



This guide is designed to provide a clear and accessible overview of essential SS knowledge. Created by the RedLotus team, it is an ideal starting point for those who wish to delve into more advanced methods at a later date.

Why is this guide important?

Ensuring a solid and consistent understanding of the topics covered is essential for promoting effective learning. This document provides a structured foundation that prepares readers to tackle more complex content, whether through webinars or in the forums of our community.

How did this guide come about?

The guide originates from a series of videos I, ItzIceHere, published on YouTube, initially intended for the Italian community. The videos, recorded in Italian, offer detailed explanations of the methods presented, but creating versions in other languages would have required a significant effort.

For this reason, I have chosen to create this written guide, which can be used either as an alternative or as a complement to the videos. Thanks to the automatically generated subtitles on YouTube, the videos remain accessible even to those who do not speak Italian, but this guide allows for a more precise following of the visually presented concepts, providing a clear and structured reference.

The project was also made possible thanks to the contribution of Omqr and StrqfeToggled, who transcribed the video content. I then reorganized and refined the material to create the document you are reading

The added value of video support?

Purely theoretical learning can be demanding and not very engaging. The videos represent an indispensable support, thanks to practical demonstrations that facilitate both understanding and memorization.

With this guide, I wanted to expand the educational experience offered by the videos, providing a tool that allows anyone, regardless of language, to follow the lessons with greater attention. The combination of visual explanations and a well-organized textual reference offers a complete approach, ideal for effective learning

[RedLotus Community](#)

[Video Playlist](#)

Terminology and Level of Detail Warning

It is important to underline that the terminology and explanations provided within this document have been deliberately simplified, avoiding excessive technicalities and an excessively in-depth level of detail. This choice was dictated by the desire to make the material accessible to a wide audience, avoiding overloading the reader with excessively complex or specific information. The primary objective is to provide a clear and essential overview of the concepts covered, allowing an effective understanding of the methods illustrated.

Introduction to ScreenSharing [SS]

Many companies that develop non-competitive video games avoid adopting client-side AntiCheat systems, mainly due to high costs and technical complexity. However, in competitive contexts such as Minecraft or FiveM servers, ScreenShares are essential to ensure a fair and cheater-free gaming environment. Overtime, the methods used to perform these checks have been refined to counteract increasingly advanced bypasses, with the main goal of gathering reliable evidence of cheat use by players.

In this guide, we will focus on basic methods to detect hacks,
avoiding advanced techniques.

How to Check Forge Mods

During ScreenShares, it is important to be aware that some players may try to bypass using cheats hidden inside seemingly normal mods. For this reason, an analysis of the mods used by the player is essential.

Step 1: Check Modified Date of Mod Folder

Before examining individual mods, it is essential to check the last modified date of the folder containing the player's mods. If this date coincides with a moment immediately before the check, it is advisable to proceed with the player's ban. This action is necessary because it indicates possible tampering with the mods, which occurred shortly before the check.

Step 2: Analyze Mod Weight

A quick way to spot anomalies is to check the weight (size) of the mod files. Legitimate mods usually have a weight that falls within a range considered normal. If a mod's weight seems suspicious, because it is too large or too small compared to the standard, a more thorough investigation is needed.

[Mods Weight](#)

Step 3: Deep Analysis with a Java Decompiler

If the weight of a mod raises concerns, the next step is to use a Java decompiler. This tool allows you to analyze the source code of the mod and determine if it contains elements that should not be there, such as unauthorized functions. In this way, you can understand with certainty whether the mod is legitimate or not..

How to Access the .minecraft Folder

To begin the check, you need to locate the .minecraft folder, where all the mods are located installed by the player. To do this, follow these simple steps:

Go to the game Options, select the Resource Packages item, click on the "Open Packages Folder" button.

In the folder that opens, go back to the previous folder (the one called .minecraft). From here look for the "mods" folder.

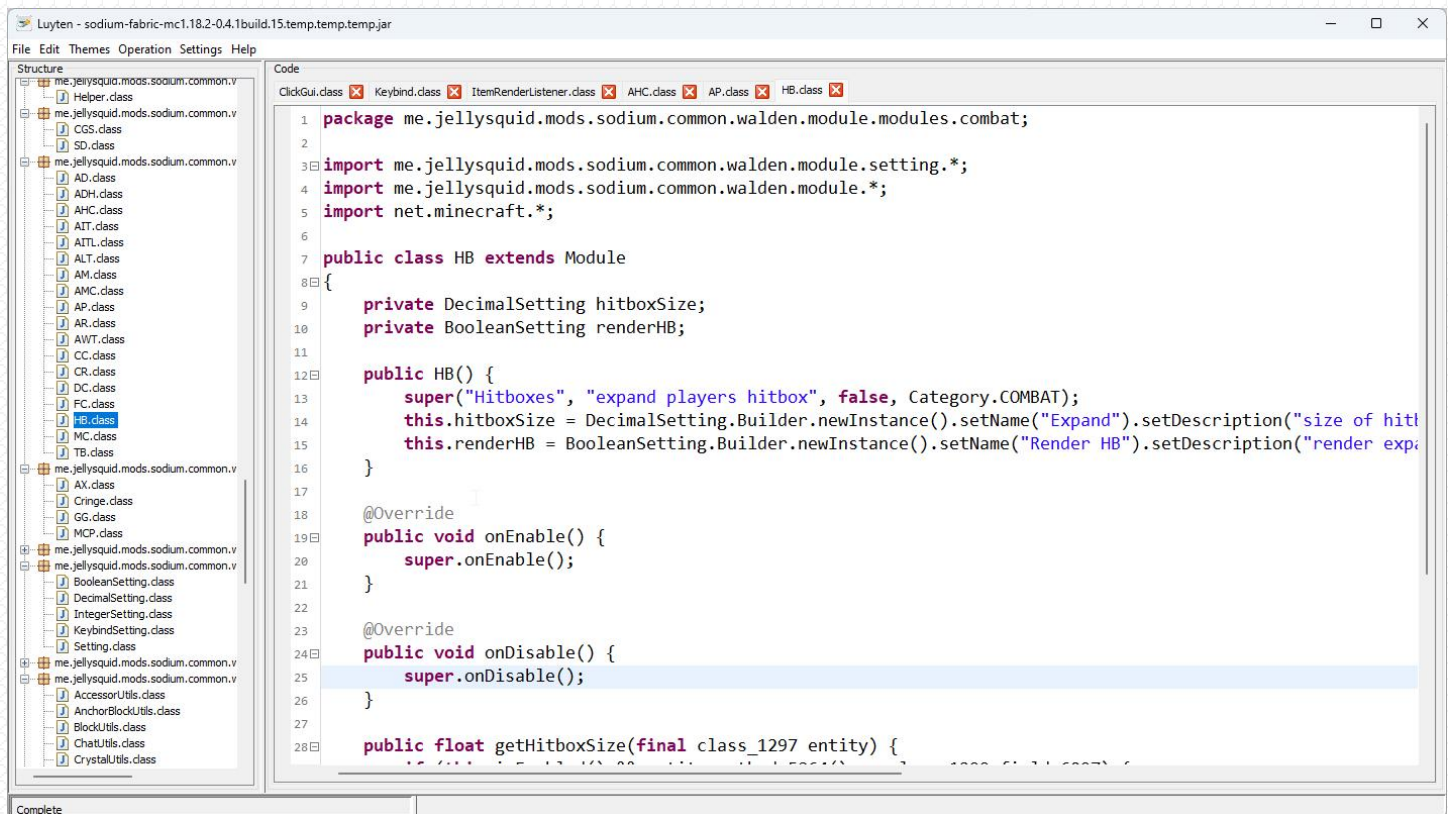
Luyten

Luyten is a Java decompiler that allows you to view the source code of a .jar file, such as those of mods, to verify whether they contain unauthorized code or cheats.

Steps to use Luyten:

Start by opening the Luyten program on the computer, then locate the mod file you want to analyze (the .jar file) and drag it into the Luyten window. Once the mod is loaded, Luyten will display the decompiled source code. Carefully examine the different classes to identify any suspicious elements, such as unnecessary code or unexpected modifications that could indicate the presence of illegitimate functionality.

[Luyten download](#)



RedLotus Mod Analyzer

It is a tool created by Red Lotus, called ModAnalyzer, that simplifies the analysis of Minecraft mods. This tool is useful for detecting any suspicious modifications or automatically hidden features.

Video: For an overview of how the tool works, a demo video is available.

ModAnalyzer download

Unloaded Mod

A method that some players use to bypass is to "unload" a mod. This means stopping Minecraft from using it, allowing you to delete, move, or rename it even if it was in use during the game session. To find these mods, you need to follow a specific procedure:

Start the "System Informer" tool on the computer, locate the process called "javaw.exe" in the process list, use the program's filter function. Set a "Contains (Case-Insensitive)" filter, and paste the path to the folder containing the player's mods. Compare the results obtained from the filter with the list of mods actually present in the player's mod folder. If you notice any differences, i.e. mods appearing in the process but not in the folder, the player may have moved, deleted, or renamed the mod after unloading it.

System Informer

System Informer is an advanced tool, developed by Winsiderss, designed to monitor system resources, debug software and detect malware. In a ScreenShare context during hack checks, it is mainly used to detect traces of cheats by analyzing the memory of processes and services.

Key Features of System Informer:

Allows you to observe the real-time usage of system resources.

Provides tools to analyze the operation of programs.

Helps identify suspicious activity related to malicious software.

Allows you to examine the memory of processes and services to detect anomalies.

Processes and Services Monitored:

During a ScreenShare, several processes and services are monitored, including: explorer, csrss, MsMpEng, SearchIndexer, Javaw, PcaSvc, Diagtrack and many others.

System Informer Configuration:

Download System Informer from the official website, start the program with administrator privileges, access the Options menu, select General, check the Kernel-Mode Driver option, finally restart the program. This option also allows you to view protected processes such as csrss and MsMpEng.

Process Filtering:

Find the process you want to analyze (eg: explorer.exe) and right-click on it, select Properties, then the Memory tab, click on Options and check Hide free pages and Hide reserved pages, set a minimum value of 5, select Extended Unicode and Mapped, then click on Ok. Once you have done this, a Results window will open. Click on Filter and choose the contains (case-insensitive) or Regex (case-insensitive) option depending on the type of search you want to perform:

Contains (case-insensitive): Filters for a specific keyword within the process (eg: "autoclicker").

Regex (case-insensitive): Allows you to perform more complex searches based on "search patterns" (eg: specific patterns).

Journal

The Journal is a log of system file activity that Windows keeps in the hidden and protected folder "\$Extend\$UsnJrnl", in a specific data stream called \$J. This log tracks changes, creations, deletions and other operations on system files. Journal analysis can reveal suspicious activity performed by the player. There are three main methods used in SS to "view" the Journal, each with its own characteristics and advantages:

CMD (Prompt dei Comandi)

Open Command Prompt as administrator and use the following command to export the Journal to a text file:

```
fsutil usn readjournal C: csv > Journal.txt
```

This command saves the entire Journal on the C: drive to a file called "Journal.txt".

To get more specific results, you can modify the command. For example, to display only logs containing ".exe", use:

```
fsutil usn readjournal C: csv | findstr /i /C:".exe" > Exe.txt
```

This command exports to "Exe.txt" only the logs that include the keyword ".exe".

You can modify the filter to search for other file extensions, keywords or to perform increasingly specific filters depending on your needs.

Echo Journal

Echo-Journal is a tool developed to view the Journal quickly and easily. Once opened, simply select the boxes for the operations you are interested in (Delete, Create, Renamed from, Renamed to, Closed and Data Changed).

[Echo Journal Download](#)

Journal Trace

Journal Trace is a tool developed by Ponei to view the Journal more efficiently.

To use it you can follow the steps below:

Open Journal Trace with administrator permissions, click on "Drive" and then on "Select" to choose the disk you want to analyze, after selecting the disk, click on "Drive" again and choose "Scan" to start scanning the Journal, once the upload is complete, go to "Layout" and select "Data Grid", click on the "Date" header to sort the results by the most recent date. Change the "Name" or "Reason" header and enter the term you want to search for (for example: "Delete", "Rename", "Data Extend").

[JournalTrace download](#)

BAM

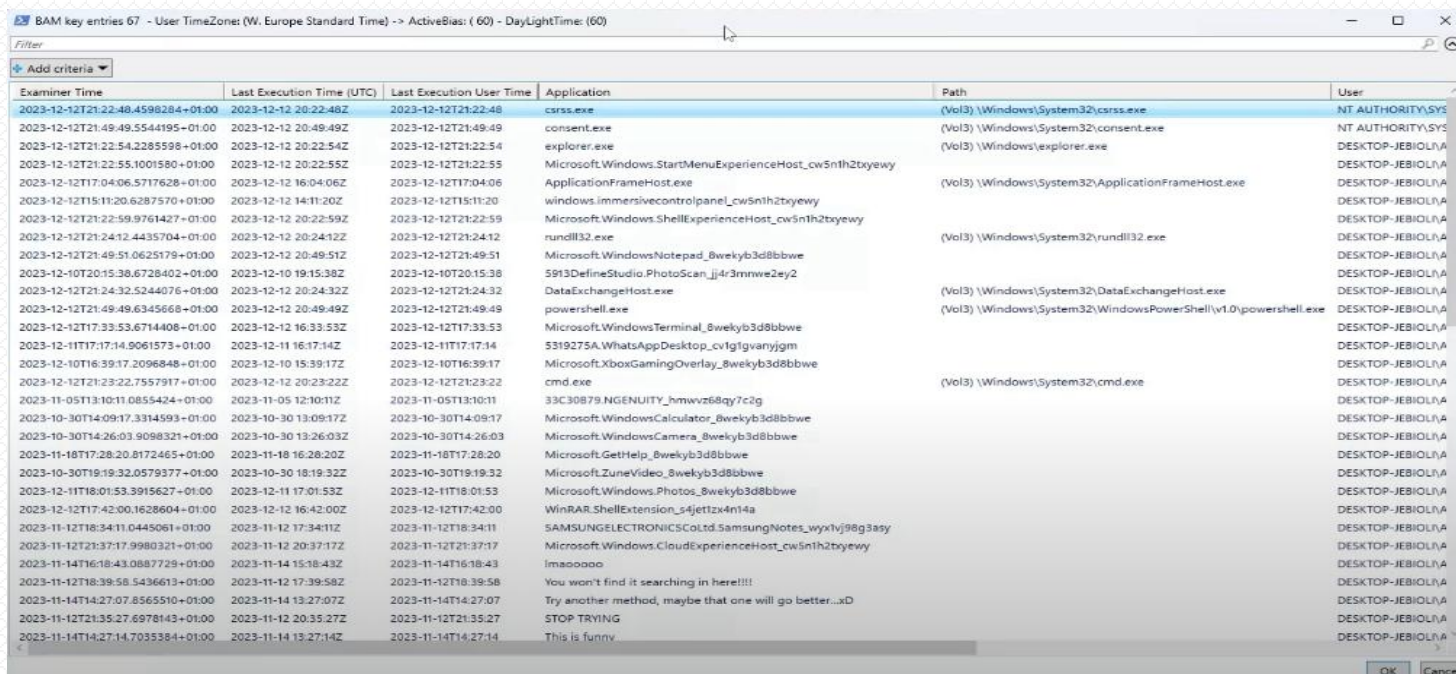
The BAM, or Background Activity Monitor, is a Windows driver introduced starting with Windows 10. Its function is to manage the background activities of applications. When an application is executed, the BAM creates a specific value in the registry (Regedit) that includes important information about the execution of the program. This information can be valuable for identifying suspicious activities or traces of cheats.

To view the BAM, a command developed by RedLotus is usually used, this is because it offers the possibility of checking the status of the digital signature of the file.

How to view the BAM

Start the Command Prompt with administrator privileges, paste the following command in the [Command Prompt](#). A window will then open. By double-clicking on "Last Execution User Time", you will be able to view the date and time of the last "activity" that occurred on the program.

As soon as a program is opened, the date in the BAM will indicate the opening time, subsequently every time an activity is done on the program window, this date will be updated, finally, if the program is closed the date will update one last time.



BAM key entries 67 - User TimeZone: (W. Europe Standard Time) -> ActiveBias: (60) - DayLightTime: (60)

Examiner Time	Last Execution Time (UTC)	Last Execution User Time	Application	Path	User
2023-12-12T21:22:48.4598284+01:00	2023-12-12 20:22:48Z	2023-12-12T21:22:48	csrss.exe	(Vol3) \Windows\System32\csrss.exe	NT AUTHORITY\SYSTEM
2023-12-12T21:49:49.5544195+01:00	2023-12-12 20:49:49Z	2023-12-12T21:49:49	consent.exe	(Vol3) \Windows\System32\consent.exe	NT AUTHORITY\SYSTEM
2023-12-12T21:22:54.2285598+01:00	2023-12-12 20:22:54Z	2023-12-12T21:22:54	explorer.exe	(Vol3) \Windows\explorer.exe	DESKTOP-JEBIOL/A
2023-12-12T21:22:55.1001580+01:00	2023-12-12 20:22:55Z	2023-12-12T21:22:55	Microsoft.Windows.StartMenuExperienceHost_cw5nth2xyewy		DESKTOP-JEBIOL/A
2023-12-12T17:04:06.5717628+01:00	2023-12-12 16:04:06Z	2023-12-12T17:04:06	ApplicationFrameHost.exe	(Vol3) \Windows\System32\ApplicationFrameHost.exe	DESKTOP-JEBIOL/A
2023-12-12T15:11:20.6287570+01:00	2023-12-12 14:11:20Z	2023-12-12T15:11:20	windows.immersivecontrolpanel_cw5nth2xyewy		DESKTOP-JEBIOL/A
2023-12-12T21:22:59.9761427+01:00	2023-12-12 20:22:59Z	2023-12-12T21:22:59	Microsoft.Windows.ShellExperienceHost_cw5nth2xyewy		DESKTOP-JEBIOL/A
2023-12-12T21:24:12.4435704+01:00	2023-12-12 20:24:12Z	2023-12-12T21:24:12	rundll32.exe	(Vol3) \Windows\System32\rundll32.exe	DESKTOP-JEBIOL/A
2023-12-12T21:49:51.0625179+01:00	2023-12-12 20:49:51Z	2023-12-12T21:49:51	Microsoft.Windows.Notedpad_8wekyb3d8bbwe		DESKTOP-JEBIOL/A
2023-12-10T20:15:38.6728402+01:00	2023-12-10 19:15:38Z	2023-12-10T20:15:38	5913DefineStudio.PhotoScan_jj4r3mnw2ey2		DESKTOP-JEBIOL/A
2023-12-12T21:24:32.5244076+01:00	2023-12-12 20:24:32Z	2023-12-12T21:24:32	DataExchangeHost.exe	(Vol3) \Windows\System32\DataExchangeHost.exe	DESKTOP-JEBIOL/A
2023-12-12T21:49:49.6345668+01:00	2023-12-12 20:49:49Z	2023-12-12T21:49:49	powershell.exe	(Vol3) \Windows\System32\WindowsPowerShell\v1.0\powershell.exe	DESKTOP-JEBIOL/A
2023-12-12T17:33:53.6714408+01:00	2023-12-12 16:33:53Z	2023-12-12T17:33:53	Microsoft.Windows.Terminal_8wekyb3d8bbwe		DESKTOP-JEBIOL/A
2023-12-11T17:17:14.9061573+01:00	2023-12-11 16:17:14Z	2023-12-11T17:17:14	5319275A.WhatsAppDesktop_cv1g1gvanyjgm		DESKTOP-JEBIOL/A
2023-12-10T16:39:17.2096848+01:00	2023-12-10 15:39:17Z	2023-12-10T16:39:17	Microsoft.XboxGamingOverlay_8wekyb3d8bbwe		DESKTOP-JEBIOL/A
2023-12-12T21:23:22.7557917+01:00	2023-12-12 20:23:22Z	2023-12-12T21:23:22	cmd.exe	(Vol3) \Windows\System32\cmd.exe	DESKTOP-JEBIOL/A
2023-11-05T13:10:11.0655424+01:00	2023-11-05 12:10:11Z	2023-11-05T13:10:11	33C30879.NGENUITY_hmwvz68qy7c2g		DESKTOP-JEBIOL/A
2023-10-30T14:09:17.3314593+01:00	2023-10-30 13:09:17Z	2023-10-30T14:09:17	Microsoft.Windows.Calculator_8wekyb3d8bbwe		DESKTOP-JEBIOL/A
2023-10-30T14:26:03.9098321+01:00	2023-10-30 13:26:03Z	2023-10-30T14:26:03	Microsoft.Windows.Camera_8wekyb3d8bbwe		DESKTOP-JEBIOL/A
2023-11-18T17:28:20.8172465+01:00	2023-11-18 16:28:20Z	2023-11-18T17:28:20	Microsoft.GetHelp_8wekyb3d8bbwe		DESKTOP-JEBIOL/A
2023-10-30T19:19:32.0579377+01:00	2023-10-30 18:19:32Z	2023-10-30T19:19:32	Microsoft.ZuneVideo_8wekyb3d8bbwe		DESKTOP-JEBIOL/A
2023-12-11T18:01:53.3915627+01:00	2023-12-11 17:01:53Z	2023-12-11T18:01:53	Microsoft.Windows.Photos_8wekyb3d8bbwe		DESKTOP-JEBIOL/A
2023-12-12T17:42:00.1628604+01:00	2023-12-12 16:42:00Z	2023-12-12T17:42:00	WinRAR.ShellExtension_s4jettzx4n14a		DESKTOP-JEBIOL/A
2023-11-12T18:34:11.0445061+01:00	2023-11-12 17:34:11Z	2023-11-12T18:34:11	SAMSUNG ELECTRONICS Co., Ltd SamsungNotes_wyxhv98g3asy		DESKTOP-JEBIOL/A
2023-11-12T21:37:17.9980321+01:00	2023-11-12 20:37:17Z	2023-11-12T21:37:17	Microsoft.Windows.CloudExperienceHost_cw5nth2xyewy		DESKTOP-JEBIOL/A
2023-11-14T16:18:43.0887729+01:00	2023-11-14 15:18:43Z	2023-11-14T16:18:43	Imagoooo		DESKTOP-JEBIOL/A
2023-11-12T18:39:58.5436613+01:00	2023-11-12 17:39:58Z	2023-11-12T18:39:58	You won't find it searching in here!!!!		DESKTOP-JEBIOL/A
2023-11-14T14:27:07.8565510+01:00	2023-11-14 13:27:07Z	2023-11-14T14:27:07	Try another method, maybe that one will go better...xD		DESKTOP-JEBIOL/A
2023-11-12T21:35:27.6978143+01:00	2023-11-12 20:35:27Z	2023-11-12T21:35:27	STOP TRYING		DESKTOP-JEBIOL/A
2023-11-14T14:27:14.7035384+01:00	2023-11-14 13:27:14Z	2023-11-14T14:27:14	This is funny		DESKTOP-JEBIOL/A

Injected DLL

There are several methods to find out if a .dll file has been injected. In this guide I will explain 3 of them. The first two methods are explained only for "general knowledge" and not for their actual use during SS. This is not because they do not work, but simply because the third is clearly superior to the first two. The

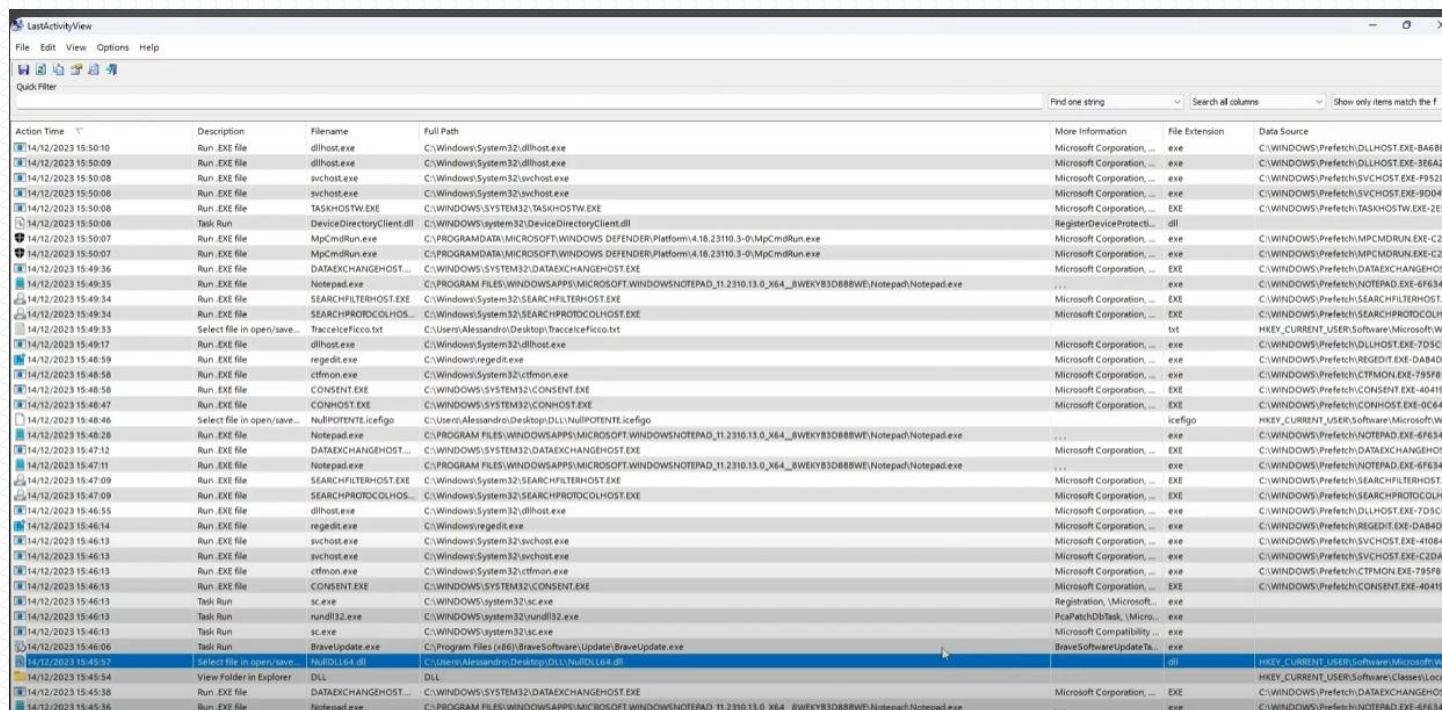
first two also work only and exclusively to identify injected DLLs as basic methods, for example by processhackers or poor Injectors.

LastActivityView

LastActivityView is a tool from NirSoft that collects data from various sources, such as prefetch, system registry, and recent file history (shell:recent).

This tool can be useful for detecting the launch of an injected .dll file even with modified (spoofed) extensions.

Download and launch LastActivityView, then analyze the results to detect suspicious file launches.



The screenshot shows the LastActivityView application window. It has a menu bar (File, Edit, View, Options, Help) and a toolbar. Below the toolbar is a search bar with a 'Find one string' dropdown and a 'Search all columns' dropdown. The main area is a table with columns: Action Time, Description, Filename, Full Path, More Information, File Extension, and Data Source. The table contains a list of system events, including file launches, task runs, and registry changes. The events are sorted by time, with the most recent at the top. The table is scrollable, and the bottom of the list is highlighted in blue.

Action Time	Description	Filename	Full Path	More Information	File Extension	Data Source
14/12/2023 15:50:10	Run .EXE file	dllhost.exe	C:\Windows\System32\dllhost.exe	Microsoft Corporation, ...	exe	C:\WINDOWS\Prefetch\DLLHOST.EXE-B468B8
14/12/2023 15:50:09	Run .EXE file	dllhost.exe	C:\Windows\System32\dllhost.exe	Microsoft Corporation, ...	exe	C:\WINDOWS\Prefetch\DLLHOST.EXE-366A2F
14/12/2023 15:50:08	Run .EXE file	svchost.exe	C:\Windows\System32\svchost.exe	Microsoft Corporation, ...	exe	C:\WINDOWS\Prefetch\SVCHOST.EXE-F952D
14/12/2023 15:50:08	Run .EXE file	svchost.exe	C:\Windows\System32\svchost.exe	Microsoft Corporation, ...	exe	C:\WINDOWS\Prefetch\SVCHOST.EXE-9D04D
14/12/2023 15:50:08	Run .EXE file	TASKHOSTW.EXE	C:\WINDOWS\SYSTEM32\TASKHOSTW.EXE	Microsoft Corporation, ...	EXE	C:\WINDOWS\Prefetch\TASKHOSTW.EXE-2E5D
14/12/2023 15:50:08	Task Run	DeviceDirectoryClient.dll	C:\WINDOWS\system32\DeviceDirectoryClient.dll	RegisterDeviceProtect...	dll	
14/12/2023 15:50:07	Run .EXE file	MpCmdRun.exe	C:\PROGRAMDATA\MICROSOFT\WINDOWS DEFENDER\Platform\4.18.23110.3-0\MpCmdRun.exe	Microsoft Corporation, ...	exe	C:\WINDOWS\Prefetch\MPCMDRUN.EXE-C2C
14/12/2023 15:50:07	Run .EXE file	MpCmdRun.exe	C:\PROGRAMDATA\MICROSOFT\WINDOWS DEFENDER\Platform\4.18.23110.3-0\MpCmdRun.exe	Microsoft Corporation, ...	exe	C:\WINDOWS\Prefetch\MPCMDRUN.EXE-C2C
14/12/2023 15:49:36	Run .EXE file	DATAEXCHANGEHOST...	C:\WINDOWS\SYSTEM32\DATAEXCHANGEHOST.EXE	Microsoft Corporation, ...	EXE	C:\WINDOWS\Prefetch\DATAEXCHANGEHOST...
14/12/2023 15:49:35	Run .EXE file	Notepad.exe	C:\PROGRAM FILES\WINDOWSAPPS\MICROSOFT\WINDOWSNOTEPAD_11.2310.13.0_X64_8WEKY83D88BWE\Notepad\Notepad.exe	...	exe	C:\WINDOWS\Prefetch\NOTEPAD.EXE-6F634F
14/12/2023 15:49:34	Run .EXE file	SEARCHFILTERHOST.EXE	C:\Windows\System32\SEARCHFILTERHOST.EXE	Microsoft Corporation, ...	EXE	C:\WINDOWS\Prefetch\SEARCHFILTERHOST.E
14/12/2023 15:49:34	Run .EXE file	SEARCHPROTOCOLHOS...	C:\Windows\System32\SEARCHPROTOCOLHOS...	Microsoft Corporation, ...	EXE	C:\WINDOWS\Prefetch\SEARCHPROTOCOLHOS...
14/12/2023 15:49:33	Select file in open/save...	Traceloc\Ficco.txt	C:\Users\Alessandro\Desktop\Traceloc\Ficco.txt		txt	HKEY_CURRENT_USER\Software\Microsoft\Wi
14/12/2023 15:49:17	Run .EXE file	dllhost.exe	C:\Windows\System32\dllhost.exe	Microsoft Corporation, ...	exe	C:\WINDOWS\Prefetch\DLLHOST.EXE-7D5CB
14/12/2023 15:48:59	Run .EXE file	regedit.exe	C:\Windows\regedit.exe	Microsoft Corporation, ...	exe	C:\WINDOWS\Prefetch\REGEDIT.EXE-DAB4D4
14/12/2023 15:48:58	Run .EXE file	ctfmon.exe	C:\Windows\System32\ctfmon.exe	Microsoft Corporation, ...	exe	C:\WINDOWS\Prefetch\CTFMON.EXE-785F81
14/12/2023 15:48:58	Run .EXE file	CONHOST.EXE	C:\WINDOWS\SYSTEM32\CONHOST.EXE	Microsoft Corporation, ...	EXE	C:\WINDOWS\Prefetch\CONHOST.EXE-404193
14/12/2023 15:48:47	Run .EXE file	CONHOST.EXE	C:\WINDOWS\SYSTEM32\CONHOST.EXE	Microsoft Corporation, ...	EXE	C:\WINDOWS\Prefetch\CONHOST.EXE-0C643
14/12/2023 15:48:46	Select file in open/save...	NullPOTENTE.icefigo	C:\Users\Alessandro\Desktop\DLL\NullPOTENTE.icefigo		icfigo	HKEY_CURRENT_USER\Software\Microsoft\Wi
14/12/2023 15:48:28	Run .EXE file	Notepad.exe	C:\PROGRAM FILES\WINDOWSAPPS\MICROSOFT\WINDOWSNOTEPAD_11.2310.13.0_X64_8WEKY83D88BWE\Notepad\Notepad.exe	...	exe	C:\WINDOWS\Prefetch\NOTEPAD.EXE-6F634F
14/12/2023 15:47:11	Run .EXE file	DATAEXCHANGEHOST...	C:\WINDOWS\SYSTEM32\DATAEXCHANGEHOST.EXE	Microsoft Corporation, ...	EXE	C:\WINDOWS\Prefetch\DATAEXCHANGEHOST...
14/12/2023 15:47:11	Run .EXE file	Notepad.exe	C:\PROGRAM FILES\WINDOWSAPPS\MICROSOFT\WINDOWSNOTEPAD_11.2310.13.0_X64_8WEKY83D88BWE\Notepad\Notepad.exe	...	exe	C:\WINDOWS\Prefetch\NOTEPAD.EXE-6F634F
14/12/2023 15:47:09	Run .EXE file	SEARCHFILTERHOST.EXE	C:\Windows\System32\SEARCHFILTERHOST.EXE	Microsoft Corporation, ...	EXE	C:\WINDOWS\Prefetch\SEARCHFILTERHOST.E
14/12/2023 15:47:09	Run .EXE file	SEARCHPROTOCOLHOS...	C:\Windows\System32\SEARCHPROTOCOLHOS...	Microsoft Corporation, ...	EXE	C:\WINDOWS\Prefetch\SEARCHPROTOCOLHOS...
14/12/2023 15:46:55	Run .EXE file	dllhost.exe	C:\Windows\System32\dllhost.exe	Microsoft Corporation, ...	exe	C:\WINDOWS\Prefetch\DLLHOST.EXE-7D5CB
14/12/2023 15:46:13	Run .EXE file	regedit.exe	C:\Windows\regedit.exe	Microsoft Corporation, ...	exe	C:\WINDOWS\Prefetch\REGEDIT.EXE-DAB4D4
14/12/2023 15:46:13	Run .EXE file	svchost.exe	C:\Windows\System32\svchost.exe	Microsoft Corporation, ...	exe	C:\WINDOWS\Prefetch\SVCHOST.EXE-410B4F
14/12/2023 15:46:13	Run .EXE file	svchost.exe	C:\Windows\System32\svchost.exe	Microsoft Corporation, ...	exe	C:\WINDOWS\Prefetch\SVCHOST.EXE-C2D4A
14/12/2023 15:46:13	Run .EXE file	ctfmon.exe	C:\Windows\System32\ctfmon.exe	Microsoft Corporation, ...	exe	C:\WINDOWS\Prefetch\CTFMON.EXE-785F81
14/12/2023 15:46:13	Run .EXE file	CONSENT.EXE	C:\WINDOWS\SYSTEM32\CONSENT.EXE	Microsoft Corporation, ...	EXE	C:\WINDOWS\Prefetch\CONSENT.EXE-404193
14/12/2023 15:46:13	Task Run	sc.exe	C:\WINDOWS\system32\sc.exe	Registration, \Microso...	exe	
14/12/2023 15:46:13	Task Run	rundll32.exe	C:\WINDOWS\system32\rundll32.exe	PcfetchDBTask, \Micro...	exe	
14/12/2023 15:46:13	Task Run	sc.exe	C:\WINDOWS\system32\sc.exe	Microsoft Compability ...	exe	
14/12/2023 15:46:06	Task Run	BraveUpdate.exe	C:\Program Files (x86)\Brave Software\Updater\BraveUpdate.exe	BraveSoftwareUpdateTa...	exe	
14/12/2023 15:45:57	Select file in open/save...	NullDll.L64.dll	C:\Users\Alessandro\Desktop\DLL\NullDll.L64.dll		dll	HKEY_CURRENT_USER\Software\Microsoft\Wi
14/12/2023 15:45:54	View Folder in Explorer	DLL	DLL			HKEY_CURRENT_USER\Software\Classes\Local
14/12/2023 15:45:38	Run .EXE file	DATAEXCHANGEHOST...	C:\WINDOWS\SYSTEM32\DATAEXCHANGEHOST.EXE	Microsoft Corporation, ...	EXE	C:\WINDOWS\Prefetch\DATAEXCHANGEHOST...
14/12/2023 15:45:36	Run .EXE file	Notepad.exe	C:\PROGRAM FILES\WINDOWSAPPS\MICROSOFT\WINDOWSNOTEPAD_11.2310.13.0_X64_8WEKY83D88BWE\Notepad\Notepad.exe	...	exe	C:\WINDOWS\Prefetch\NOTEPAD.EXE-6F634F

Regedit

Open the registry (Regedit) and go to this path:

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

Find the subkeys that contain the extension ".dll", right-click on the found subkey (eg: ".dll"), save the file with a name (eg: "DLL") and the extension ".txt", click "OK".

Open the exported .txt file and analyze its contents to locate the .dll files mentioned.

If you suspect that the .dll file has a different extension (eg: .cfg), repeat the procedure, locating and exporting the subkey related to the new extension.

System Informer + RL Signature Check

Open System Informer and find the "csrss" process. Select the process that uses the most "private bytes". Right-click the selected process, then choose "Properties" and then "Memory", in the "Options" tab, check "Hide free pages" and "Hide reserved pages", in the "Strings" tab, set "Minimum length" to 4, check "Extended Unicode", "Mapped" and "Image".

Use the following regex in the "Filter" field:

```
^[A-Z]:\\.+\\.dll$
```

This regex searches for full paths to files that end with ".dll". It can be modified if necessary to search for spoofed extensions. Select the results that contain .dll files, right-click and select "Copy Result", paste the copied paths into a text file called "paths.txt" on your desktop, open Command Prompt as administrator.

Type: `cd C:\Users\%username%\Desktop`

Type: `powershell Set-ExecutionPolicy -Scope Process -ExecutionPolicy Bypass && powershell Invoke-Expression (Invoke-RestMethod https://raw.githubusercontent.com/bacanoicua/Screenshare/main/RedLotusSignatures.ps1)`

This script will show the paths of the found .dll files and the status of the digital signature

In the screen that opens, double-click on "Signature Status" and analyze the .dll files.

JAR Cheats (Not mods)

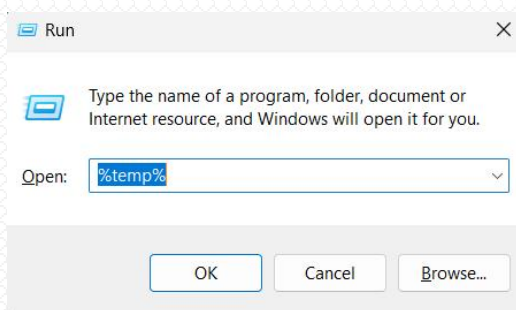
Files with the .jar extension are often associated with Java programs. Detecting the launch of such files can be critical in detecting the execution of unauthorized software, such as cheats or other suspicious programs.

JnativeHook

JnativeHook is a Java library that allows you to intercept keyboard and mouse events. Some cheats in .jar use this library.

To get this test:

Press Windows + R, type %temp% and press Enter.



In the Temp folder, look for files or folders with this name. If you find a file with the name "JnativeHook", it means that a .jar program (potentially a cheat) that uses this library has been executed. The modification date of these files corresponds to the time of execution.



Note: This method is not always reliable. Some .jar cheats do not use JnativeHook and therefore do not leave traces in this file. Also, the player may have deleted the JnativeHook files.

In that case, use the Journal to check if the files have been deleted.

Also, as many can imagine, you could completely skip the procedure of searching inside %temp% for JnativeHook and just check its creation date through the Journal from the start.

WinPrefetchView

WinPrefetchView is a NirSoft tool that analyzes prefetch (.pf) files. Prefetch records information about frequently launched programs, including .jar files.

Open the tool and check the "Indexes" of the .pf files related to "java.exe" or "javaw.exe". If you find a .jar file (e.g. "7Clicker.jar") in the "Indexes" of a Java .pf, it means that the file was started by Java. Prefetch also shows the path where the file was located when it was started.

For a reason that we will spare you for now, given the digression and the details that it would involve, this method could lead to false flags in very rare cases. Specifically, the index related to the .jar present in the .pf could be left over from a previous start of the process. For this reason, it is advisable to integrate it with further checks, for example through the following method.

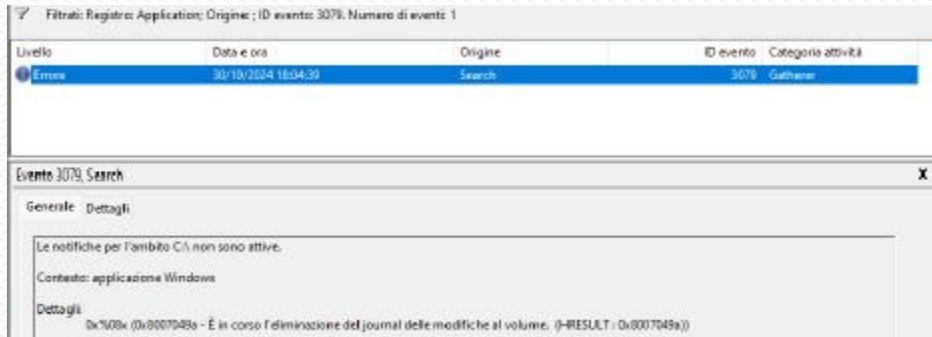
[illegible]

0x22013e0750d	0x22013e01000	166	File\\Java\\jre-1.8.0\\bin\\javaw.exe" ja "C:\\Users\\Alessandro\\Desktop\\VCLiber ja"
0x22013e080e6	0x22013e01000	166	File\\Java\\jre-1.8.0\\bin\\javaw.exe" ja "C:\\Users\\Alessandro\\Desktop\\VCLiber ja"
0x22013e0c850	0x22013e11000	80	\\Users\\Alessandro\\Desktop\\VCLiber ja"
0x270468a9920	0x2704683c3300	8	36R
0x270468b4850	0x2704687e4000	8	ja"

Event Viewer is mainly used for the following purposes in SS at basic levels:

Finding Journal Deletion:

Open Event Viewer, go to "Windows Logs" section and select "Application", click "Filter Current Log", enter Event ID 3079 and analyze the result..



System Registry

Event ID 104 indicates deletion of registry log events



Time Change

Open Event Viewer, go to the "Windows Logs" section and select "Security", click on "Filter Current Log", enter the event ID 4616 and analyze the result.

Events associated with C:\Windows\System32\svchost.exe: Generally generated by the system (but also by the user, if the time is changed from the settings).

Events associated with C:\Windows\System32\cmd.exe: Indicate a time change made via the Command Prompt and, therefore, by the user..

Controllo riuscito	25/10/2024 10:00:00	Microsoft Windows secur...	4616	Security State Change
Controllo riuscito	25/10/2024 21:42:36	Microsoft Windows secur...	4616	Security State Change
Controllo riuscito	25/10/2024 21:42:36	Microsoft Windows secur...	4616	Security State Change
Controllo riuscito	25/10/2024 22:32:12	Microsoft Windows secur...	4616	Security State Change

Security Log

Open Event Viewer, go to "Windows Logs" section and select "Security", click on "Filter Current Log", enter event ID 1102.

Note: If you try to delete this event as well, the system will automatically recreate it..

Deletions and Replaces in Fat32

One way to detect file deletion or replacement on FAT32 is to use a tool like AccessData's FTK Imager. This tool allows you to view changes made to many different types of drives, including FAT32.

Open FTK Imager with administrator permissions, select the "Add All Attached Devices" option, locate and select the folder you want to scan. Then check the files on the volume, looking for deleted files. FTK Imager highlights the files that have been deleted with a red X in it's icon.



-14-



How to Use FTK Imager to Find a Simple Replace:

The procedure to find a replace on FAT32 is similar to that used to detect a deletion. When a file is replaced, the previous file is in fact deleted from the file system. Therefore, you can use FTK Imager to detect the removal of the original file.

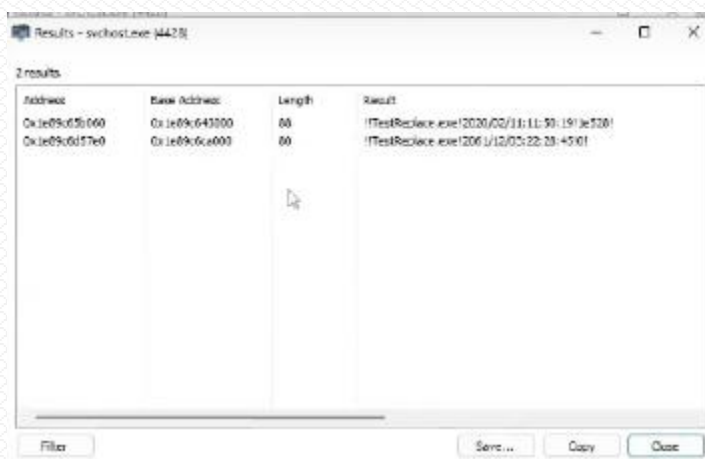
To prove that the previous file and the current one are different, you can use several methods. As for the exe, a recommended and quick one is that of DPS.

First of all, start the exe currently present in the folder.

Then start System Informer with administrator privileges, locate the -s DPS process and filter for "!!"

Then filter for "FileName.exe" by entering the name of the .exe file that you suspect has been replaced.

Finally, analyze the results. If you find two results with different timestamps (date and time) related to the same .exe file, it means that two different exe with the same name have been opened in the instance.



Attention:

The presence of two files with the same name and with different (or identical) TimeStamp is not in itself a valid proof to ban a player.

In fact, it is necessary to perform a final check before being able to take action against the player, that is, it is necessary to prove that the executable currently present in the folder in FAT32 is different from the one previously present.

To do this, we must first of all make sure that the timestamps inside the DPS do not belong to other files with the same name present in the player's PC. To do this, through a tool like everything we can check the various files present in the player's PC with the same name, open them and see if their opening generate new strings inside the DPS.

Once we have ascertained that the two strings initially present in the DPS did not belong to other programs with the same name present in the player's computer, we can ban the player.

Note: A further step that could be taken, but only if the timestamps of the legit and unlegit files are different, is to prove that one timestamp belongs to the file currently present in the folder, and the other timestamp belongs to a file that at the time of the check is no longer present on the computer and has therefore been deleted. This can be done very simply through VirusTotal website in the details tab by grabbing the timestamp of the file currently present in the pc.

History ⓘ	
Creation Time	2009-04-15 20:41:42 UTC
First Seen In The Wild	2009-04-15 12:42:00 UTC
First Submission	2009-05-29 20:07:34 UTC
Last Submission	2024-12-12 16:54:38 UTC
Last Analysis	2024-11-16 03:20:49 UTC