primo consiste nel filtrare nel processo del PowerShell la seguente stringa:
»» PowerShell
»» Properties
»» Memory
»» Togliamo hide free regions
»» Selezioniamo 4 al posto di 10
»» Attiviamo la spunta su Image e Mapped
»» Filter
»» Contains (case-insensitive)
»» $(Get-Item
»» Se l'utente ha modificato qualcosa di troveremo davanti a risultati come: $(Get-ite Koid.exe).creationtime=$("12/23/2020")

Nota Bene »»» Per prima cosa dovremmo aprire il PowerShell in modo da far apparire il processo stesso su ProcessHacker, poi cerchiamo sulla barra di ricerca
PowerShell.exe

Il secondo metodo consiste nel controllare la cronologia del powershell:

»» Esegui (Win + R)

»» C:\Users\%Username%\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine

»» Apriamo il file di testo "Consolehost_History.txt"

»» E cosi troveremo una cronologia di tutti i comandi che l'utente ha eseguito su powershell

Oppure andiamo su PowerShell e inseriamo la stringa:

»» > cat (get-PSReadlineoption).Historysavepath

Nota Bene »»» In entrambi casi però, non potremo sapere in che data e orario è stata effettuata la modifica quandi possiamo decidere se bannare o continuare a investigare.

Estensione Spoffata

Per estensioni spoffate si intende quando un utente cambia l'estensione di un file in un estensione inesistente, ad esempio un "cheat.exe" viene rinominato in "cheat.ciaociao" e poi avviato.

Esempio: rinominiamo un "Yukuma.exe" in "Yukuma.ciaociao" e lo avviamo dal cmd facendo start directory client

Possiamo trovare delle estensioni spoffate con 3 metodi:

Il primo consiste nell'inserire nel Regedit questa directory:

»» Esegui (Win + R)

»» regedit

»» Computer\HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU\

In questo modo troveremo delle sottocartelle denominate coi nomi delle varie estensioni e troveremo anche la nostra estensione spoffata, in questo caso ciaociao.

Nota Bene »»» Cliccando sull'estensione, ci troveremo sulla destra una lista di numeri per ogni client che abbiamo avviato con la rispettiva estensione si creerà un numero diverso

In questo caso troviamo solo lo "o" poichè abbiamo avviato un solo client con l'estensione "ciaociao"

»» doppio click sullo "o"

»» scendiamo in basso

»» visualizziamo il nome del client, in questo caso Yakuma

Nota Bene »»» Non è per forza detto che abbia avviato il client oggi, ma potrebbero averlo fatto giorni prima,tuttavia questo passaggio può rivelarsi davvero utile per farci un'idea di cosa potrebbe star usando il nostro utente.

Un altra directory utile per vedere una lista di estensioni spoffate create sul pc è questa:

»» Esegui (Win + R)

»» regedit

»» Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\

Nota Bene »»» Scorrendo troviamo tutte le ipotetiche estensioni spoffate che potrebbero essersi create

Nota Bene »»» Non è per forza detto che abbia avviato il client oggi, ma potrebbero averlo fatto giorni prima,tuttavia questo passaggio può rivelarsi

davvero utile per farci un'idea di cosa potrebbe star usando il nostro utente.

Il Secondo metodo consiste nel vedere come trovare un avvio di un client con estensione spoffata dal csrss.exe

»» csrss

»» Properties

»» Memory

»» Togliamo hide free regions

»» Selezioniamo 4 al posto di 10

»» Attiviamo la spunta su Image e Mapped

»» Filter

»» Regex (case-insensitive)

»» ^[A-Z]:\\((?!Exe|dll|jar|ini).)*$

In questo modo troveremo l'avvio di un client con l'estensione modificata

Nota Bene »»» Una volta trovato l'avvio di un file con un'estensione inesistente possiamo bannare direttamente l'utente.

Il Terzo metodo consiste nel trovare un estensione spoffata dal dps, con un procedimento simile a quello del csrss, utilizzando sempre come esempio

il nostro Yukuma.exe con un estensione cambiata in Yukama.ciaociao:

»» -s dps

»» Properties

»» Memory

»» Togliamo hide free regions

»» Selezioniamo 4 al posto di 10

»» Attiviamo la spunta su Image e Mapped

»» Filter

»» Regex (case-insensitive)

»» ^!![A-Z](.)((?!Exe|dll).)*$

In questo modo ci troveremo davanti a una lista di risultati, ma noi dovremmo fare caso solo a risultati come: "Yukama.ciaociao!2020/10/15:23:48:34! 1eb4b3"

Nota Bene »»» Una volta trovato l'avvio di un file con un estensione inesiste possiamo bannare direttamente l'utente.

METODO Journal

Il journal delle modifiche USN, quando vengono aggiunti, eliminati, modificati file, directory e altri oggetti NTFS fornisce un log permanente di tutte le modifiche apportate ai file nel volume, quindi possiamo utilizzarlo in vari modi nei controlli hack.

Journal FILE ELIMINATI

Alcuni utenti provano a bypassare un controllo eliminando il file residui di cheat, per fortuna possiamo visualizzare un elenco dei file eliminati dal Journal, inserendo l'id degli Eliminati:

Stringa »» fsutil usn readjournal c: csv | findstr /i /C:"%date%" | findstr /i /C:"0x80000200" | findstr /i /C:.exe\^" /i /C:.pf\^" /i /C:.com\^ /i /C:.jar\^" /i /C:.pif\^" /i /C:.bat\^ /i /C:.zip\^" /i /C:.cmd\^" /i /C:.?\^" /i /C:.com\^ /i /C:.rar\^" > Eliminati.txt

Apriamo il file di testo e ci troveremo davanti a una lista di tutti i file eliminati con tanto di data e orario

Nota Bene »»» A questa stringa ho aggiunto %date% (data del giorno corrente) e un tot di estensioni in modo tale da ridurre più false flag possibili.

Nota Bene »»» Ovviamente ciò non vuol dire che possiamo bannare l'utente se ha eliminato qualcosa prima del controllo, perchè alcuni potrebbero essere file di sistema
che si sono eliminati automaticamente, ma possiamo farlo solo se ha eliminato un file sospetto che è stato avviato o se addirittura ha eliminasto il cheat prima del controllo.

Journal FILE RINOMINATI

Quando rinominiamo un file, il suo nomev aria in un orario preciso, quindi dal journal potremo vedere sia il nome precedente che il nuovo nome inserendo
l'ID dei file rinominati:

```
Stringa »» fsutil usn readjournal c: csv | findstr /i
/C:"%date%"| findstr /i /C:"0x00001000" /i
/C:"0x00002000" | findstr /i /C:.exe^" /i /C:.pf\^" /i
/C:.com\^ /i /C:.jar\^" /i /C:.pif\^" /i /C:.bat\^ /i
/C:.zip\^" /i /C:.cmd\^" /i /C:.?\^" /i /C:.com\^ /i
/C:.rar\^" /i /C:.reg\^" > Rinominati.txt
```

Nota Bene »»» Se l'utente ha rinominato un file, troveremo due risultati allo stesso identico orario (Vecchio nome e Nuovo nome) in cui saranno indicati
il nome precedente e il nuovo nome, con tanto di data e orario in cui è stato cambiato

Nota Bene »»» Ovviamente ciò vuol dire che non possiamo bannare l'utente se ha rinominato qualcosa ma possiamo farlo solo se ha rinominato un file che
è stato avviato o se addirittura ha rinominato il cheat prima del controllo.

```
fsutil usn readjournal c: csv | findstr /i
/C:"0x80000200" /i /C:"0x00001000" /i  /C:”0x00002000" |
findstr /i /C:.exe\^" /i /C:.pf\^" /i /C:.com\^" /i
/C:.cmd\^" /i /C:".jar" /i /C:.pif\^" /i /C:.bat\^" /i
/C:"?" > filemoved.txt
```

Journal Stringhe

```
fsutil usn readjournal c: csv | findstr /i
/C:"JnativeHook" > Jar.txt
```

[Clicker .jar]

```
fsutil usn readjournal c: csv | findstr /i /C:0x00008000
/i /C:0x80008000 | findstr /i /C:"Sola lettura |
Archivio" > SolaLettura.txt
```

[File con sola lettura]

```
fsutil usn readjournal c: csv | findstr /i
/C:"0x00000800" /i /C:"0x80000800" | findstr /i
/C:"Prefetch" > modificasicurezza.txt
```

[Cacls o modifica dei permessi del prefetch]

```
fsutil usn readjournal c: csv | findstr /i
/C:"0x00000800" /i /C:"0x80000800" | findstr /i /C:"Logs"
> ModificaEventvwr.txt
```

[Cacls o modifica dei permessi del Visualizzatore Eventi]

```
fsutil file queryFileNamebyid C:\ 0x
```

[Leggere la directory]

```
fsutil usn readjournal C: csv | findstr /i /c: x80200120
→ 0x80000060 (Wmic)
```

```
fsutil usn readjournal c: csv | findstr /i
/C:"0x80000200" | findstr /i /C:".pf" | findstr /i
/C:"%date%" > prefetcheliminato.txt
```

[Pf eliminato]

```
fsutil usn readjournal c: csv | findstr /i /C:"%date%" |
findstr /i /C:"Jnativehook" | findstr /i /C:".dll" >
jh.txt
[JNativeHook]

fsutil usn readjournal c: csv | findstr /i /C:"%date%" |
findstr /i /C:"0x80000200" |findstr /i /C:.exe\^" /i
/C:.com\^" /i /C:.cmd\^" /i /C:.pif\^" /i /C:.bat\^" /i
/C:"?" > fileliminati.txt

fsutil usn readjournal c: csv | findstr /C:"0x00001000" |
findstr /i /C:"%date%" > rinominati.txt

fsutil usn readjournal c: csv | findstr /i /C:0,3,0,96 |
findstr /i /C:prefetch | findstr /i /C:"%date%" >
Cacls.txt

fsutil usn readjournal c: csv | findstr /i
/C:"0x80200120" /i /C:"0x00200000" > BestEuW-Mic.txt

fsutil usn readjournal c: csv | findstr /i
/C:"0x80000200" > w-mic2.txt

fsutil usn readjournal c: csv | findstr /i /C:"?" |
findstr /i /C:"%date%"  > specialcaracters.txt

fsutil usn readjournal c: csv | findstr /i
/C:"0x00200000" /i /C:"0x80200120" | findstr /i
/C:"%date%" > Type.txt

fsutil usn readjournal c: csv | findstr /i /C:.exe\^" /i
/C:.com\^" /i /C:.cmd\^" /i /C:.pif\^" /i /C:.bat\^" /i
/C:"?" | findstr /i /C:"%date%" | findstr /i
/C:"0x00000100" > GenericCheatCheck.txt
```

```
fsutil usn readjournal c: csv | findstr /i
/C:".timestamp" /i /C:"jar_cache" | findstr /i
/C:"%date%" | findstr /i /C:"0x00000004" /i
/C:"0x00000102" > jar.tx

fsutil usn readjournal c: csv | findstr /i /C:%date% |
findstr /i /C:regsvr32 | findstr /i /R
/C:"[0-9],0x00000100" > CmdDll.txt f

fsutil usn readjournal c: csv | findstr /i
/C:"0x00000100" | findstr /i /C:"%date%" | findstr /i
/C:".dll.lnk" > NotepadDll.txt

fsutil usn readjournal c: csv | findstr /i /C:".pf" |
findstr /i /C:"%date%" | findstr /i /C:"net" /i /C:"net1"
> restartprocess.txt

fsutil usn readjournal c: csv | findstr /i 0x00000060 |
findstr /i 0000000000000000001400000000013d >
DetectWmicprivate.txt
```

METODO Java-Jar

Il metodo javar-jar è un metodo che usano gli utenti per provarci a bypassare utilizzando un autoclicker.jar avviato tramite il cmd con il comando Java-jar (clicker.jar)
e eliminando il file che si crea nel %temp% sempre tramite il cmd con il comando Del file.

Nota Bene »»» In questo modo non potremmo trovarlo tramite l'explorer di processhacker

Possiamo però trovare sia la creazione del file sia che l'eliminazione usando il Journal e chiedendogli di filtrare con "JNativeHook":

Stringa »» fsutil usn readjournal c: csv | findstr /i /C:"JnativeHook"> JNativeHook.txt

Apriamo il file di testo e ci troveremo davanti tutti i JNativeHook che sono stati creati o eliminati, con tanto di data e orario.

Nota Bene »»» Se troviamo i risultati della creazione di un JNativeHook fatta durante la sessione di gioco possiamo bannare l'utente.

»»»» SOLA LETTURA

Come abbiamo già visto in precedenza con il Prefetch, è possibile mettere in modalità Sola lettura un file in modo tale da non fare aggiornare la sua ultima modifica.

Abbiamo già visto il detect ma se in caso l'utente tolga la sola lettura al file prima del controllo allora non sarà più possibile trovarla con il comando

Dir /Ar dal cmd e dovremo chiedere al journal di filtrare con l'id per la sola lettura:

Stringa »» fsutil usn readjournal c: csv | findstr /i /C:0x00008000 /i /C:0x80008000 | findstr /i /C:"Sola lettura | Archivio" > Solaletturapf.txt

Nota Bene »»» In questo modo troveremo tutti i file a cui è stata messa la sola lettura con tanto di data e orario. A questa stringa per evitare

False Flag gli è stata aggiunta un "findstr /i /C:Sola lettura | Archivio". Ciò vuol dire che questa stringa funzionerà solo con i pc impostati sulla lingua Italiana,

mentre per i pc in altre lingue bisognerà tradurre "Sola lettura | Archivio" nella lingua che ci interessa.

Nota Bene »»» Se troviamo i risultati della sola lettura a un file del prefetch fatta durante la sessione di gioco possiamo bannare l'utente.

Replace

Alcuni utenti, provano a bypassare un controllo sostituendo un file unlegit con un file legit e si può fare in due modi molto simili.

»» Primo modo : avvio un AnyDesk.exe (autoclicker) e al momento del controllo lo chiudo e trascino in quella directory un AnyDesk.exe (reale)
e clicco su sostituisci elementi, in questo modo quando andremo a incollare su Esegui (Win + R) la directory del cheat, ci troveremo davanti ad un AnyDesk legit.

»» Secondo modo : avvio un AnyDesk.exe (autoclicker) al momento del controllo lo chiudo e lo shift-cancello, poi rinomino un altro file legit presente
in quella directory in AnyDesk.exe

»» In questo modo quando troveremo l'avvio di un AnyDesk.exe andando a controllare il file, ci troveremo davanti ad un file completamente Legit.

Nota Bene »»» Per fortuna possiamo verificare un replace fatto con sostituisci file utilizzando il Journal e inserendo L'ID dei file Eliminati e Rinominati :

Stringa: »» fsutil usn readjournal c: csv | findstr /i /R /C "0x80000200" /i /C:"Ox00001000" /i /C:0x00002000" | findstr /i /C:.exe\^" /i /C:.pf\^" /i /C:.com\^" /i /C:.cmd\^" /i /C:".jar" /i /C:.pif\^" /i /C:bat\^" /i /C:"?" > file.txt

Nota Bene »»» Per il primo metodo dobbiamo trovare una combinazione di 3 risultati nel journal che possiedono lo stesso "file name"

»» 2 Metodo (replace manualmente)

Per fortuna possiamo verificare un replace fatto manualmente utilizzando il Journal e inserendo l'ID dei file Eliminati e Rinominati

(quindi la stessa stringa del primo metodo)

Per il secondo metodo dobbiamo trovare una combinazione di 3 risultati nel journal di cui 2 avranno il "file name" del file che vogliamo sostituire e

1 avrà il "file name" del file che abbiamo rinominato.
Vediamo ora un esempio dei risultati interessanti

»» AnyDesk.exe > Eliminazione File

»» Replace.exe > Ridenominazione : vecchio nome

»» Anydesk.exe > Ridenominazione: nuovo nome

Nota Bene »»» Anche in questo caso è molto semplice, ci basta trovare il file eliminato e la ridenominazione del file fatta pochi istanti dopo.

ovviamente io ho fatto l'esempio eliminando un Anydesk.exe e rinominando in AnyDesk.exe un file chiamato Replace.exe ma l'utente potrebbe averlo

fatto con qualsiasi altro file legit.

»»»» File Spostati

Possiamo vedere i file spostati utilizzando sempre la stringa vista per i replace, i risultati che ci interessano sono molto simili a quelli visti nel

primo metodo (Replace automatico), ma in questo caso non sarà presente l'eliminazione del file quindi in questo caso i risultati sono la ridenominazione

vecchio nome e la rinominazione nuovo nome, fatta allo stesso orario preciso e con lo stesso "file name",
Vediamo ora un esempio dei risultati che ci interessano :

»» AnyDesk > Ridenominazione : vecchio nome

»» AnyDesk > Ridenominazione : nuovo nome

Nota Bene »»» Anche in questo caso è molto semplice, ci basta trovare la ridenominazione di un file a cui non varia il "file name", ovviamente io ho fatto l'esempio con anydesk ma l'utente avrebbe potuto farlo con qualsiasi altro file.

ProcessHacker

Process Hacker è un programma che ci permette di vedere i processi in esecuzione, è una sorta di task manager (gestione attività) ma che ci darà la possibilità di cercare le stringhe rilasciate da attività svolte sul pc, nel nostro caso ad esempio: stringhe rilasciate dal self destruct di un client, l'avvio di un programma, un metodo di bypass e molto altro.

1) Ricordati di avviarlo sempre come amministratore altrimenti non potrai controllare alcuni processi come il CSRSS

2) Se ti sei dimenticato di avviarlo come amministratore allora devi andare su:
»» Hacker
»» Show details for all process

3) Una volta aperto Process Hacker assicuriamoci che l'utente non abbia nascosto dei processi.
»» View
»» Hide process from other users
»» e togliamo la spunta

4) Se quando cerchi un processo, ti usciranno più risultati allora fai sempre riferimento a quello col peso maggiore.

5) Ricordiamoci appena abbiamo finito di utilizzare ProcessHacker di andare su

»» Hacker
»» Options...
»» Reset
»» In questo modo resetteremo le ricerche del ProcessHacker e un utente non potrà salvarsi le nostre stringhe.

6) Ricordati sempre di controllare se l'utente ha riavviato un processo.
»» nome del processo
»» Properties
»» General
»» Controlla l'orario che uscirà su Started:

7) Controllare sempre per prima cosa il PcaClient ---> Spiegherò cos'è e a cosa serve di sotto nella parte "Explorer"

8) Ricordati sempre di controllare se l'utente ha riavviato un processo.
»» nome del processo
»» Properties
»» General
»» Controlla l'orario che uscirà su Started:

Nota Bene »»» Se un utente ha riavviato un processo fondamentale come l'explorer allora puoi bannarlo.

Nota Bene »»» Processi come il CSRSS e lsass non possono essere riavviati

Nota Bene »»» Processi come Explorer | Csrss | lsass | pcasvchost | -s Dps (svchost) NON devono essere stati avviati dopo l'avvio del processo javaw.exe,
Se uno di questi processi è stato riavviato dopo l'avvio di minecraft possiamo bannare l'utente.

Explorer

Utility »» Ecco come verificare i programmi avviati da quando l'explorer si è avviato (quindi da quando si è avviato il pc)

Processo »» Explorer
Filtro »» Contains (case-insensitive)
Stringa »» file:///
poi
Filtro »» Contains (case-insensitive)
Stringa »» .exe

Nota Bene »»» (Oltre a .exe puoi mettere altre estenzioni che ti interessano, esempio: .dll o .py)

Utility »» Il PcaClient è un metodo che ci mostrerà gli ultimi 10 file "Eseguibili" avviati sul pc.

Processo »» Explorer
Filtro »» Contains (case-insensitive)
Stringa »» Pcaclient
»» Save...
»» Salviamoci i risultati sul desktop come file .txt
»» Apriamo e vediamo gli ultimi 10 .exe avviati.
»» Ricordiamoci di copia incollare la directory su Esegui (Win + R) per vedere se l'utente ha rinominato un cheat ad esempio in Anydesk.exe che si
trova in una directory sospetta.
Nota Bene »»» Se tra questi file è presente un cheat allora bisogna bannare l'utente.

Nota Bene »»» Se ci darà un errore quando copia incolliamo una directory sull'Esegui (Win + R) allora l'utente ha probabilmente spostato il file in un altra directory.

Utility »» Ecco come vedere se l'utente ha avviato un cheat da telegram desktop.

Processo »» Explorer
Filtro »» Regex (case-insensitive)
Stringa »» ^[A-Z:.Users.+.Telegram Desktop.+\.(.*)$

Nota Bene »»» In questi risultati ci saranno i file avviati da telegram desktop
Nota Bene »»» Se ci sono 4 o + risultati uguali dello stesso cheat allora banniamo l'utente.

Utility »» Ecco come controllare se l'utente ha avviato un cheat all'interno di archivi WinRAR o 7Zip

Processo »» Explorer
Filtro »» Regex (case-insensitive)
Stringa »» ^[C-H]:\\Users\\.*\\appdata\\.*\\Temp\\.*.$

Nota Bene »»» In questi risultati ci saranno i file avviati da archivi WinRAR o 7Zip
Nota Bene »»» se ci sono 4 o + risultati uguali dello stesso cheat allora banniamo l'utente.

Utility »» Questa stringa esclude tutti i file del Disco Locale (C:), quindi fa vedere tutti i file avviati che si trovano in altri dischi // chiavette.

Processo »» Explorer
Filtro   »» Regex (case-insensitive)
Stringa »» ^(?!C:)[A-Z]:\\.+

Utility »» Per trovare autoclicker.dll nascosti nel system 32

Processo »» Explorer
Filtro   »» Regex (case-insensitive)
Stringa »» ^\w:\.+\system32\.+.dll$

Utility »» Per trovare autoclicker.dll nascosti nel system 32

Processo »» Explorer
Filtro   »» Regex (case-insensitive)
Stringa »» [C-G]:\\(?!windows\\system32).*dll

Utility »» file rinominati// usb history

Processo »» Explorer
Filtro »» Regex (case-insensitive)
Stringa »» ^(?!C:)[A-Z]:\\.+

Utility »» file registrazione ecc

Processo »» Explorer
Filtro »» Regex (case-insensitive)
Stringa »»
^[A-Z]:.+\.(|flv|divx|avi|asf|mp4|3gp|swf|mp3|mpeg|mpg|ogm|wmv|mov|mkv|nbr|rm|vob|sfd|webm|xvid)$

Utility »» Caratteri speciali

Processo »» Explorer
Filtro »» Regex (case-insensitive)
Stringa »» ^file:///[A-Z]:/.+./$

Utility »» detect Mountvol

Processo »» Explorer

```
Filtro   »» Regex (case-insensitive)
Stringa  »» ^\\\\?\\.+.Volume.+.\\.+.$
------------------------------------------------------------
------------------------------------------------------------
------------------------------------------------------

Utility »» detect Mountvol

Processo »» Explorer
Filtro   »» Regex (case-insensitive)
Stringa  »» \\\?\\Volume{.+}\\.+

------------------------------------------------------------
------------------------------------------------------------
------------------------------------------------------

Utility »» Ogni file .exe

Processo »» Explorer
Filtro   »» Regex (case-insensitive)
Stringa  »» ^file:///.+\.exe$


------------------------------------------------------------
------------------------------------------------------------
------------------------------------------------------

Utility »» Qualsiasi estensione

Processo »» Explorer
Filtro   »» Regex (case-insensitive)
Stringa  »» ^file:///.+$

------------------------------------------------------------
------------------------------------------------------------
------------------------------------------------------
```

Utility »» File stream (type etc.)

Processo »» Explorer
Filtro »» Regex (case-insensitive)
Stringa »» ^[C-H]:\\.+:

Utility »» Ogni jnativehook

Processo »» Explorer
Filtro »» Regex (case-insensitive)
Stringa »» ^.+jnativehook-.+\.dll$

Utility »» File .cfg programmi

Processo »» Explorer
Filtro »» Regex (case-insensitive)
Stringa »» ^\w:\\.+{directory}.+\.(exe|cfg)$
(DA USARE IN COMBINAZIONE CON FILE://, RICORDA CHE NELLE DIRECTORY VA MESSO "\\" AL POSTO DI "\")

Utility »» Per trovare estensioni spooffate

Processo »» Explorer

Filtro »» Regex (case-insensitive)

Stringa »»
^c:.+\.(|pif|txt|jpg|lnk|mp4|ico|sys|sys|log|dat|tmp|bat|pif|cmd|comocx|vbs|bat|js|msi|reg|shs|sys|vb|vbe|wsc|wsf|wsh|scr|asm|zip|ini||pifhtm|html|xls|ppt|docx|docx|xlsx|dot|xlt|xml|bin|ax|fon|chm|msp|tlb|aspx|asp|cpl|drv|msc|api|app|apl|aup)$

Csrss

All'interno del csrss possiamo trovare tutti i programmi avviati.

Utility »» Ecco come controllare gli eseguibili avviati con Doppio click o dal CMD o dal TaskManager (gestione attività)

Processo »» Csrss

Filtro »» Contains (case-insensitive)

Stringa »» ^[A-Z]:\\.+.exe$

Nota Bene »»» In questo modo troveremo una lista di tutti i .exe avviati, sta a noi verificare se siamo cheat o meno.

Utility »» Ecco come controllare se ci sono dll injectati dal Notepad

Processo »» Csrss

Filtro »» Contains (case-insensitive)

Stringa »» ^[A-Z]:\\.+.dll$

Nota Bene »»» In questo modo troveremo tutti i .dll avviati, ovviamente solo uno fra tanti sarà il nostro client, starà a noi verificare i
dll presenti in directory sospette, per provare ad aprirli ci basterà aprire il cmd come amministratore ed eseguire il comando:

Comando »» regsvr32 directory.dll

Utility »» Estensioni spooffate
Processo »» Csrss
Filtro »» Regex (case-insensitive)
Stringa »»
^c:.+\.(|pif|txt|jpg|lnk|mp4|ico|sys|sys|log|dat|tmp|bat|pif|cmd|comocx|vbs|bat|js|msi|reg|shs|sys|vb|vbe|wsc|wsf|wsh|scr|asm|zip|ini||pifhtm|html|xls|ppt|docx|docx|xlsx|dot|xlt|xml|bin|ax|fon|chm|msp|tlb|aspx|asp|cpl|drv|msc|api|app|apl|aup)$

Utility »» Estensioni spooffate
Processo »» Csrss
Filtro »» Regex (case-insensitive)
Stringa »»
^\w:.+\.(|pif|txt|jpg|lnk|mp4|ico|sys|sys|log|dat|tmp|bat|pif|cmd|comocx|vbs|bat|js|msi|reg|shs|sys|vb|vbe|wsc|wsf|wsh|scr|asm|zip|ini||pifhtm|html|xls|ppt|docx|docx|xlsx|dot|xlt|xml|bin|ax|fon|chm|msp|tlb|aspx|asp|cpl|drv|msc|api|app|apl|aup)$

Utility »» Per vedere file .exe/.dll avviati fuori dalla cartella users
Processo »» Csrss
Filtro »» Regex (case-insensitive)
Stringa »» ^\w:\(?!Users).+exe$ oppure ^\w:\(?!Users).+dll$

Utility »» Estensioni spooffate
Processo »» Csrss
Filtro »» Regex (case-insensitive)
Stringa »» [a-z]:\\.+.((?<!\\)(?<!exe))(?<!dll)(?<!;)(?<!config)(?<!manifest)(?<!cpl)$

Utility »» File .exe avviati
Processo »» Csrss
Filtro »» Regex (case-insensitive)
Stringa »» ^[A-Z]:\\.+.exe$

Utility »» File .dll avviati
Processo »» Csrss

Filtro »» Regex (case-insensitive)

Stringa »» ^[A-Z]:\\.+.dll$

Utility »» Per trovare autoclicker.dll nascosti nel system 32

Processo »» Csrss

Filtro »» Regex (case-insensitive)

Stringa »» [A-Z]:\\.+\\System32\\.+\.Config

Utility »» Il .config perche il csrss i file eseguiti cosi li segna dal sys32

-s Dps

Ogni file ha una data di creazione e nel dps possiamo trovare tracce di cheat sfruttando proprio questa "data di creazione" ecco come:

Processo »» -s dps

Filtro »» Regex (case-insensitive)

Stringa »» ^!!(?!svchost|dwm|csrss|explorer|taskhostw|ctfmon|rundll32|conhost|lsass|usoclient|sihost|dashost|nissrv|smss|sc|servicehost|settingsynchost|consent|dllhost|sppsvc|wermgr).+.exe

Nota Bene »»» Se troviamo risultati come: !!CRWindowsClientService.ex!2020/08"24:10:48:54!5ftxd6!

controlliamoli tutti e vediamo se troviamo qualcosa di sospetto ad esempio il nome di un cheat o più nomi uguali con date di creazione diverse.

Se troviamo ad esempio più risultati di "AnyDesk" con date di creazione diverse, l'utente potrebbe aver avviato oltre al vero "AnyDesk" un autoclicker/client

chiamato con lo stesso nome oppure aver fatto un replace.
Tra le parentesi la stringa rimuove tutti i file di sistema con quel nome che solitamente sono false flags ciò vuol dire che se un utente rinomina il cheat ad esempio in "svchost" non lo troveremo in questi risultati. Se vogliamo però possiamo sostituire la stringa con questa:

Processo »» -s dps
Filtro »» Regex (case-insensitive)
Stringa »» ^!!.+.exe

Nota Bene »»» Ma ci troveremo davanti a numerosi false flag almeno che non ci troviamo davanti ad un cheat esplicito come Vape_Lite prendiamo questi risultati solo come spunto.

Javaw

Il processo Javaw è il processo a cui si appoggia Minecraft e viene modificato da Ghost e Injection client, perciò possiamo sfruttarlo per cercare le varie stringhe rilasciate da alcuni di questi client.

»» Javaw
»» Properties
»» Memory
»» Togliamo hide free regions
»» Selezioniamo 4 al posto di 10
»» Attiviamo la spunta su Image e Mapped
»» Filter
»» Contains (case-insensitive)
»» E mettiamo una di queste stringhe:

modules/reach
modules/combat
combat/hitbox

combat/autoclicker
combat/aimassist
combat/velocity
modules/aura.class
Nofall.class
Min CPS
aimbotgui.java
aimboat.class
aimbot.class
autoarmor.class
autoarmor.java
clicker/setvalue
clicker.setvalue
java.lang.Thread
Click to self-destruct
SelfDestruct.class

Mountvol

[Bypass]

»» Aprire il CMD
»» Assicurarsi che si è nel C:\Users. (Se dopo Users c'è "utente" o un altra cosa bisogna fare cd...)
»» Scrivere mountvol
Vi appariranno delle stringhe (Esempio: \\?\Volume{5348501a-d444-48db-9dd1-b2db38367a1ff\) voi NON dovrete copiare le stringhe con scritto:
"*** NESSUN PUNTO DI MONTAGGIO ***"
»» Dopo aver copiato la stringa digitate "start (Incollate Stringa)" e vi si aprirà la cartella del volume che avete startato.
»» Inserite qualunque client dentro alla cartella ed ecco fatto il bypass

Nota Bene »»» Ricordate che se usate il metodo, vi consiglio di utilizzare con il client/clicker un altro metodo bypass, (Esempio: Wmic, Anche altri metodi)

[Detect]

1)

»» Rechiamoci su Regedit

»» Inseriamo la key Computer\HKEY_LOCAL_MACHINE\SYSTEM\MountedDevices

Nota Bene »»» Se è stato effettuato il Mountvol vi apparirà la/le stringa/e (Esempio: \\?\Volume{5348501a-d444-48db-9dd1-b2db38367a1ff\)

2)

Andiamo su Process Hacker

Processo »» Explorer

Filtro »» Regex (case-insensitive)

Stringa »» ^\\\\?\\.+.Volume.+.\\.+.$

3)

Andiamo su Process Hacker

Processo »» Explorer

Filtro »» Contains (case-insensitive)

Stringa »» \\?\Volume

Partizione

Questo metodo di bypass consiste nel creare una partizione e inserirne un cheat all'interno, in modo tale da avviarlo e poi eliminare la partizione per lasciare meno tracce possibili.

[Creazione Partizione]

»» Apriamo il CMD

»» Diskpart.exe

»» List Disk (Esempio : selezioniamo il numero di un disco con spazio disponibile)

»» Select Disk "Numero del disco che ci interessa*

»» CREATE PARTITION PRIMARY SIZE=1000

»» Assign letter - "Lettera a caso"

Nota Bene »»» Una volta fatta mettiamo un cheat all'interno, lo avviamo e eliminiamo la partizione, vediamo come farlo.

[Eliminazione Partizione]

»» Apriamo il CMD

»» Diskpart exe

»» Select disk (selezioniamo il numero dello stesso disco di prima)

»» List volume

»» Select Volume "Numero del volume corrispondente alla lettera scelta prima)

»» Delete Volume

[Detect Partizione]

Possiamo trovare la creazione o l'eliminazione di una partizione tramite il EventVWR, andando a cercare in un registro relativo troveremo

4 risultati di eventi risalenti alla creazione e all'eliminazione di una partizione con ID: 114/115/116/117 (Esempio), vediamo ora il registro e come utilizzarlo.

»» Visualizzatore Eventi

»» Registri applicazioni e servizi

»» Microsoft

»» Windows

»» VolumeSnapshot-Driver

»» Filtro registro corrente

»» tutti gli id

»» 116 (oppure "117")

CACLS

[Modifica di sicurazza]

La modifica di sicurezza consiste semplicemente nel modificare i permessi di una cartella (Nel 90% dei casi del "Prefetch") per impedire che essa venga modificata.

Per esempio : tolgo i permessi alla cartella "Prefetch" e subito dopo avvio una Koid.exe, in questo modo nel "Prefetch" non si creerà il
file .pf della Koid, infine restituisco i permessi alla cartella per far credere allo staffer che non sia successo nulla.

Possiamo effettuare questo metodo in due modi diversi:

Il primo metodo è il "Calcs" che consiste nel togliere e poi restituire i permessi a una cartella tramite due comandi dal CMD, vediamo quali

»» 1 comando : Cacls C:\Windows\Prefetch /p "Nome:r"
(serve a togliere i permessi)

»» 2 comando : Cacls C:\Windows\Prefetch /p "Nome:f"
(serve a restituire i permessi)

Nota Bene »»» Dobbiamo sostituire "Nome" con il nostro nome utente.

Il secondo metodo è "Manuale" e consiste nel togliere e poi restituire i permessi a una cartella tramite le sue Proprietà, vediamo come:

»» Proprietà

»» Sicurezza

»» Avanzate

»» Autorizzazioni

»» Selezioniamo il nostro utente

»» leviamo tutte le spunte

»» Applica

Dopo di che possiamo avviare il cheat e restituire i permessi al prefetch, nella maggior parte dei casi questo metodo viene fatto alla
cartella Prefetch per non far caricare appunto i file .pf, vediamo ora come trovare una modifica di sicurezza fatta a una di queste due cartelle.

[Detect Modifica sicurezza]

Possiamo trovare una modifica ai permessi alla cartella Prefetch e l'orario in cui è stata fatta tramite il Journal, filtrando con l'ID
della modifica di sicurezza, inseriamo questa stringa.

Stringa »» fsutil usn readjournal c: csv | findstr /i /C: "Ox00000800" /i /C: "Ox80000800"
| findstr /i /C:"Prefetch" > Security.txt

Nota Bene »»» Filtrando in questo modo ridurremo i false flag possibili, ma potrebbe capitarci comunque qualche false flag che contiene
la parola "prefetch" nel nome come ad esempio "WinPrefetchView", quindi noi facciamo caso solo ai risultati in cui esce come file name solo "Prefetch".

Nota Bene »»» I primi due risultati sono risalenti alla modifica sicurezza che avviene quando una volta acceso il pc noi entriamo per la
prima volta nella cartella "Prefetch" (infatti se ci facciamo caso ci chiede i permessi di amministratore per visitare la cartella), quindi

i primi due risultati vanno sempre esclusi se sono stati fatti allo stesso orario, se invece abbiamo più risultati in orari diversi allora possiamo bannare l'utente.

W-Mic

Il Wmic è un metodo di bypass che consiste nel non far apparire l'avvio di un client, andando ad eseguire un *Type" su un file diverso dal cheat stesso e aggiungendo uno "Stream" alla fine della directory di quel file, vediamo meglio con un esempio.
Voglio avviare un presunto "Cheat.exe", situato sul mio Desktop, facendo il type utilizzando il carattere speciale "╪", su un file pf chiamato *ACTIONURISERVER.EXE-A0A48DF6.pf"., che si trova nella cartella "BestSS", per farlo apro il cmd e faccio due comandi:

»» 1 comando : type C:\Users\%username%\OneDrive\Desktop\Cheat.exe > C:\Users\filip\OneDrive\Desktop\BestSS\ACTIONURISERVER.EXE-AA0A48DF6.pf:╪

»» 2 comando : wmic process call create C:\Users\filip\OneDrive\Desktop\BestSS\ACTIONURISERVER.EXE-A0A48DF6.pf:╪

Nota Bene »»» Lo stream è quello che si trova dopo i ":" alla fine della seconda directory, nel nostro caso è la "╪" ma può essere fatto con qualsiasi carattere, i metodi che tratteremo funzioneranno per ogni tipo di carattere

»» 1 metodo (Regedit)
Per fortuna è possibile trovare il file su cui è stato fatto il Type, vediamo come trovarlo dal Regedit.

Inseriamo questa directory nella barra di ricerca del Regedit:

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\

E cerchiamo in queste sottocartelle una directory con uno stream.

Nota Bene »»» Se troviamo la directory di un "type" non è per forza detto che l'utente abbia effettuato il metodo durante questa sessione di gioco,

ma è comunque uno spunto interessante per il nostro controllo, vediamo ora come verificarlo tramite i prossimi metodi.

»» 2 metodo (Explorer)

Ora vediamo come trovare il file su cui è stato fatto il Type utilizzando process hacker e il processo "Explorer.exe"

»» Explorer.exe

»» Properties

»» Memory

»» togliamo hide free regions

»» selezioniamo 4 al posto di 10

»» spuntiamo tutte le caselle

»» filter

»» Regex (case-insensitive.)...

»» ^[A-Z]:\\.+:

Scendiamo verso il basso e cerchiamo risultati in cui compaia una directory con i ":" alla fine, che risalgono alla directory del file su cui è

stato fatto il type.

Nota Bene »»» Se troviamo più di 4 risultati uguali possiamo bannare l'utente.

»» 3 metodo (Dps)

»» -s dps
»» Properties
»» Memory
»» togliamo hide free regions
»» selezioniamo 4 al posto di 10
»» spuntiamo tutte le caselle
»» filter
»» Regex (case-insensitive).
»» ^!![A-Z]+(.*)[A-Z]:

In questo modo ci troveremo spesso davanti a un solo risultato, ovvero il file su cui è stato fatto il type, in caso contrario non troveremo nulla.

Nota Bene »»» Se troviamo anche solo un risultato possiamo bannare l'utente.

»» Altri detect:

»» Il primo detect che possiamo utilizzare è andando su eventvwr e seguendo questo percorso:
Registri Applicazioni e Servizi > microsoft > windows > Wmi-Activity > Operational > 5857
Questo metodo non è preciso al 100% ma possiamo capire da qui se c'è stata attività del Wmic

»» Il secondo detect è quello di utilizzare AlternateStreamView, un tool che trova gli stream,
Filtreremo nello scan C:\ in modo da filtrare tutto il disco.
Compariranno dei file chiamati "Zone.Identified:$DATA" che non vanno considerati e file chiamati con lo stream.

Pesi Mod e Sha-256

Ecco qui moltissime mod con i loro rispettivi pesi e scendendo giù troverete tutte le sha256 delle versioni di minecraft (fino ad 1.16.5)

StatusEffect: ~ 24-26 kb
DirectionHud: ~ 23-24 kb
BspkrscoreMod: ~ 193-195 kb
ToggleSneak ~ Minore/uguale di 24 kb
TcpNoDelayMod: ~ 4-6 kb
TimeChanger: ~ 14 kb
CpsMod: ~ 7.6-10 kb
Batty'sCoordMod: ~ 17 kb
FastCraftMod ~ 179-183 kb
Pesi mod:ArmorStatusHUD v1.26 >> 25-27 KB
ArmorStatusHUD v1.27 >> 25 KB
ArmorStatusHUD v1.28 >> 26-27 KB
ArmorStatusHUB [1.8.9] >> 29-30 KB
Autotip (V2.0.2) >> 57 KB
BattyCordinates >> 14 - 19 KB
BetterFPS Mod >> 18-62 KB
BetterFps-1.0.1 >> 62 KB
BetterSprint >> 70 KB
BetterSprinting >> 65 KB
BiomesOPlenty >> 5.652 KB
BspkrsCore v6.14-v6.16 >> 193-196 KB
BspkrsCore [1.8.9] >> 62 KB
CheatBreaker HUD v4 >> 35-36 KB
CheatBreaker HUD V3 >> 33 KB
CheatBreaker HUD V2 >> 27 KB
CPS Mod v1.1 >> 8-10 KB
Core >> 194 KB
CoordinatesMOD >> 31 KB
CoordsMod v2 >> 11 KB
Custom Crosshair Mod >> 32-64 KB
DirectionHUD v1.23 >> 24 KB

DirectionHUD v1.24 >> 23 KB
Fast Chat >> 4-5 KB
FastCraft Mod >> 115-183 KB
FastRecraft Mod >> 3 KB
FPS Plus >> 147 KB
FPS Spoofer >> 9 KB
In-Game Account Switcher >> 66 KB
ItemPhysic >> 31 KB
Keystrokes mod v1-2 >> 11 KB
Keystroke Mod v3 >> 13-14 KB
KeyMod 1.1 >> 59KB
Legacy Java Fixer >> 7 KB
LunatriusCore-1.7.10 >> 57 KB
MemoryFix (0.3) >> 12 KB
MotionBlur Mod >> 7 KB
MouseDelayFix >> 5 KB
OldAnimationsMod v2.3.1 Classloader >> 72 KB
OldAnimationsMod v2.3.1 >> 2.209 KB
OldAnimationsMod v2.4 >> 1.437 KB
Optifine_1.7.10_HD_u_C1 >> 929 KB
OptiFine_1.7.10_HD_U_C1 >> 849 KB
OptiFine_1.7.10_HD_U_D3 >> 1,166 KB
Optifine_1.7.10_HD_U_D4 >> 1,167 KB
Optifine_1.7.10_HD_U_E7 >> 1,733 KB
Optifine_1.7.10_HD_U_E3 >> 1.626 KB
Optifine_1.7.10_HD_U_D8 >> 1.599 KB
Optifine_1.7.10_HD_U_D7 >> 1.579 KB
OptiFine_1.8.9_HD_U_H2 >> 1.314 KB
OptiFine_1.8.9_HD_U_H6 >> 1.686 KB
Optifine_1.8.9_HD_U_I7 >> 1.969 KB
Optifine_1.8.9_HD_U_I3 >> 1.840 KB
Optifine_1.8.9_HD_U_H8 >> 1.773 KB
Optifine_1.8.9_HD_U_H7 >> 1.747 KB
Optifine_1.8.9_HD_U_H5 >> 1.616 KB
PerspectiveMod >> 32 KB

Physical Items >> 36kb Lite - 48 KB
Ping Display Mod >> 9 KB
PlayerAPI >> 260-276 KB
PotAlerts Mod >> 29 KB
Potion Counter Mod >> 9 KB
QuickSW >> 4 KB
ReachDisplayMod 1.0 >> 9-10 KB
ReiMinimap Sem Entity / Player Radar >> 178 KB
Saturation Mod >> 39 KB
Sidebar Mod 1.01 >> 10-12 KB
Spinner CPS Mod >> 47 KB
StatusEffectHUD v1.26 >> 23 KB
StatusEffectHUD v1.27 >> 24 KB
StatusEffectHUD (Max) >> 26 KB
ShinyPots >> 5 KB
TabbyChat >> 379 KB
TCPNoDelay >> 4-6 KB
TimeChanger >> 15 KB
ToggleSneak / ToggleSprint >> 21 KB
VoxelMinimap sem Entity/Player Radar >> 466 KB
ToggleSneak >> 20-30 KB
StatusEffect: ~ 24-26 kb
DirectionHud: ~ 23-24 kb
BspkrscoreMod: ~ 193-195 kb
ToggleSneak ~ Minore/uguale di 24 kb
TcpNoDelayMod: ~ 4-6 kb
TimeChanger: ~ 14 kb
CpsMod: ~ 7.6-10 kb
Batty'sCoordMod: ~ 17 kb
FastCraftMod ~ 179-183 kb
ArmorStatusHUD v1.26 >> 25-27 KB
ArmorStatusHUD v1.27 >> 25 KB
ArmorStatusHUD v1.28 >> 26-27 KB
ArmorStatusHUB [1.8.9] >> 29-30 KB
Autotip (V2.0.2) >> 57 KB

BattyCordinates >> 14 - 19 KB
BetterFPS Mod >> 18-62 KB
BetterFps-1.0.1 >> 62 KB
BetterSprint >> 70 KB
BetterSprinting >> 65 KB
BiomesOPlenty >> 5.652 KB
BspkrsCore v6.14-v6.16 >> 193-196 KB
BspkrsCore [1.8.9] >> 62 KB
CheatBreaker HUD v4 >> 35-36 KB
CheatBreaker HUD V3 >> 33 KB
CheatBreaker HUD V2 >> 27 KB
CPS Mod v1.1 >> 8-10 KB
Core >> 194 KB
CoordinatesMOD >> 31 KB
CoordsMod v2 >> 11 KB
Custom Crosshair Mod >> 32-64 KB
DirectionHUD v1.23 >> 24 KB
DirectionHUD v1.24 >> 23 KB
Fast Chat >> 4-5 KB
FastCraft Mod >> 115-183 KB
FastRecraft Mod >> 3 KB
FPS Plus >> 147 KB
FPS Spoofer >> 9 KB
In-Game Account Switcher >> 66 KB
ItemPhysic >> 31 KB
Keystrokes mod v1-2 >> 11 KB
Keystroke Mod v3 >> 13-14 KB
KeyMod 1.1 >> 59KB
Legacy Java Fixer >> 7 KB
LunatriusCore-1.7.10 >> 57 KB
MemoryFix (0.3) >> 12 KB
MotionBlur Mod >> 7 KB
MouseDelayFix >> 5 KB
OldAnimationsMod v2.3.1 Classloader >> 72 KB
OldAnimationsMod v2.3.1 >> 2.209 KB

OldAnimationsMod v2.4 >> 1.437 KB
Optifine_1.7.10_HD_u_C1 >> 929 KB
OptiFine_1.7.10_HD_U_C1 >> 849 KB
OptiFine_1.7.10_HD_U_D3 >> 1,166 KB
Optifine_1.7.10_HD_U_D4 >> 1,167 KB
Optifine_1.7.10_HD_U_E7 >> 1,733 KB
Optifine_1.7.10_HD_U_E3 >> 1.626 KB
Optifine_1.7.
10_HD_U_D8 >> 1.599 KB
Optifine_1.7.10_HD_U_D7 >> 1.579 KB
OptiFine_1.8.9_HD_U_H2 >> 1.314 KB
OptiFine_1.8.9_HD_U_H6 >> 1.686 KB
Optifine_1.8.9_HD_U_I7 >> 1.969 KB
Optifine_1.8.9_HD_U_I3 >> 1.840 KB
Optifine_1.8.9_HD_U_H8 >> 1.773 KB
Optifine_1.8.9_HD_U_H7 >> 1.747 KB
Optifine_1.8.9_HD_U_H5 >> 1.616 KB
PerspectiveMod >> 32 KB
Physical Items >> 36kb Lite - 48 KB
Ping Display Mod >> 9 KB
PlayerAPI >> 260-276 KB
PotAlerts Mod >> 29 KB
Potion Counter Mod >> 9 KB
QuickSW >> 4 KB
ReachDisplayMod 1.0 >> 9-10 KB
ReiMinimap Sem Entity / Player Radar >> 178 KB
Saturation Mod >> 39 KB
Sidebar Mod 1.01 >> 10-12 KB
Spinner CPS Mod >> 47 KB
StatusEffectHUD v1.26 >> 23 KB
StatusEffectHUD v1.27 >> 24 KB
StatusEffectHUD (Max) >> 26 KB
ShinyPots >> 5 KB
TabbyChat >> 379 KB
TCPNoDelay >> 4-6 KB

TimeChanger >> 15 KB

ToggleSneak / ToggleSprint >> 21 KB

VoxelMinimap sem Entity/Player Radar >> 466 KB

ToggleSneak >> 20-30 KB

1.7.2_OptiFine
507fb3660e77ab1a3000424d9b08c61606ae1e5a9be41caa3728bddd9597365f

1.7.10_OptiFine
a4fc2284657544e0f4bcc964f927c2fda3e3a205178ed1d5d58883aaf9780cce

1.8.0_Optifine
ccccd0a92f76fbb24279691daad9b67f85d80471a37e59e0da76d7754982dfe8

1.8.1
66a749ad95adcb929439155c0341309e89e437444867e108dcb36fd16493b0bd

1.8.2
5cc5b24312f3d182bf06e7f1a4da3a05ce94be6c861d5c9995c86e6d8811fbe9

1.8.3
a4fc2284657544e0f4bcc964f927c2fda3e3a205178ed1d5d58883aaf9780cce

1.8.4
d68a3aa5271abece4ce2b7048f6caf4f58071476344d9a52fe9ab1410c5d458b

1.8.5
2d825073de0da4383c0525e81d181ec81f92d17daa2f0b81faff3850492e461d

1.8.6
e597384cf964950b02650a39f73c2cbf5ce9e51d934cdfa1291530896e7cf100

1.8.7
2e45066ec194c6daec5f7dbb27822ef0b5855d5829f62392906620145689a3e0

1.8.8_OptiFine
9481ed51d7fc4be54ec38c509f84124fbac5d9fea238bbde5b2e6c4f753b1ac8

1.8.9_OptiFine
14f0d96d1a56fb4f5c3b2233d00699525893fe5ce3dcf181e7de59120595d298

1.9.0_OptiFine
0273b5c79d6b96799c6480ae61366d6b1d042655970de87f77f1a3f1ebea9307

1.9.1
56ad7e53f6f4ad393844e274aa2190692b61d2ad9f6b3d12b33a8b7332fd51f9

1.9.2_OptiFine
ef87eb71250df1b871deab8d3ef10aac3290b9e78667ad548fde4d0e14af0d65

1.9.3
ab8fdde789c5b4614ffc98249e04fdcce7dfce320b55215bfe5418608af6a63b

1.9.4_OptiFine
23e90103a1ca2ac71100004c6d5846de09f85695f579843ef8da41571e60c908

1.9.5

1.10.0_OptiFine
c00f8170ebf4fd834f552246743a64885a6dffb3dd1e3a3f3dba9676b7a0af35

1.10.1
338b205f20c22b9c676d9d3227a5e6c5e190f30ad84d7caad035150b3e05ba72

1.10.2_OptiFine
7cdf7fcdc1c92584a233bf3c42bd7f0df1bdad3007d306831fe50410692be1e9

1.11_OptiFine
f0d11987ea743f55a2c03bf77216e6dc9baea7201cc7bf498ceb18043e984634

1.11.1
eff72a31339cd9a96a61092eed2d95b95e4cc91516bea4e9105c3d73574147f6

1.11.2_OptiFine
be3fff4f2cc005a1310a96389efdeb983d2bcb4b8e747c402acd616ae73d0ba2

1.12_OptiFine
59e84cf6acc3912e1705ab05c722485afb3ec33343eef4756d8c16edfe6411ca

1.12.1_OptiFine
19331fb29bf8b8d5ed764677c94cca9d66481e10104f660eb555894a4300cf22

1.12.2_OptiFine
8ada07da5ee77dad3527bd7278fbd05ee1fc8a597813b216a871a2d7d64cc64f

1.13_OptiFine
d807a5ed9428b6c16b64888fd2b7fa76dcf5c55d06f96f7c0c47762c3fc3e26e

1.13.1_OptiFine
f0b4cf6d1a87ae150f87a535651138ca7b82bdad8853f76e7ddbff1dd610ac87

1.13.2_OptiFine
3410887ba652f25792c7675bfaf9140e73b60e93cfbf113a803f8a98cb05c0f9

1.14.1
7194d1326cf796f62ac55f3cb56f851c232895639ae27510f3207d5a73f91814

1.14.2_OptiFine
9b740c9fd4955981125ebd3cd086baa8b4392963d043a3480b5b942a96637c25

1.14.3_OptiFine
40630626774339 88e012fba53e42e4c21adb6919ac7f061f19f3c6e75b334e07

1.14.4_OptiFine
b3b2a798e2d67b566008fe4a03767ae2c7ff3f8c7ba6751e7b71fc7299672d0a

1.15.1
6e28ecd008d0ca5e1dcd346dbc2882430f02a77a78864d57acc49fc8bc1b5358

1.15.2_OptiFine
4a73008a73f3824b7c711750a5a37556df8614f193c0a531e292dad159a73a7c

1.16
00740ef4475d4cd0a1d7064f89602f759c45ff9afe29da9b0ee0b9037ebb2a71

1.16.1_OptiFine
b4831e7b63b10588ff06ea86322108d916c536446f3aea3ae988b7fe3e1f66ef

1.16.2_OptiFine
19960f4e3c60f2723f361844d2b4020b8bf2160bd91a1e1efde8ce5aea4ff73d

1.16.3_OptiFine
da85197babd989a7de318774cf5d97bcef95e89a70c9fa9a4c8180463e9589fa

1.16.4_OptiFine
d6740464ee2bdf37d285c5d368d2e16497492427fb5783e2db3482bbf0079ed0

1.16.5_OptiFine
00b5ebbc33e95ea88c1ab80601599c9827e9aa861d93ccc2cfcbbfd996e86263

OptiFine_1.7.10_HD_U_D4
1ce3a1ab348aac5cfe70fbc60496146c594faa21bb1bc5fc73dfb16432108940

OptiFine_1.7.10_HD_U_D3
a5a99de3615acfe0171cde06dfdd8ed1308b534a58b4617d99c0fe39887040be

OptiFine_1.7.10_HD_U_D6
415cba487ea5eddca981c6a00a5426236f8df36c635f5808aba227ad96d1b478

OptiFine_1.7.10_HD_U_D7
80695aafaa471eaf51507901cc242f1d4564c4e10d81d01c5a162215c788733f

OptiFine_1.7.10_HD_U_D8
cc5a3c4d7b169cc0b0899f8304360b38e69d34311546e1b36631fb2c6a44f742

OptiFine_1.7.10_HD_U_E3
1dc0f1fe2614c5354292473e44649f90508ae069d249550ee4d9ce794ea8f0bf

OptiFine_1.7.10_HD_U_E7
8bcd9d83de001a0591f498105f369f070c47d2c9192774d5a5b69f646e44fab4

OptiFine_1.8.0_HD_U_I7
d3d9168f06ad10e033720348e41d6a56c874b5acdb321b0c90feb860e808e0c5

OptiFine_1.8.0_HD_U_I3
20ab62ca61874c9bf5e1dc2a66795182a43021f45b116b2675eae489d
e6e4a9d

OptiFine_1.8.0_HD_U_H8
8d862d71ccac7e93abedafe9a50f045f0db3e41599bbe1e978f125e22
c346d9a

OptiFine_1.8.0_HD_U_H7
0a22202f839b091e06a515f6b52d6fcfb0e6860868801fc7d34a6fd85
747cd53

OptiFine_1.8.0_HD_U_H6
b10b3f73f6b0d815e97f87abbac3cdef7c24d9414c023a2e8d72c6afe
d8f0dc6

OptiFine_1.8.0_HD_U_H5
8551257e8000f735a5a3fde96e7e36ba7028ef91c2959683138000c69
533d745

OptiFine_1.8.8_HD_U_H8
446eb1067d44a004b8940416c22020acd44d9012eef46275d6e8c4b2e
87b1d7f

OptiFine_1.8.8_HD_U_I3
ddc9c2ae7e771416abfbbed288e09076657e580ab9125b81627e0efaa
f07af64

OptiFine_1.8.8_HD_U_I7
5e792a05d932a89353d5bc1be58a989c0d48b81477926a154d9c4fa15
7558a74

OptiFine_1.8.8_HD_U_H7
476eb23bf24d4d48dfee41723e9c196b3b947e525ced5cde73b76256b
3dd49aa

OptiFine_1.8.8_HD_U_H6
e9b11adaf4adc1fd4c0681a94f0548cd2d98942176f8842e82a057aee
94e8230

OptiFine_1.8.8_HD_U_H5
f9e29775670bcf94860c9c80beb91b62a70e958dedd2ea483624b7a97
b7dac9a

OptiFine_1.8.9_HD_U_M5
2739760a70fca6ae5c7dc817bcc6283f18f55e38fa23778da7f387a6b
724b2c4

OptiFine_1.8.9_HD_U_L5
b442bf55e4c703c55f5f48055d79c07eb853fcb76fa88f85587e911af
4f2b084

OptiFine_1.8.9_HD_U_I7
778f1aa163c4d1e3f1a5a45436da7801b54ee30f3bc2345c1f0ac5c06b6b4d62

OptiFine_1.8.9_HD_U_I3
4959e003c0199cf178a25dac24a06e2404145cabc6f7e2d0b15ec8549f80d0b3

OptiFine_1.8.9_HD_U_H8
b6785e65bb8c1dd277bbb5830196022ec4f9b232c72caff5b5d0f24ea4aa09c2

OptiFine_1.8.9_HD_U_H7
9b61d1c1b930353525c4a9891d7523a614e838c1b9a04f12d16bf8425699042c

OptiFine_1.8.9_HD_U_H6
24030c73daaab3d24485b266229d426244956a88226d98ac19777ff348ec0e30

OptiFine_1.8.9_HD_U_H5
fa8a6c5aefeef9753d164bd8dd681a30a403f24e2249479a774da7fce28f4c23

OptiFine_1.9.0_HD_U_I5
36b5a8d5836f2c5ac68a2da37a6f12830ae35882d5a84e8828e6a40a43dad1db

OptiFine_1.9.0_HD_U_H5
5cc9499e4c771e86da9b24191327d9aa5befdcd887dd466896ca5b850e149601

OptiFine_1.9.0_HD_U_E7
f0aa3ad69f3c950dd02d5df6f8408de1768becb2da670b002d8c816c2e5d53d8

OptiFine_1.9.0_HD_U_E3
0a70a7fde63bb64351bee74f48bb1ed49bb1e24f4924e300b07dd36030c8fd80

OptiFine_1.9.0_HD_U_D8
b99007eacc6916370b9ebd52c38213c472b4a5347dcc6a1de2c7fdafbcef58de

OptiFine_1.9.0_HD_U_D7
efb4e5482430dfacd6554abed12ae6bb0f315729fc1089fe4b79458d1c10bb48

OptiFine_1.9.0_HD_U_B5
e7da9234c57bb300aad88b3cd1ddbd9b9b7e724eab979db4a0ba102a345cd8bd

OptiFine_1.9.0_HD_U_B3
5df53e75096dbff81294ca52e8406725a6c32495680b67906536dce78c6b3c0b

OptiFine_1.9.0_HD_U_B2
a51ad036ddf9f0d8286a3b996e4173542864cb1c58af3cfb1f73101f6b8cd0ba

OptiFine_1.9.0_HD_U_B1
68f7016b651bc3cfd8d04d46f674e07c557ccfaac391ec246c2d0fced47ae1b1

OptiFine_1.9.2_HD_U_B1
564484d61685d944fbddfc5faca284bec35542765188fb9e7703af1870c62af8

OptiFine_1.9.2_HD_U_B2
e36c71638786ce0b76975d3e26e62eb68615f7db9b3b992c55b75f8bba6d93b5

OptiFine_1.9.2_HD_U_B3
4904f392550ce03761415269a24bff8ad3ece7630aca3537fa08957f0d2355e8

OptiFine_1.9.2_HD_U_E3
37b367332eefc4c78daa1225b64a6bf659a8aaa9d5ea16b7e29a935234ecfead

OptiFine_1.9.2_HD_U_D7
67d8134634c90db7d5bc158744c86b23d62c8d010a94c360b9d9b42534cb9588

OptiFine_1.9.2_HD_U_D8
59d9d5f83b5d0f59952e9b54abbf59588f64f815b5d9661e54ee769341df99a5

OptiFine_1.9.4_HD_U_B4
48bf477961b8c658273a7393c9999eb31439b4712db2edfea626c74e8533f85c

OptiFine_1.9.4_HD_U_B5
aa083413535264417ab0c277d0a296d79cd1e548f4f5ba494e03baa7cbb02601

OptiFine_1.9.4_HD_U_B6
63594d2b448673fc31ae1d82630453fa7b0d2b12d2be3ddaae9a6d2e35a9adc7

OptiFine_1.9.4_HD_U_E3
58d7297cca20fce29faf63e13445910bffb3e6c523de137f32585af53107dfbc

OptiFine_1.9.4_HD_U_E7
28bebdf461807f6005702f3361cafb47b5f17c1684eedcfdc2c5ee7b9c3b8593

OptiFine_1.9.4_HD_U_H5
0462daff5cd87a97cd9767808cb8bee148d65207629da1386560b8d3b8fc62c3

OptiFine_1.9.4_HD_U_I5
b7e3b121fd1397f359c544e5f8b1a759152113067ebf18997e1725c4401feb22

OptiFine_1.9.4_HD_U_D7
4ac5421fc94128e7e5e2725b63232c0c7bc9bd89da2e6efd791ddc2887c8f03f

OptiFine_1.9.4_HD_U_D8
e1d0d89391fe5505fbeba068333b2b985354d1a420f4f34ca9bc8b12ba456e87

OptiFine_1.10_HD_U_I5
a0a3ac68d16738a7e158b0c3606ff467887f6420edc89592f4b5cf68a000a5cd

OptiFine_1.10_HD_U_H5
0780a17c3d3697288e5e5e2bacc575fcca8128ad0c316ce643d8a67623da43d2

OptiFine_1.10_HD_U_E7
870d886113ac4f84dad70d33902ad5ce069f3bda603e43675be9265cedef4809

OptiFine_1.10_HD_U_E3
9f1cc1a58a0893d5f6a017b8b364f4966f93ecda4e82a1b27184fd90ba24b131

OptiFine_1.10_HD_U_D8
a21ece99d096d41b9ddc3220b4259bc6e71c3a6070bc8f59769db7851587dce5

OptiFine_1.10_HD_U_D7
7a290b5af4a5bf153a9dfc23cf1c02cdcb97be9f2aaee93d085158304a05837f

OptiFine_1.10_HD_U_C1
60db41a9609f5fe57f570bb6d8b4d936a53fa81a1829f1e39301e5a71d51444d

OptiFine_1.10_HD_U_B7
1f9a84c75eae9773a2b988fc7da73248bfcc90d89339fb01f5e013f6f1ee270e

OptiFine_1.10_HD_U_B6
ddc8d07f7b55f1be5a54d1f2488e925957b60278c4b107ea42e4d92a7cfa9866

OptiFine_1.10.2_HD_U_E3
5f7fca5b48e9cee4c032d6df75ef537954d36f4b6df53050e82aa47b4aea0516

OptiFine_1.10.2_HD_U_E7
2145fb35cf4dbe343d252a045534ba5ef4e6354e67acce73117ca89279414046

OptiFine_1.10.2_HD_U_D3
7d99694ccf0836e69e470949989a182c3d23725d521924b35a3d2fb15e3ed69d

OptiFine_1.10.2_HD_U_D8
c812c3648ef4c2aeb75a6abc90b419bd7cf8be85e5563be9c574962d81a5222f

OptiFine_1.10.2_HD_U_D1
6c4ee9d709617293b623ad3ee9621b9c8f28c1430e1ac86e04baa3da47647f64

OptiFine_1.10.2_HD_U_H5
67005964e4cd3219af28f2e22e0d4d5137964516ff6c0c1479b05d896eed4bd0

OptiFine_1.10.2_HD_U_D2
1107a06247175298ac93748c295169d52d0136478c26c21d90d3280032e0d3f8

OptiFine_1.10.2_HD_U_D7
c088dee95cfadd135f1676f4f05ca2791be75e473a82b84f657f9591c3804429

OptiFine_1.10.2_HD_U_C2
232fb8d311b618b9fad2d3c605fc559994b119eac1120f9def20e73c34738ced

OptiFine_1.10.2_HD_U_I5
ee9458d0b08ea8ca020e8e56c513ca5c08477505df9fb2e8c66a225819ee0554

OptiFine_1.10.2_HD_U_D4
0ded07229d7db672a5694203a39d8f880e031a019adf23d26d9137e5bf4ab1a6

OptiFine_1.10.2_HD_U_D6
bb84c3a22ef23801fb661f7657bafc0e040e6bac03968d181145831c69081808

OptiFine_1.10.2_HD_U_C3
dce89b3a81d30b00ba8ba636aeb21d602096197b51dded0bedebb4b95cc88eda

OptiFine_1.10.2_HD_U_C1
9f79c07983699e72dda93a4666aaa0e43013c29f8f4dd38c43dd97d6e1e10a12

OptiFine_1.11_HD_U_B1
06961414e0d0100fec8c7441823cc65b9d986fd7ee97af5a334f02e0ef4dcad9

OptiFine_1.11_HD_U_B2
3dacc83efcb024ad80388c294873e22e4ff698ed68a3f51d9cff83ed419e6e1f

OptiFine_1.11_HD_U_B3
8d3bd2c3c6f7d75d5e171ceb249516d10e303939d2c4ac8f59a7474f633044e1

OptiFine_1.11_HD_U_B5
77a379ea8617684273abab179b04786a2fac11b954c5918a6b85751e2cd22ca9

OptiFine_1.11_HD_U_B6
94f3ccf93268a3a36d336f85dee3c5ce2d2bc5153b2fcf504c0f76bdaed66753

OptiFine_1.11_HD_U_B7
796ba91cca32e23704824167506f32eb10a7a33d0821eacf122347bac7faca76

OptiFine_1.11_HD_U_B8
850122310e4802899d9c91312f9056fd9a1b2bafc76935072569e501a10673ca

OptiFine_1.11_HD_U_C3
3dfaafb4d45f9a50933e973034cfc84afc4aac6e4311abd86480d1e74a25528c

OptiFine_1.11_HD_U_C7
faf3342478fc2dfd3aea71cf3653f96af12ddfc63d728444deefb349401819db

OptiFine_1.11_HD_U_F5
03e48d683e14e527ec981484dff4b3721ddf20c49296a10bba7f52219a4bf5b0

OptiFine_1.11_HD_U_G5
52b3495aabac5548ed528c002788e2e2377c96e7c6b681e241201cbab0b6efab

OptiFine_1.11.2_HD_U_B8
07cc65b3928b2252c065547c35dea2ca63f126185afb22bb61b8e0b27e972d1d

OptiFine_1.11.2_HD_U_B9
08fcacd5618e63922808fd9909cebfd5a20669fab0213ca8e3f78ccceb2c0659

OptiFine_1.11.2_HD_U_C1
1f3129cdeeb4675fcd8aa64cb89f7e177406cc826ba68f0bd85203187815c4e5

OptiFine_1.11.2_HD_U_C2
9d66e43b74b18582f8d51df242d35cb719040921f9c300506a08b037bdfdf2c9

OptiFine_1.11.2_HD_U_C3
dcb1008471905fd51e3d7dc0c9c6f0b43746c4cd5ca6b121cddc8cb54eb89372

OptiFine_1.11.2_HD_U_C7
065cd23754e5b4d3d3f6fccaf233906d1d724b38c7de32755328ab1c3085f97a

OptiFine_1.11.2_HD_U_F5
ec21dd70df5c28044d5d184cae55d41b344a109f914723c3b70fd695e103ce90

OptiFine_1.11.2_HD_U_G5
d6c2d406d3397b92c34d41424597fd51e1fa58e03ccd8e9302607d3c24b98afe

OptiFine_1.11.2_HD_U_B5
0f7c32f7a5f3b30c64f75f70c1bbf43d40b5bec2fde9b3324328b650bd12133b

OptiFine_1.11.2_HD_U_B6
649593889e39d25c7182107ad56b781dd5d103234c87402e9653075ef6c06f07

OptiFine_1.11.2_HD_U_B7
9e4c35c9c8017845bc307cab01ace956d6778f178b709a83d097dd5314766701

OptiFine_1.12_HD_U_C7
ae86406c2a33309bc4efbc556b8e72132421bf53db09fd8d4ac316c0641de342

OptiFine_1.12_HD_U_F5
e6856f93b1d60215a0e15711d5be071356a21a11fd42da6f96352d68ea8f1fc5

OptiFine_1.12_HD_U_G5
abdd900845376ab609b0048080b6ec97f2c298308337b23fe50f1ca335f88bea

OptiFine_1.12_HD_U_C2
b18c62762391fa0ee0cc90926d2b51967acd7261c8b12fbf2783c9cec4445182

OptiFine_1.12_HD_U_C3
31ca7b610077b7c9ffe585082933a5f5e8e35cee9bb2594dd689a9d7905580f8

OptiFine_1.12_HD_U_C4
2dd7fedffda9b41fbebc1d9f66d140b1e4cfe2c6fb845615118600302e2badfc

OptiFine_1.12_HD_U_C5
f69f4408c3c902e5c18669b88be749ee70bb75b7092f2869f17815697b907ed0

OptiFine_1.12.1_HD_U_C6
a15a45aaab47fb4c040a442a148b7215e768dcb49ec17b733a5f6f26dbecebd8

OptiFine_1.12.1_HD_U_C7
82390941574a4383bc01f20b4b556855d21bc1a6bb34f6826cf01fe7f6364d3e

OptiFine_1.12.1_HD_U_F5
7aaaaf6b94bb1993f16a03da7d6ed19d78c1c51b1f3ce060b030f99dc95b176d

OptiFine_1.12.1_HD_U_G5
f6c6eb92cd0814e82c42a19334ecc149ff39fa305b90140d16c2b86b6715c0ca

OptiFine_1.12.1_HD_U_C5
1c79ad3cf02530733a28a5dbffff2b53468da8772d5d21c804652ead900aec73

OptiFine_1.12.2_HD_U_C9
0ab6ff24829eeb06d8e00d33548be9ab9bf0191e5ad5e181bbcd5fbec23f3baf

OptiFine_1.12.2_HD_U_D1
f1dc628265459c1ddf47fd2f1fdef782a1652a2ac19bc2af2a9aa63cd3d11292

OptiFine_1.12.2_HD_U_D2
df8c66cf2698130b0386b39a2700a947c9b3645e04dd7aabea290909601983ae

OptiFine_1.12.2_HD_U_D3
33d535ea0f4e8c8456d09e7095113a6bc0d023e277396d2ad6d81b65301b3668

OptiFine_1.12.2_HD_U_E1
51b84cfb29b5e2a91298b17a64d535036fdbbd9ef77da0c4b49fdf2c2d02a9f1

OptiFine_1.12.2_HD_U_E2
88ba0f809282d4b1b0605d6e0fbb432c0fedd5636724d6dedf2ed3e8208c54cd

OptiFine_1.12.2_HD_U_E3
470f5a83a63bb2f0f361b84fe4bfad8423cb54d730f31dbb530d81b05f2d99dd

OptiFine_1.12.2_HD_U_F4
dc3442eca2fd116ea718909c078091bbe7f1a043e14d30449ed620090b1a80c4

OptiFine_1.12.2_HD_U_F5
fc70db439793b257228ad50dbb497dd50e33c3e08f7d0d6b2bba3a7d7c349619

OptiFine_1.12.2_HD_U_G5
3b0006797771feb97f2d0d2908ae7c9a78cefb2e730af1c2e85d08a839ba271e

OptiFine_1.12.2_HD_U_C5
246e950870a33f4c7f213faf6e4cd61f367d4930cdddc39b0045e9a57e3dea1a

OptiFine_1.12.2_HD_U_C6
b9f52bfa97c2b580f9a88c5994fb781c34bac04abeeb2e2f777432fdbc6ae10b

OptiFine_1.12.2_HD_U_C7
842f9e4e9225f0b980b59442a802bfa49777da6c3154e5c21d4bf8ebe13c9971

OptiFine_1.12.2_HD_U_C8
043966c34b0e9e8e50587447471e29e2b19249d85d2d522136b09ce8a0cd3903

OptiFine_1.13_HD_U_E4
83861f3922012a7019e44d610386fe379a3e79ddd5b9b1a4ca9fbe96aab51e75

OptiFine_1.13.1_HD_U_E3
b57a928c39f4c21d24a9394fe7d383500aed5600b9da7a2e8581922aeb4a157a

OptiFine_1.13.1_HD_U_E4
6395d60ff6839b4d51c34cfbdd039e9f087964a4d08218a7da28f2770738bd64

OptiFine_1.13.2_HD_U_E4
3a2e81b3fbd148cec5cdf501a8d138007affbf9fa5b99ac0aef1fdcabc45ee14

OptiFine_1.13.2_HD_U_E5
3c11d724f5ce017067e92dbb6131bc119333305292ef2e10c4f316f8fec75879

OptiFine_1.13.2_HD_U_E6
be2a7f07d5f90da43a4d0c8d517924088f592486e8f02857e06c9d58d839dddd

OptiFine_1.13.2_HD_U_E7
0ad0c5c222ec810328e90642e4e8e9c0d45f725e61989ca43325e7502bc4e306

OptiFine_1.13.2_HD_U_F5
065938b02c8d2d3e0441fe4e87815a42f45b9ffc9781a6d0b596d84e126bee78

OptiFine_1.13.2_HD_U_G5
b23510a2df1f3dd6d94e22eab7e7b16c5e53f242396cb41ebeeedab56f57bb71

OptiFine_1.14.2_HD_U_F1
c81a76d7e00169aae51f14b48ddcee3310723175d37d43cab69652f4d1688518

OptiFine_1.14.3_HD_U_F1
c80cad3ca5c09413b3fb33a04981fb7d9cd2909270e77d3cf351ccd02549a175

OptiFine_1.14.3_HD_U_F2
50e21bcff95d3c0645a23ddfdea4287e8f44a8bb5578292461dabd7a93d09e03

OptiFine_1.14.4_HD_U_G5
23eeb9bd03bac86e0043464b01f5fbdc89ac14a010913cab20e9d01e575389bb

OptiFine_1.14.4_HD_U_F5
053606de560f9ee47baf646b37239ca4fcca4331235e09dbe7f8250f0ab197fc

OptiFine_1.14.4_HD_U_F4
66df1c3b02d62cf7149992b576e34ee0a37170f68613b4d9ab5be08c792154f2

OptiFine_1.14.4_HD_U_F3
b3c3a36a3a9a8de78423c9de84b03b35ffe6202cd7579c401e45f4f544e9d312

OptiFine_1.14.4_HD_U_F2
f8c0a0b46ef5764bfab0b542673e62e392ff2ef0d71dd45c7b0d929c0dcc8aff

OptiFine_1.15.2_HD_U_G6
04afd60dfef413e4cd7d1b4248e7aca78126cae3bcb83135374503048 7371f83

OptiFine_1.16.1_HD_U_G2
bb38be37e2c7b26776a6fd6aede86f9dcdcfb00d4ebd74d7ec54a0dec6ee8bbf

OptiFine_1.16.2_HD_U_G5
a23369e9ee93b2e33b5850817605886d7952dfa2d1269dd5208b9f8931025bc5

OptiFine_1.16.2_HD_U_G3
c72f68b911dc0b1a1e2678c2178a84b0f5cf00a3e533e20dccecdb620fb3acba

OptiFine_1.16.3_HD_U_G3
39e3b20ac72135f857a1515e8843f64037f62ed60a7ea917bf4ab9c483f4b06a

OptiFine_1.16.3_HD_U_G5
f44557c3130ec32d26719bf6c9d8ee3d7b6d95af80d04869e645ed2ccfc9375e

OptiFine_1.16.3_HD_U_G4
989aea30e9cbb1422956d1a5d5418c20da82e7715c507a7d508c9d8b09aeadff

OptiFine_1.16.4_HD_U_G6
0715d49206ba4674e18a5cee78a83fc7dcc2e39426e145169e14698f1a658384

OptiFine_1.16.4_HD_U_G5
6e6e01f63f53d15f814d894a6bc9714f778f343aa7323ab93a25267744be1b89

OptiFine_1.16.4_HD_U_G7
106df3f7e5d8a039ed51dded95115d316b040058881de19b7bb2e00fab6b7f18

OptiFine_1.16.5_HD_U_G7
8066b7de597bb06ad30779a5e01dacc5c60487883b0fbd6419a88f38f099f028

OptiFine_1.16.5_HD_U_G6
8a717d779878954bdad8ac961041343fe155d942705c3eed98f0e057a40c3e8b