Windows Forensics- Part 3: File System & Execution Artifacts

Scope : Advanced File System Analysis & Program Execution Tracking

Now that we've analyzed **user behavior artifacts**, we'll dive deeper into **file system metadata and program execution evidence** to uncover **hidden activities and anti-forensic techniques.**

What We'll Cover in This Part

File System Artifacts

- **Master File Table (MFT) :** Complete file system metadata analysis
- **USN Journal :** File System change tracking
- **Background Activity Moderator (BAM) :** Background process tracking
- **AppCompatCache / Shimcache:** Applications compatibility records
- **AmCache :** Program execution metadata
- **Prefetch :** Application startup optimization data

Analysis Tools

- **MFTECmd**
- **Timeline Explorer**
- **Registry Explorer**
- **PECmd**
- **AmcacheParser**
- **Notepad++**

Investigation Goals

- **Reconstruct complete file system timeline**
- **Track program execution history**
- **Recover deleted file evidence**
- **Identify malware persistence mechanisms**

Session Objectives - Key Questions to Answer:

File Location & Identification:

- **Which files are located in the AtomicRedTeam directory?**
- **What is the MFT Entry Number for "ART-attack.ps1"?**

Timestamp Analysis:

- **What are the MACB timestamps for "ART-attack.ps1"?**
- **Was "ART-attack.ps1" timestomped?**

Deleted File Investigation:

- **When was "deleteme_T1551.004" created and deleted?**
- **What was the Entry number for "deleteme_T1551.004"?**
- **Does "deleteme_T1551.004" still exist in the MFT?**

1. Master File Table (MFT) Analysis

What is the MFT ?

The Master File Table is a **core NTFS database** storing **metadata about every file and folder on a disk**, including the MFT itself. **It preserves file information even after deletion.**

MFT Structure

- **Each entry** = FILE record (typically 1KB)

- **Contains attributes like database columns:**

Record Header: check flags to see if file is deleted, Sequence number helps track deleted files **(deleted/in-use)**

$STANDARD_INFORMATION:

- **File Timestamps** (Created, Modified, Accessed, Entry Modified).
- **File permissions**

$FILE_NAME: File names with additional timestamps

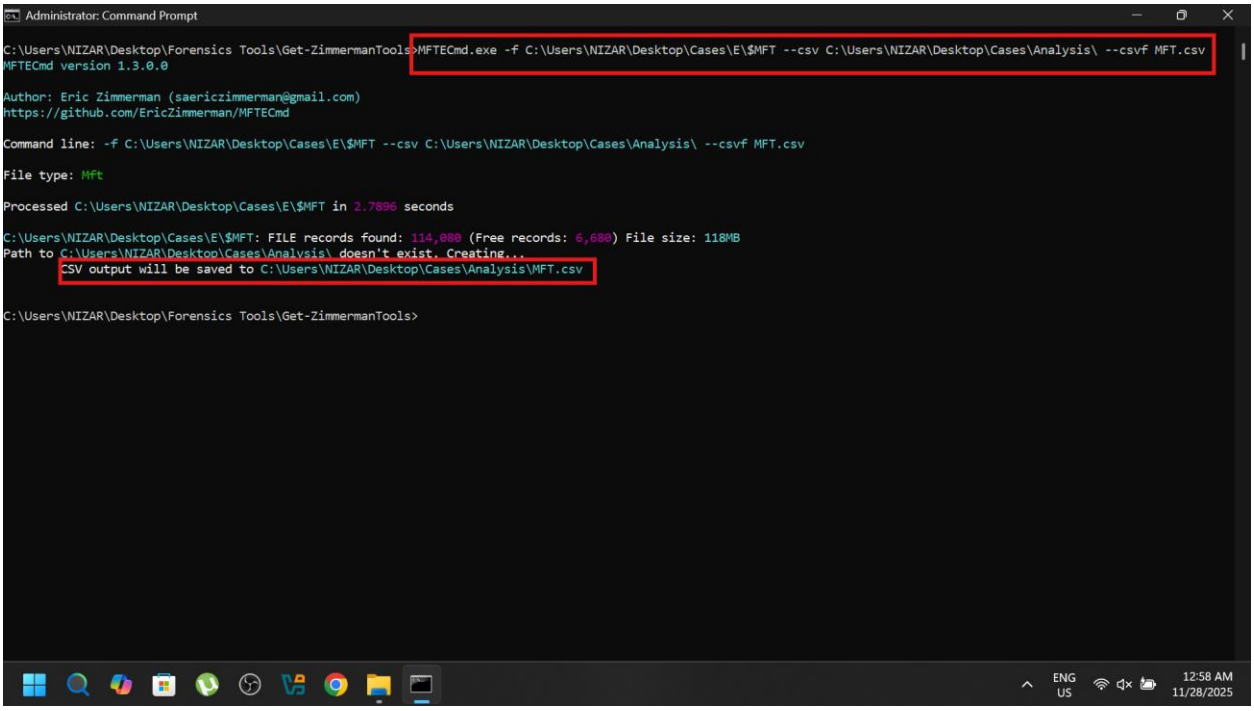
$DATA: Where the actual content of the file is stored

- **If small** → stored inside the MFT **(Resident)**
- **If big** → points to clusters on disk **(Non-Resident)**

MFT Analysis with MFTECmd

Complete MFT Parsing

⇨ **MFTECmd.exe -f C:\Users\NIZAR\Desktop\Cases\E\$MFT --csv C:\Users\NIZAR\Desktop\Cases\Analysis\ --csvf MFT.csv**

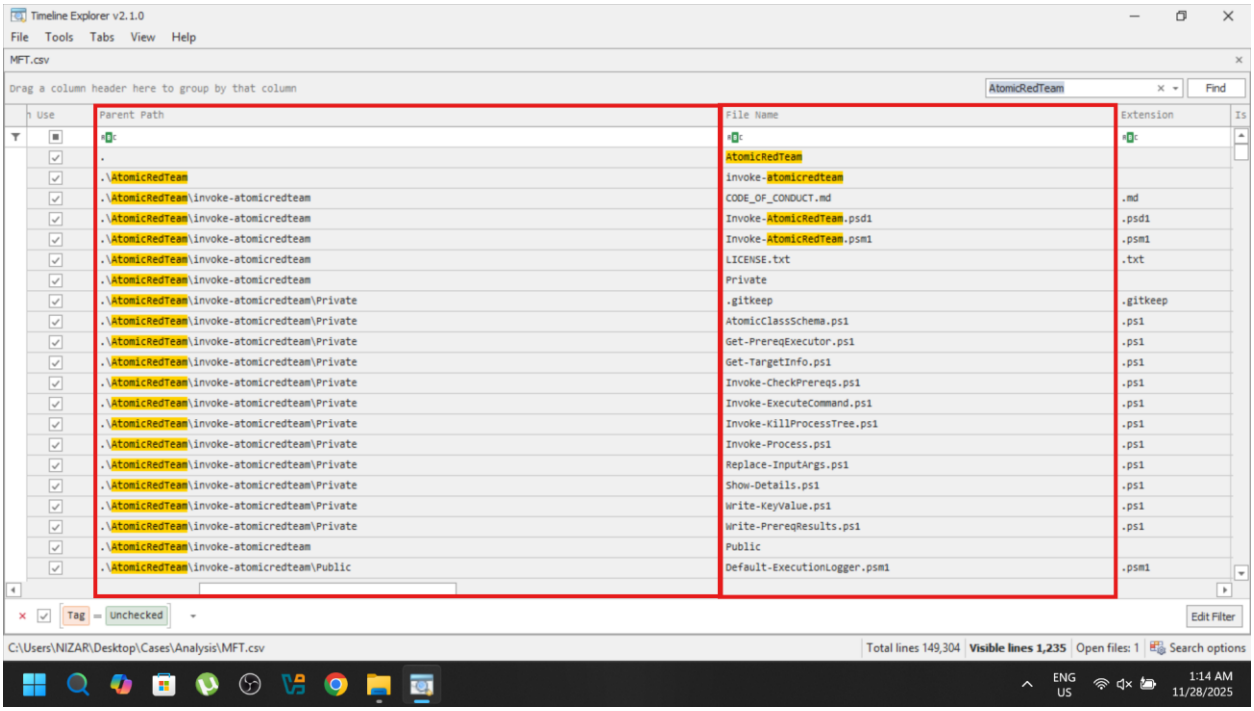


Successfully executing MFTECmd to parse the Master File Table and generate CSV output for analysis

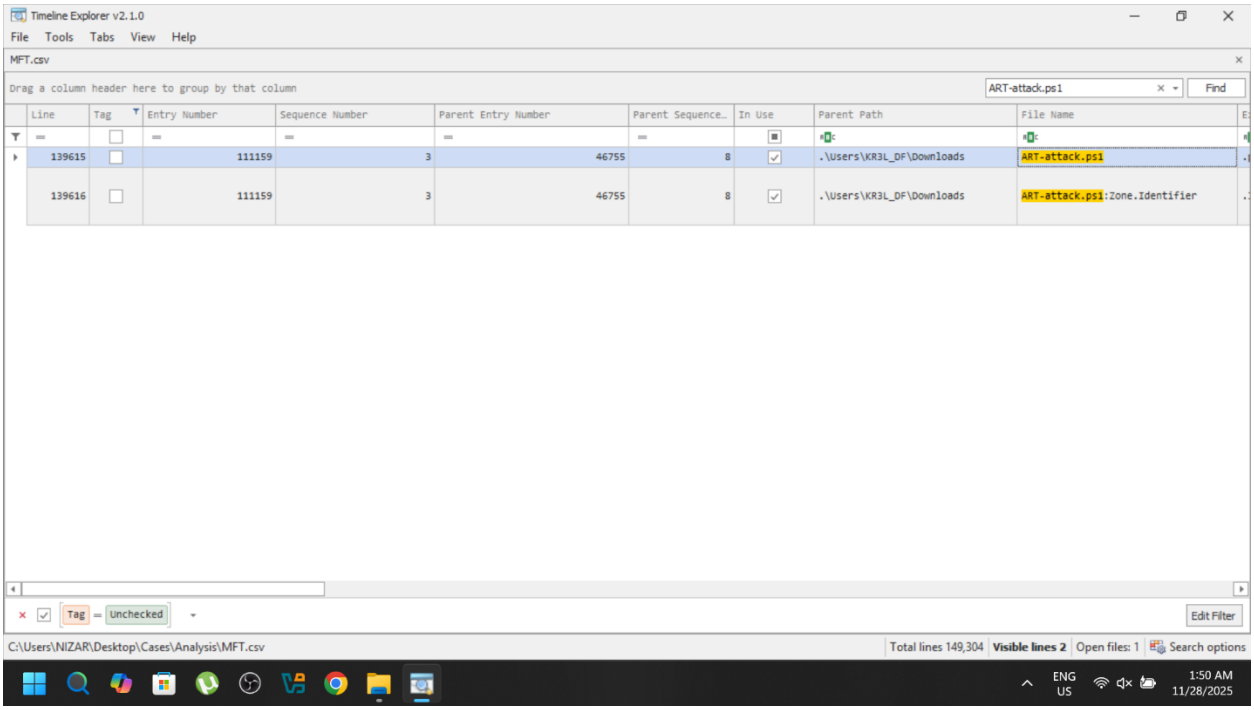
Key Investigation Questions & Findings

Some Atomic Red Team Files Discovered:

- **Invoke-atomicredteam**
- **Get-AtomicTechnique.ps1**
- **Install-atomicredteam.ps1**
- **Phant0m.exe**



- **MFT analysis revealing files inside AtomicRedTeam folder including Invoke-atomicredteam and related attack scripts**

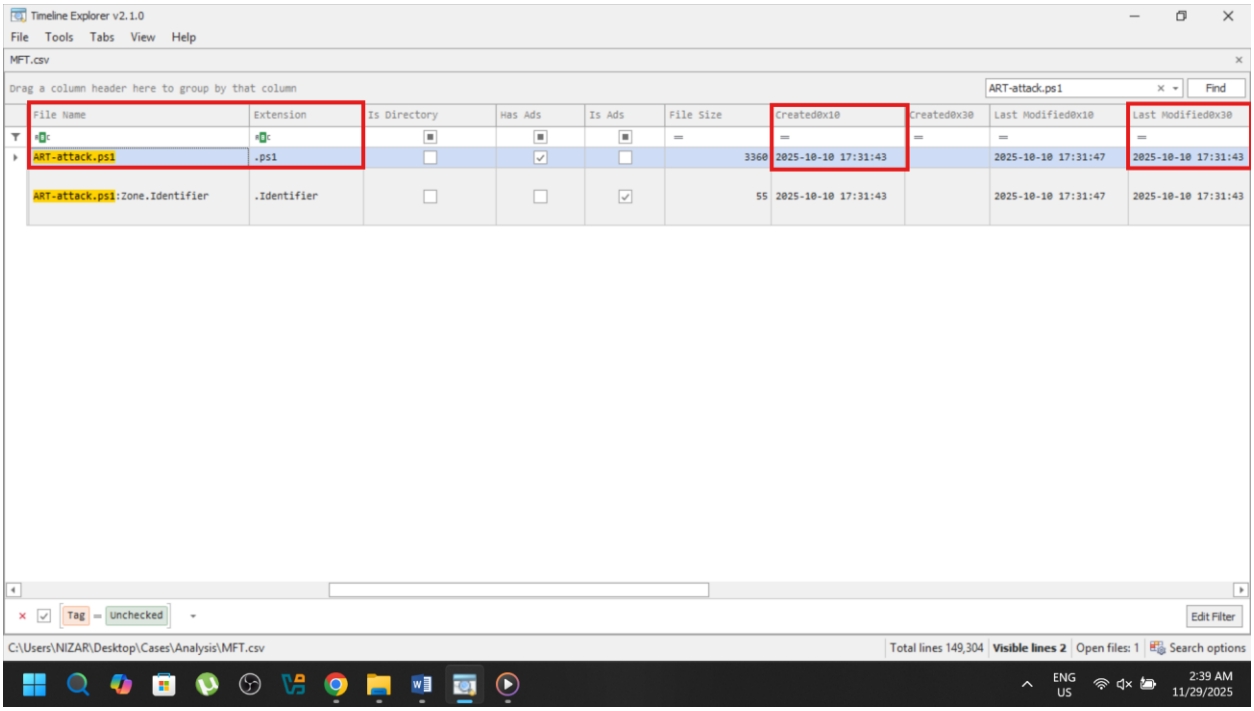


MFT record showing Entry Number 111159 for ART-attack.ps1 file

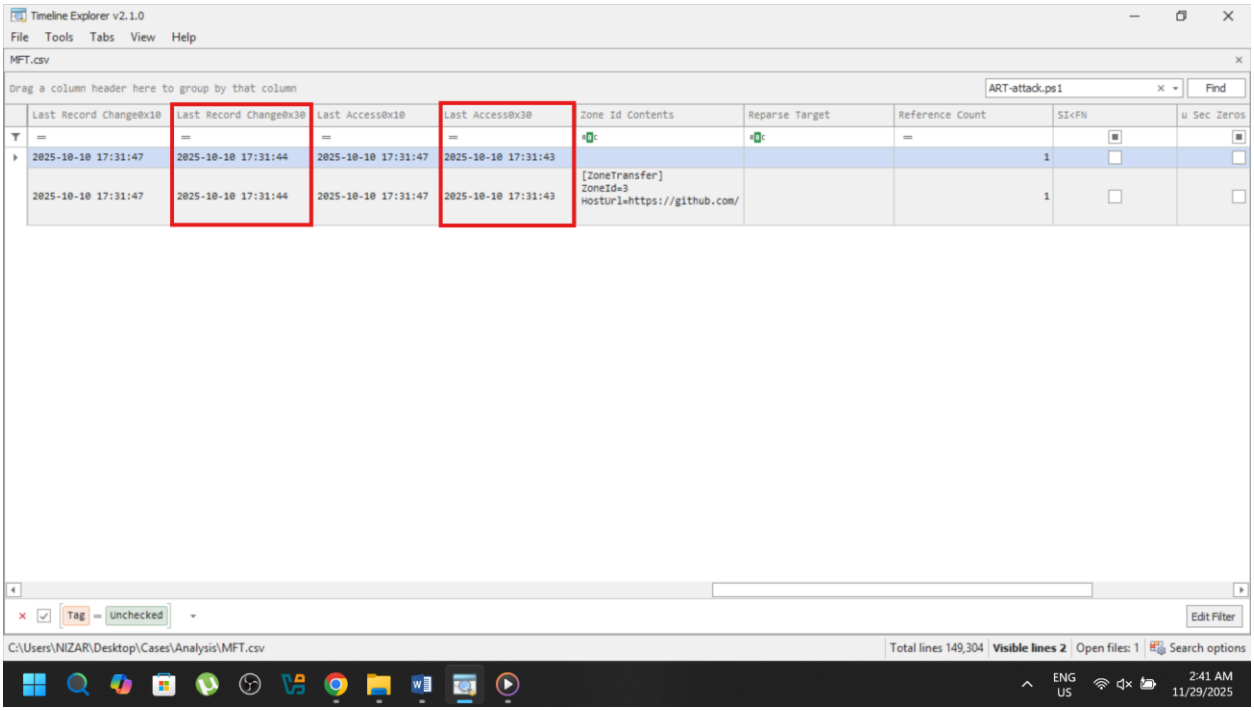
What are the MACB timestamps for "ART-attack.ps1"?

Answer:

- **Modified:** 2024-10-10 17:31:47
- **Accessed:** 2025-10-10 17:31:43
- **Changed:** 2025-10-10 17:31:44
- **Born (Created):** 2025-10-10 17:31:43



MFT entry showing creation date and last modification date for ART-attack.ps1 file



MFT timestamps showing changed date and last accessed date for ART-attack.ps1

Note: The **3-second** difference between **0x10 ($FILE_NAME)** and **0x30 ($STANDARD_INFORMATION)** timestamps is normal system behavior and **does not indicate timestomping.**

When was "deleteme_T1551.004" created and deleted?

Initial Finding: **File Not Found in Active MFT**

Current Status:

- **File not found in active MFT records**
- **Indicates file has been deleted from the file system**

Next Step: USN Journal Analysis

Since the file doesn't appear in active **MFT records**, we need to examine the **USN Journal** to **track its creation and deletion timeline.**

What is the USN Journal ?

A **Windows NTFS log** that records all file system changes like **creations, modifications, and deletions** with timestamps **for forensic tracking.**

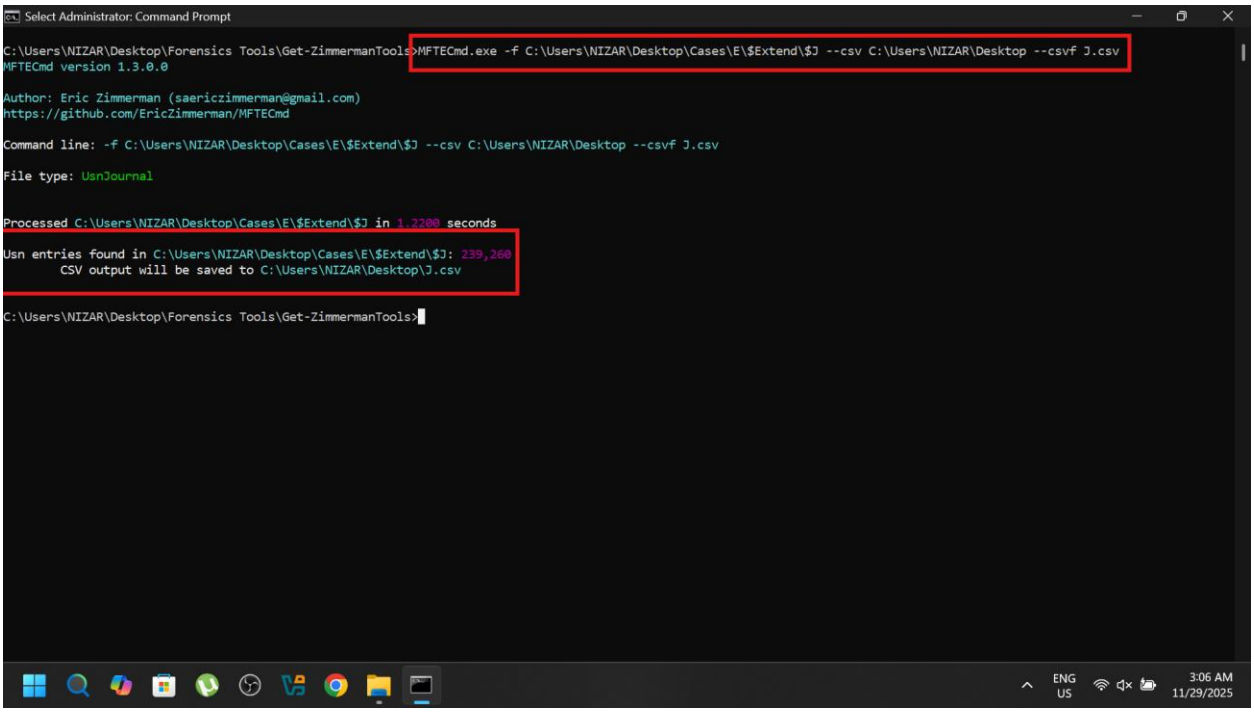
USN Journal Analysis Command:

- ⇨ **MFTECmd.exe -f C:\Users\NIZAR\Desktop\Cases\E\$Extend\$J --csv C:\Users\NIZAR\Desktop --csvf J.csv**

What USN Journal Will Reveal:

- **File creation timestamp**
- **File deletion timestamp**
- **Complete lifecycle of the deleted file**
- **File operations before deletion**

Let's parse the USN Journal to uncover the file's history...



Successfully executing MFTECmd to parse USN Journal ($Extend$J) for tracking file system changes and deleted files

- **When was "deleteme_T1551.004" created and deleted?**
- **What was the Entry number for "deleteme_T1551.004"?**

Answers:

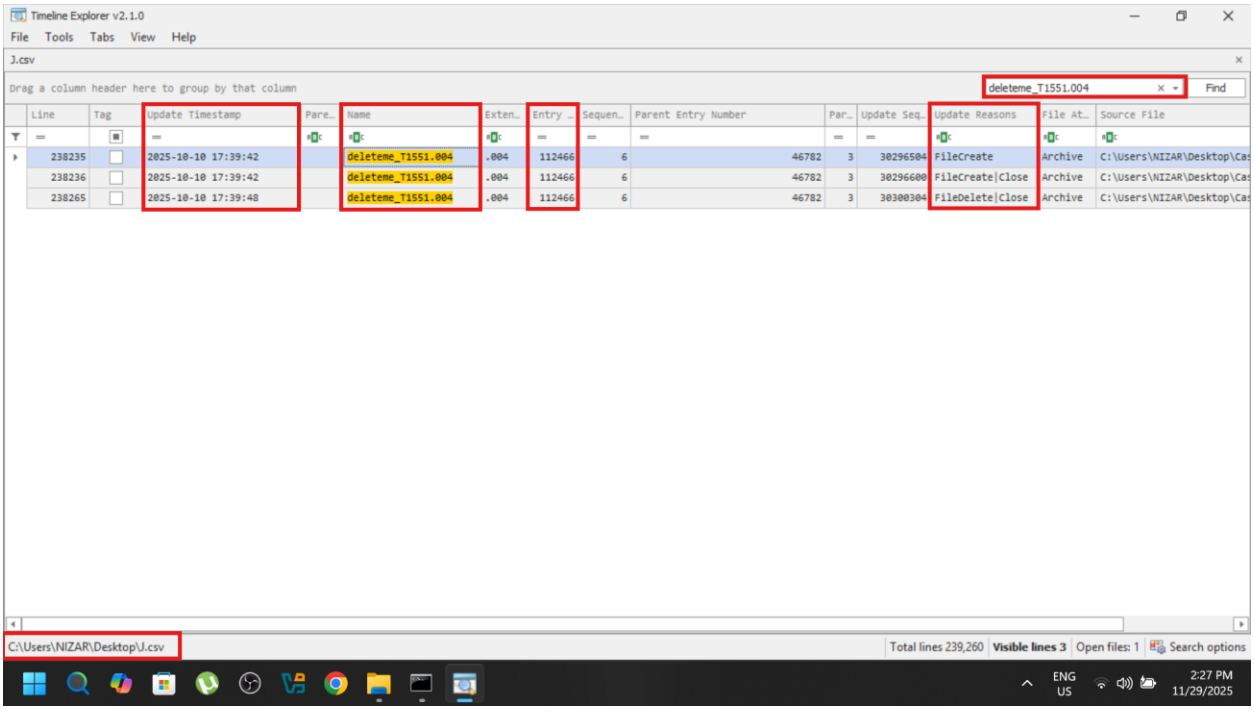
File Creation:
2025-10-10 17:39:42 - **FileCreate event** in USN Journal

File Deletion:
2025-10-10 17:39:48 - **FileDelete event** in USN Journal

Entry Number:
112466

Key Finding:

- **File lifespan:** 6 seconds - **Extremely short duration**
- **Rapid creation** and **deletion pattern suggests automated or scripted activity**
- Potential **anti-forensic technique to hide temporary files**
- This short file lifespan indicates **suspicious activity** and **possible evidence cleaning**.



USN Journal showing file creation/deletion timeline with corresponding entry numb

Does "deleteme_T1551.004" still exist in the MFT?

The file has been **deleted** from **the system**. **The MFT entry** is no longer in use. **(Resident : False)**

2. BAM Analysis (Background Activity Moderator)

What is BAM ?

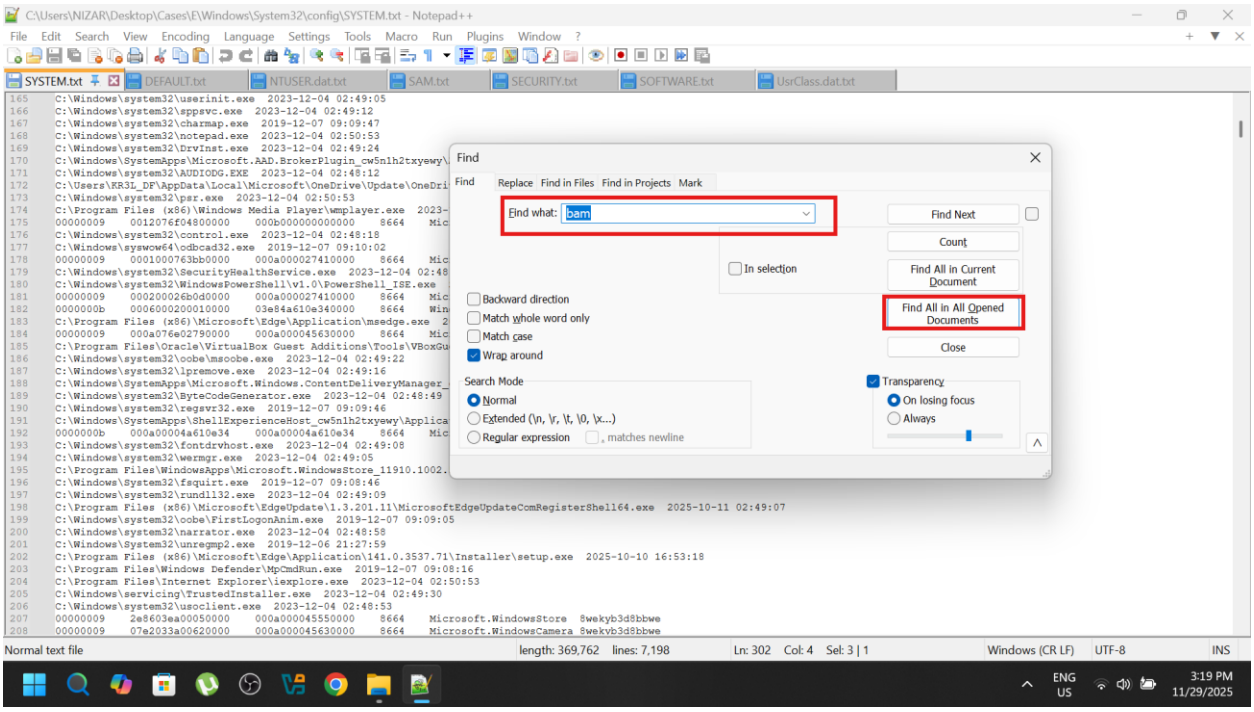
BAM is a **Windows service that tracks background application execution for resource management**, providing valuable forensic **data on program execution**.

Registry Location

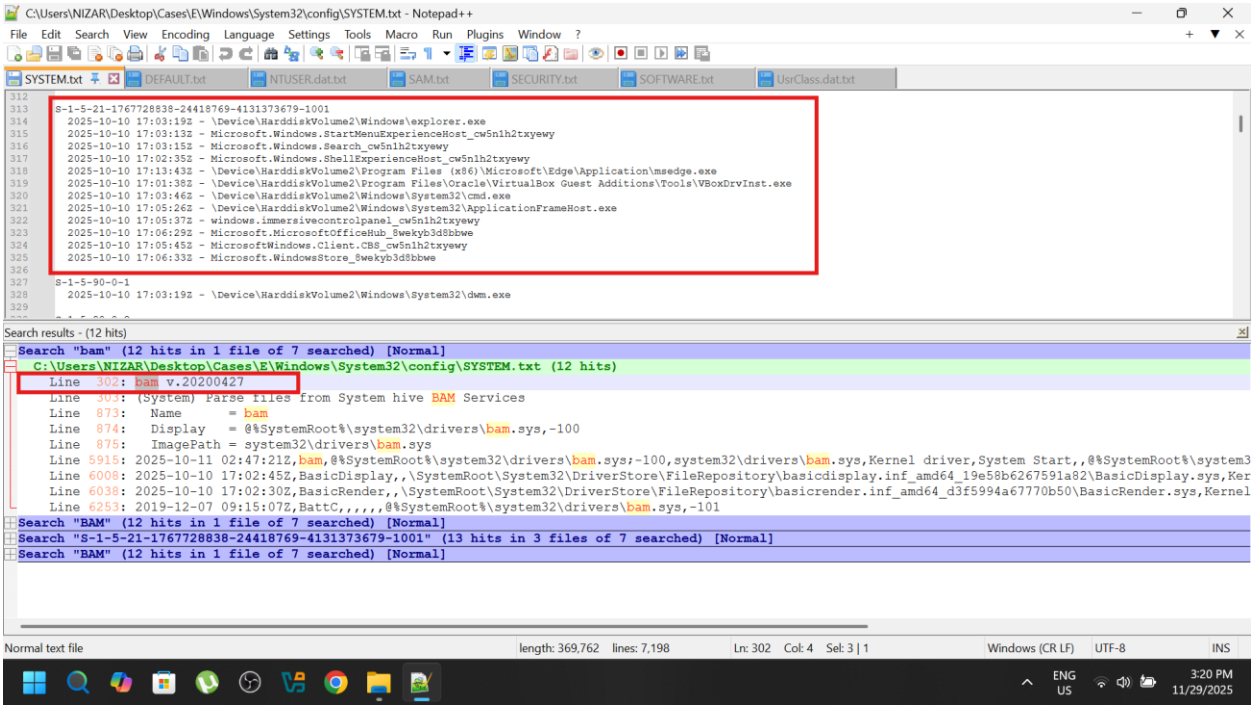
⇨ **SYSTEM\CurrentControlSet\Services\bam\UserSettings\<SID>**

Investigation Questions:

- **Which executables did BAM record for the target user (KR3L-DF) ?**
- **What were their last execution dates and times?**
- **Are there any suspicious or forensic tools executed?**



Using Notepad++ to search for BAM registry entries across all parsed registry files



BAM registry entries showing executed applications including explorer.exe, cmd.exe, and msedge.exe

BAM Analysis Results

Executables Recorded for User SID: S-1-5-21-1767728838-24418769-4131373679-1001 (KR3L-DF)

System & Application Executions:

- **explorer.exe -** 2025-10-10 17:03:19Z **(File Explorer)**
- **msedge.exe -** 2025-10-10 17:13:43Z **(Microsoft Edge)**
- **cmd.exe -** 2025-10-10 17:03:46Z **(Command Prompt)**
- **VBoxDrvInst.exe -** 2025-10-10 17:01:38Z **(VirtualBox Drivers)**

Windows System Processes:

- **StartMenuExperienceHost -** Start menu interactions
- **ShellExperienceHost -** Windows shell interface
- **ApplicationFrameHost -** Universal app hosting
- **ImmersiveControlPanel -** Settings application
- **Windows Search -** Search functionality

Store Applications:

- **Microsoft Office Hub - Office applications**
- **Windows Store - App store access**

Key Findings:

- **Normal system** activity pattern observed
- **No suspicious or forensic tools detected** in BAM records
- **Standard user workflow** with browser and system applications
- **VirtualBox components present** (expected in VM environment)
- **BAM analysis shows legitimate user activity without evidence of malicious tools.**

3. AppCompatCache/Shimcache Analysis

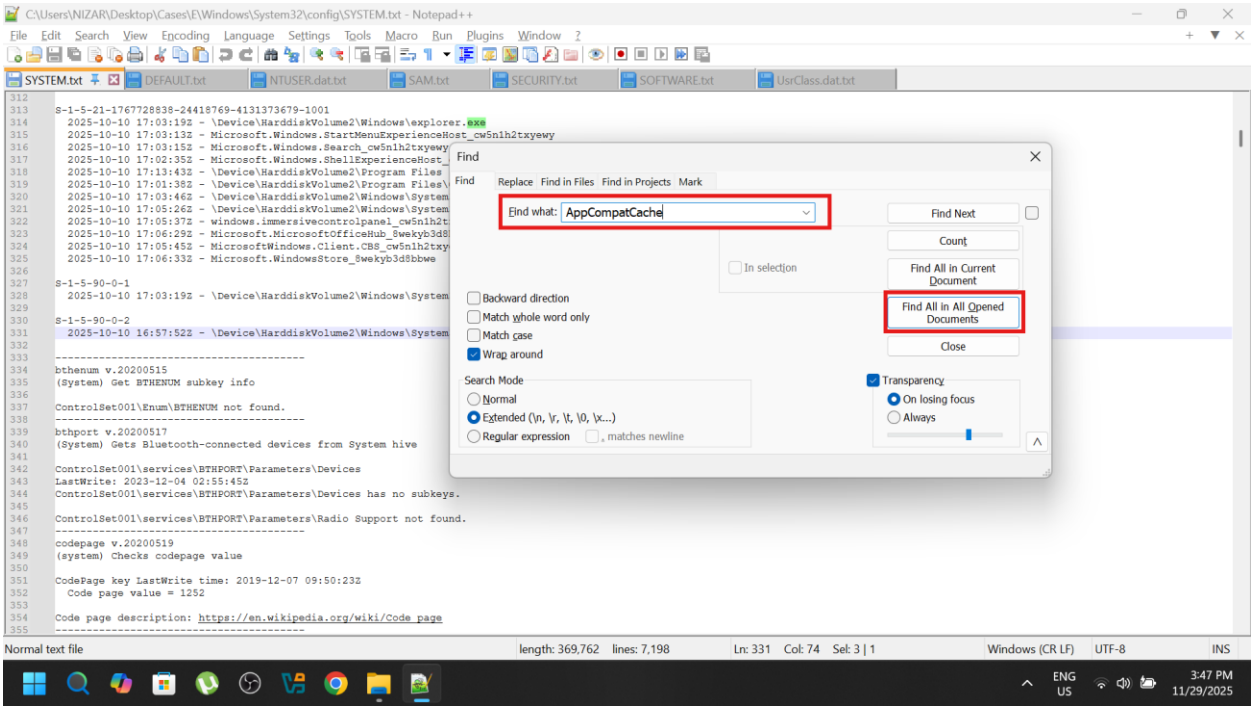
A Windows registry artifact **that stores application compatibility data**, **creating a historical record of executables** that Windows has encountered on the system.

Registry Location

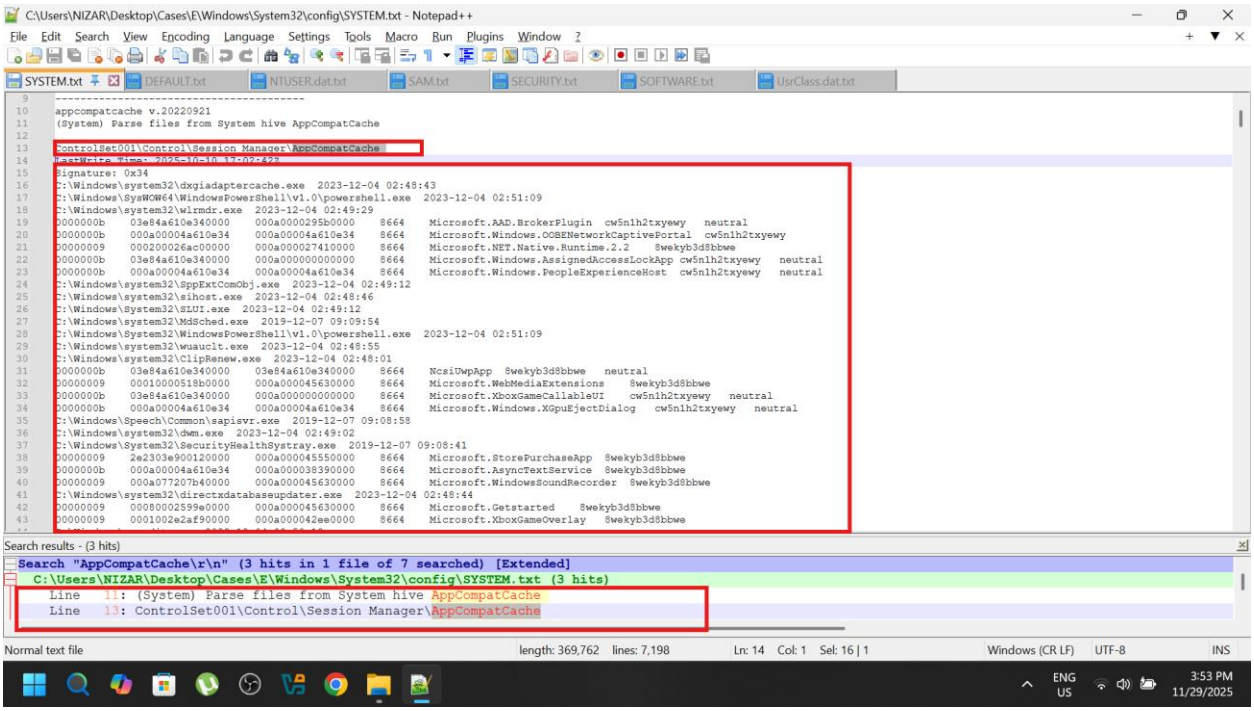
⇨ SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatCache

Key Characteristics:

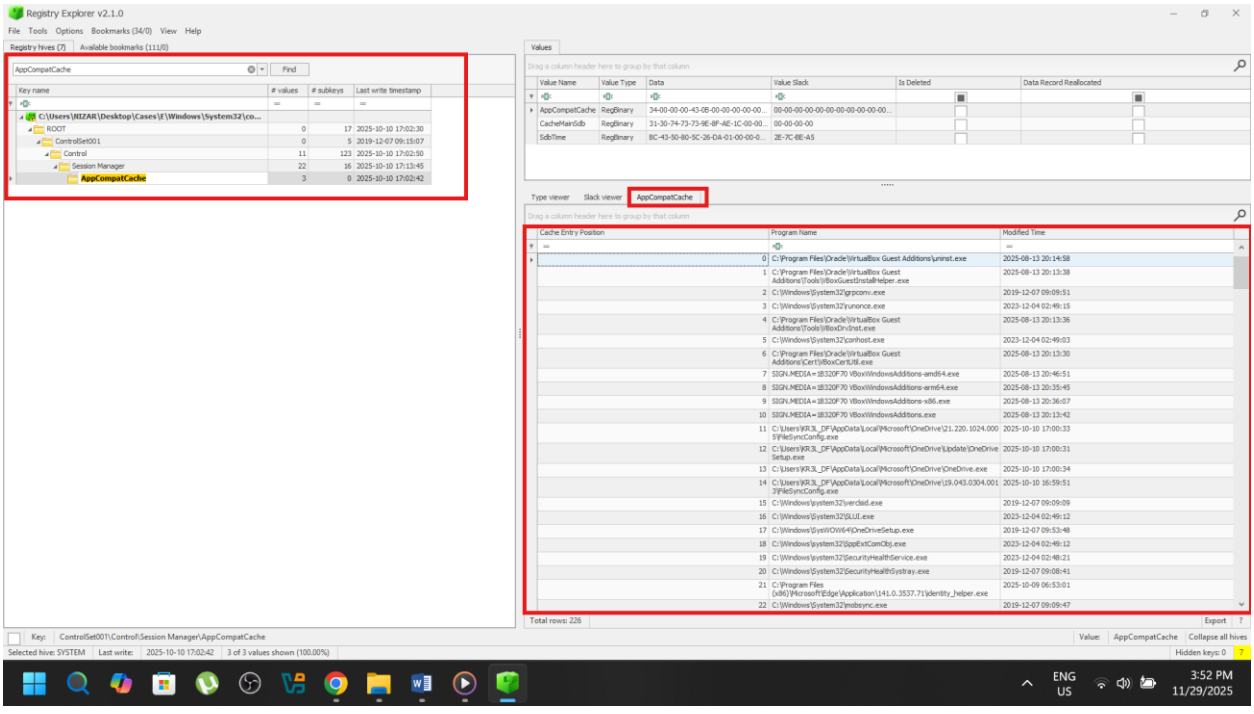
- **Records executable file paths Windows has encountered**
- **Stores last modified time of files** (not execution time)
- **Provides historical record of program presence**
- **Not definitive proof of execution** (files can be copied without running)



Using Notepad++ to search for AppCompatCache entries across all registry files for application compatibility history



AppCompatCache entries showing detected executables and their metadata in Notepad++ search results



AppCompatCache registry entries viewed in Registry Explorer showing cached executable information

Key Executables Detected:

System & Administration Tools:

- **cmd.exe** - Command Prompt **- Last Modified: 2023-12-04 02:48:51**
- **powershell.exe** - Windows PowerShell **- Last Modified: 2023-12-04 02:51:09**
- **regedit.exe** - Registry Editor **- Last Modified: 2023-12-04 02:50:12**
- **taskmgr.exe** - Task Manager **- Last Modified: 2023-12-04 02:48:59**
- **msinfo32.exe** - System Information **- Last Modified: 2023-12-04 02:50:17**
- **control.exe** - Control Panel **- Last Modified: 2023-12-04 02:48:18**

Virtualization Components:

- **VBoxDrvInst.exe** - VirtualBox Driver Installer - **Last Modified: 2025-08-13 20:13:36**
- **VBoxGuestInstallHelper.exe** - VirtualBox Guest Helpers - **Last Modified: 2025-08-13 20:13:38**
- **VBoxCertUtil.exe** - VirtualBox Certificate Utility - **Last Modified: 2025-08-13 20:13:30**

Network & Communication:

- **msedge.exe** - Microsoft Edge Browser - **Last Modified: 2025-10-09 06:52:49**
- **OneDrive.exe** - Cloud storage sync - **Last Modified: 2025-10-10 17:00:34**

Windows Store Apps:

- **Microsoft Store** applications - **Various timestamps**
- **Office Hub** components **- Various timestamps**
- **Media and entertainment apps** - **Various timestamps**

⚠ LOLBins (Living Off the Land Binaries) Alert:
Note: Several legitimate processes detected could be used for LOLBins attacks:

- **cmd.exe & powershell.exe** - Command execution and scripting
- **regedit.exe -** Registry manipulation
- **msinfo32.exe -** System reconnaissance
- **control.exe -** System configuration changes

Analysis Summary:

- **No obvious malicious software detected**
- **Multiple LOLBins** present that **could be exploited**
- **Normal system administration activity mixed with potential attack vectors**
- **VirtualBox environment confirmed**
- **Standard user applications usage pattern**

Note : While no overt malware was found, the presence of multiple LOLBins requires correlation with other artifacts to rule out Living Off the Land attacks.

4. AmCache Analysis

What is AmCache?

AmCache is a **Windows registry** artifact that stores **comprehensive metadata** about **executables and applications that have been executed on a system**, providing valuable forensic data for incident investigations.

Registry Location

⇨ **C:\Windows\AppCompat\Programs\Amcache.hve**

What AmCache Contains :

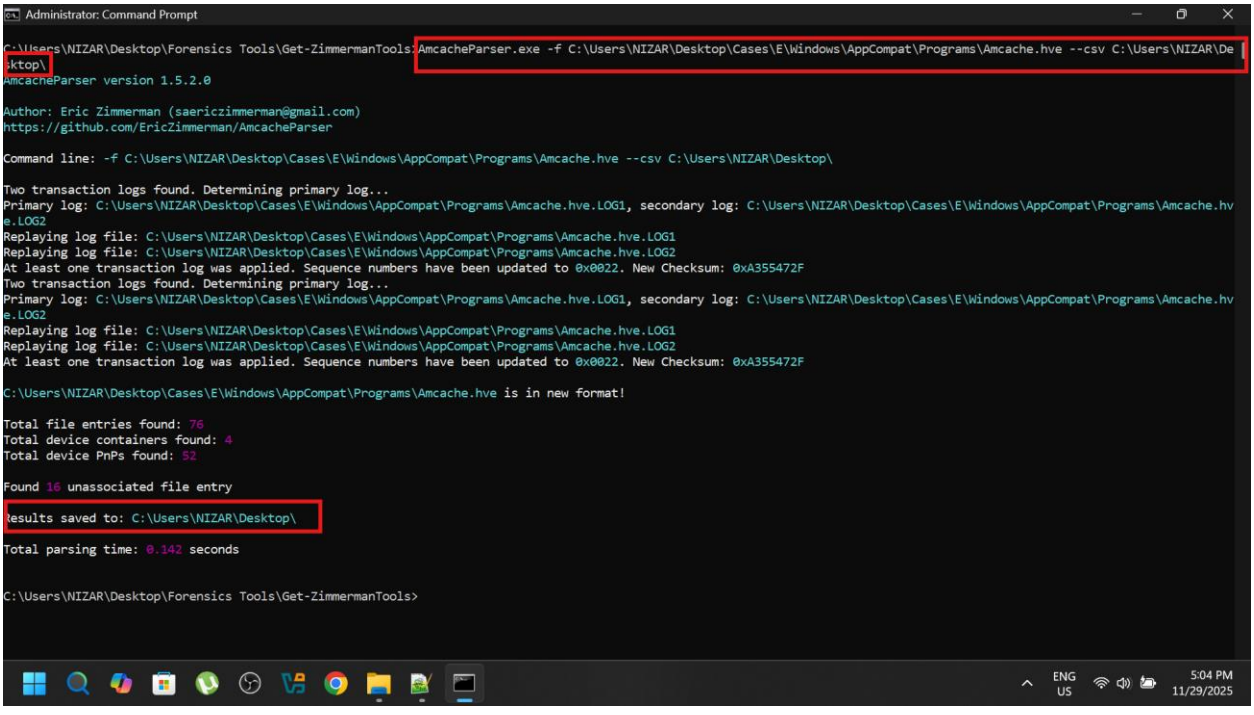
- **Executable metadata:** File paths, sizes, timestamps

- **SHA1 hashes** for file integrity verification
- **Program execution information and timestamps**
- **Software publisher details**
- **MRU (Most Recently Used) data**

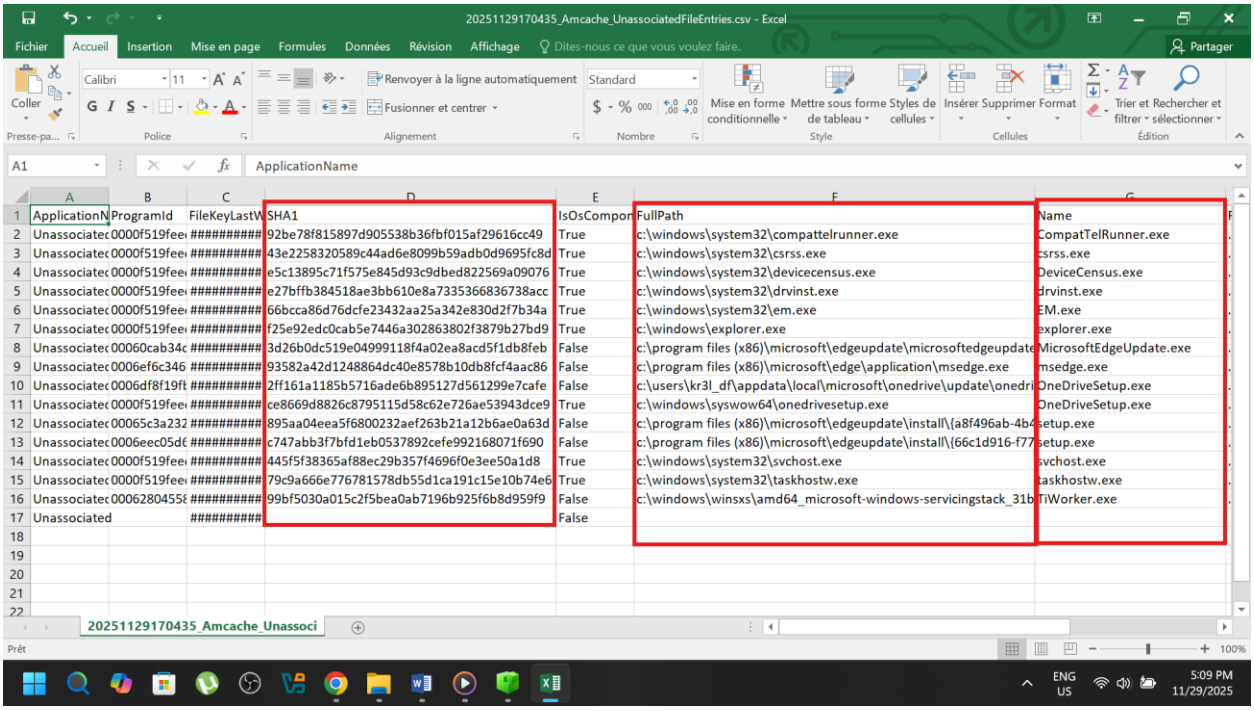
Analysis Method :

Parse AmCache Hive :

⇨ **AmcacheParser.exe -f C:\Users\NIZAR\Desktop\Cases\E\Windows\AppCompat\Programs\Amcache.hve --csv C:\Users\NIZAR\Desktop**



Successfully executing AmcacheParser to extract program execution data from AmCache.hve registry hive



Complete list of executables and their metadata extracted from AmCache.hve registry hive

AmCache Update Behavior

Empty AmCache typically indicates either:

- Programs were never executed
- The hive hasn't been updated yet

AmCache updates primarily occur when:

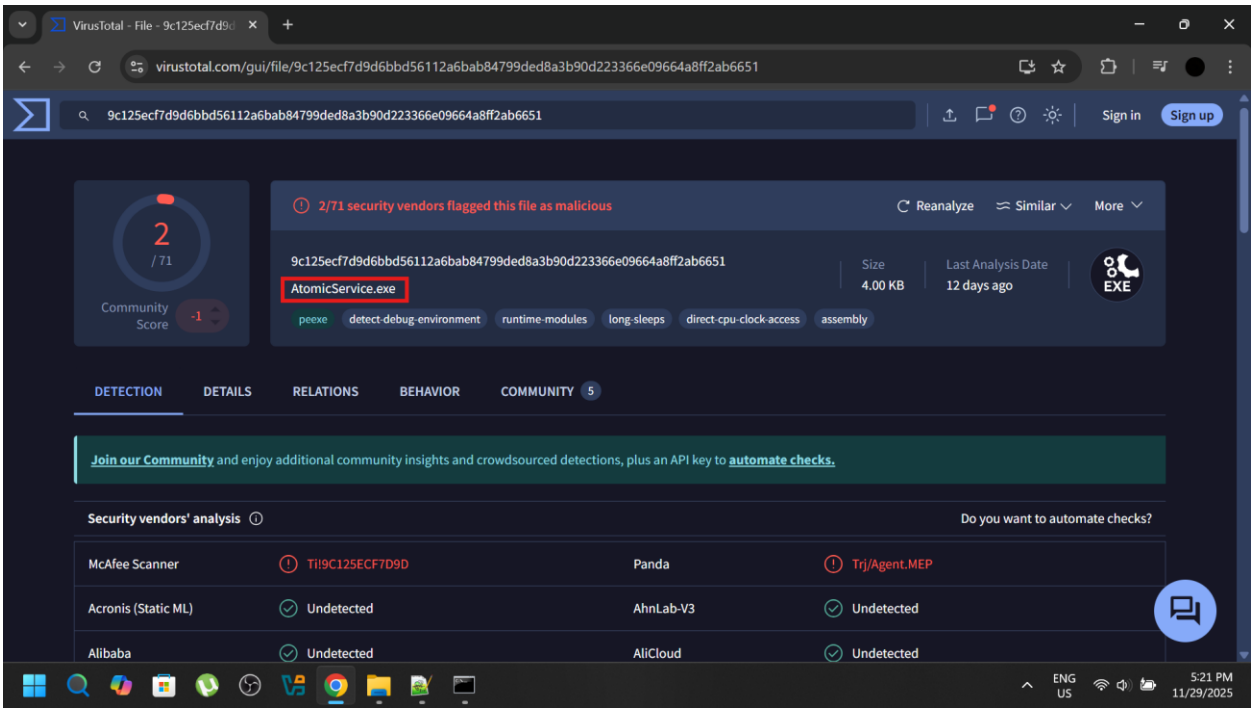
- Binaries are executed
- Scheduled tasks run (like Application Experience service)

Proactive Investigation Step :

To ensure comprehensive data, I ran the **Microsoft Compatibility Appraiser** to force **AmCache updates**, allowing us to identify **currently active malware**.

Critical Finding

Malware Hash Identified: c51217ce3d1959e99886a567d21d0b97022bd6e3 **(AtomicService.exe)**



The hash flagged as malicious in VirusTotal analysis

5. Prefetch Analysis

What is Prefetch?

Prefetch is a **Windows optimization feature that speeds up application startup by storing execution data**, creating valuable forensic artifacts that track program usage patterns.

Prefetch File Location:

⇨ **C:\Windows\Prefetch*.pf**

Forensic Value of Prefetch :

- **Executable names and file paths**
- **First and last execution timestamps**
- **Execution count** (how many times run)
- **Referenced files/DLLs used by applications**

- **Volume information and file locations**

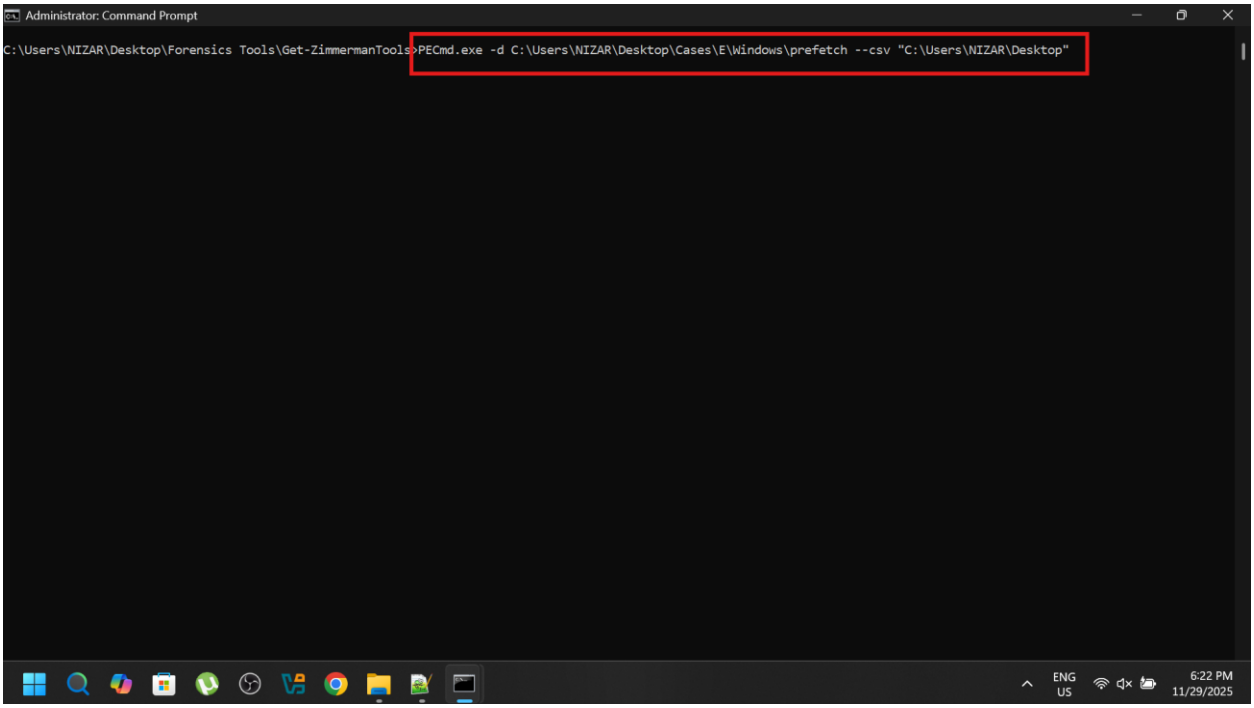
Key Characteristics :

- **Desktop Windows only** (not default on Server versions)
- **Limited storage** (128-1024 files, older ones overwritten)
- **File naming:** EXECUTABLE-RANDOMHASH.pf
- **Different hash =** different file location/path

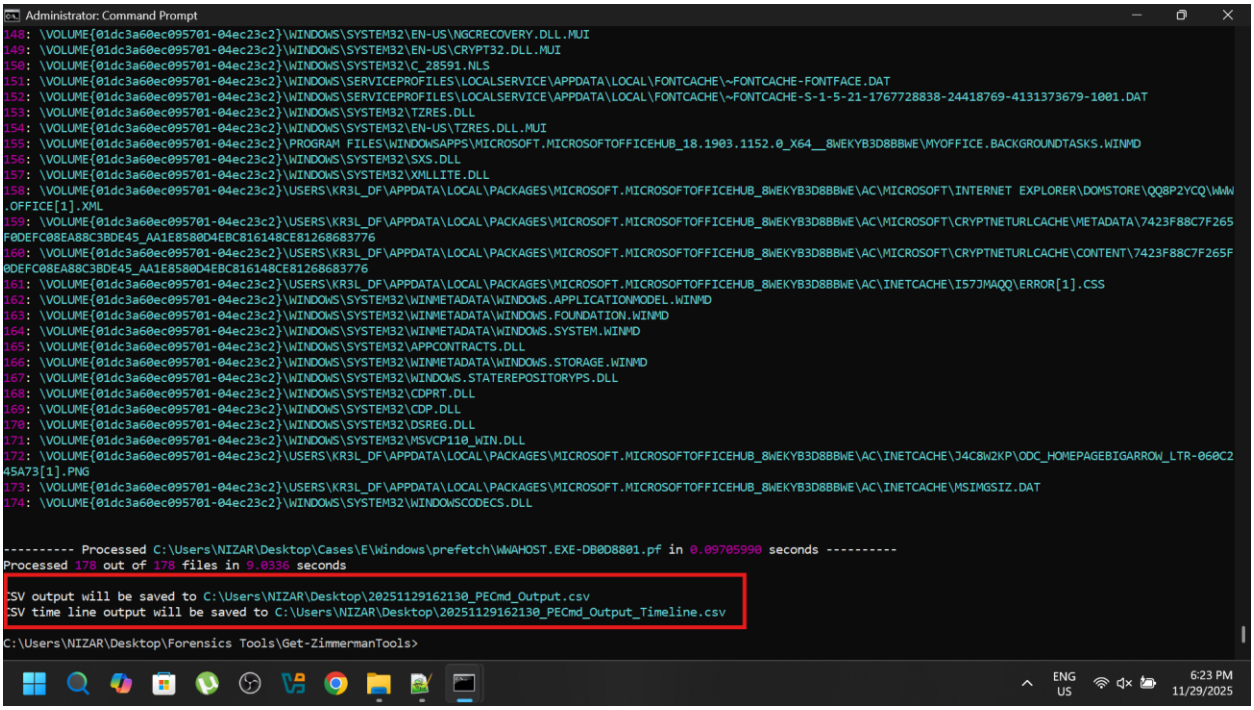
Analysis Method :

Prefetch Parsing Command :

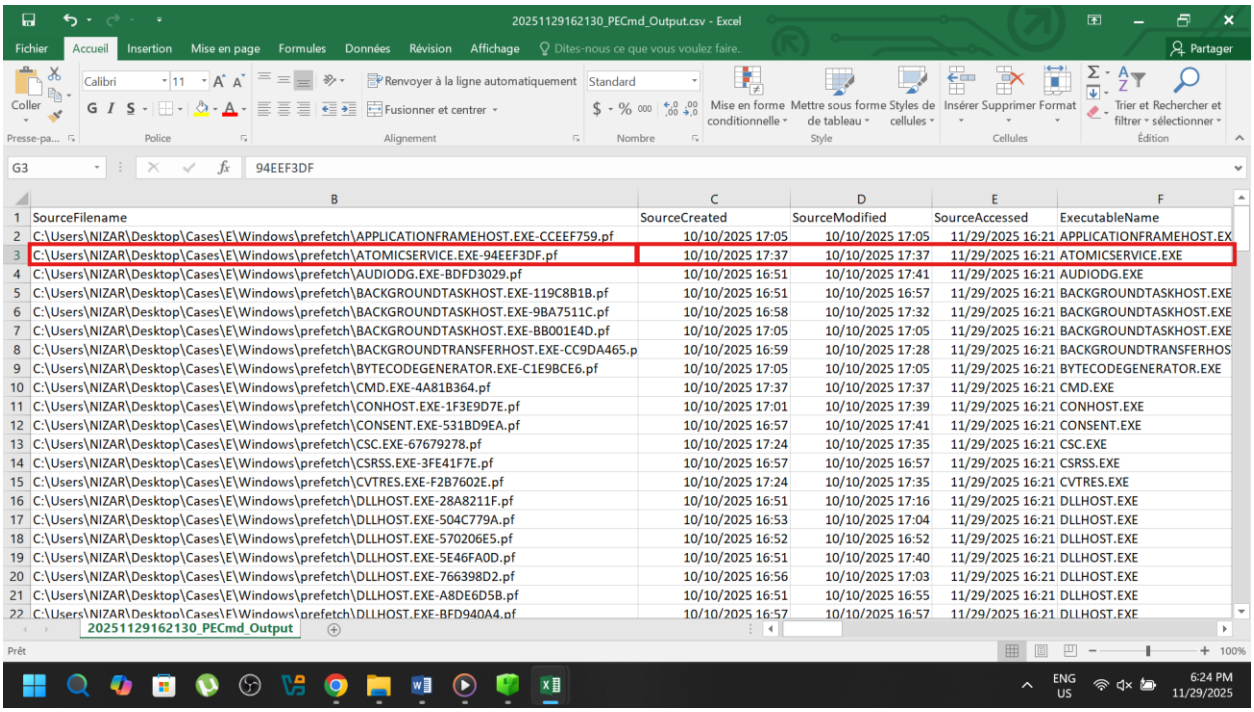
⇨ **PECmd.exe -d C:\Users\NIZAR\Desktop\Cases\E\Windows\prefetch --csv "C:\Users\NIZAR\Desktop"**



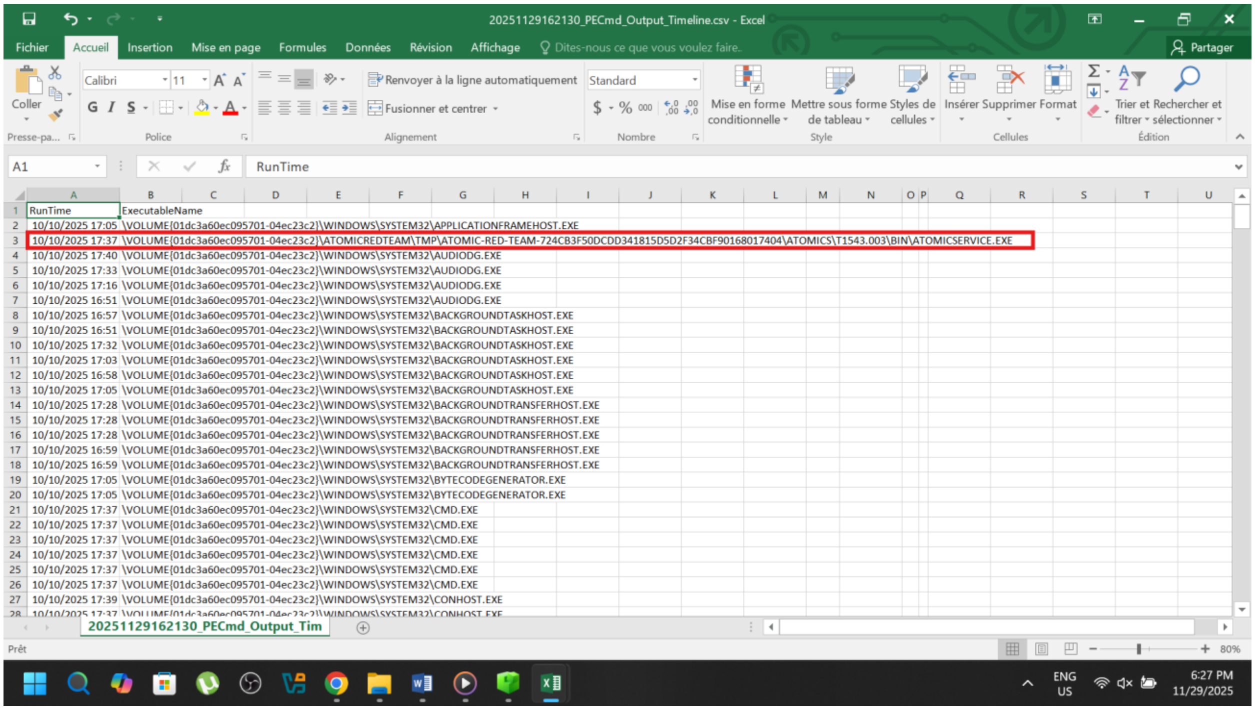
Executing PECmd to parse Windows Prefetch files and generate execution timeline data



PECmd executed successfully, Prefetch analysis completed and CSV exported



Prefetch analysis showing ATOMICSERVICE.EXE execution, confirming Atomic Red Team tool usage



RunTime	ExecutableName
10/10/2025 17:05	\VOLUME{01dc3a60ec095701-04ec23c2}\WINDOWS\SYSTEM32\APPLICATIONFRAMEHOST.EXE
10/10/2025 17:37	\VOLUME{01dc3a60ec095701-04ec23c2}\ATOMICREDTEAM\TMP\ATOMIC-RED-TEAM-724CB3F50DCDD341815D5D2F34CBF90168017404\ATOMICS\T1543.003\BIN\ATOMICSERVICE.EXE
10/10/2025 17:40	\VOLUME{01dc3a60ec095701-04ec23c2}\WINDOWS\SYSTEM32\AUDIODG.EXE
10/10/2025 17:33	\VOLUME{01dc3a60ec095701-04ec23c2}\WINDOWS\SYSTEM32\AUDIODG.EXE
10/10/2025 17:16	\VOLUME{01dc3a60ec095701-04ec23c2}\WINDOWS\SYSTEM32\AUDIODG.EXE
10/10/2025 16:51	\VOLUME{01dc3a60ec095701-04ec23c2}\WINDOWS\SYSTEM32\AUDIODG.EXE
10/10/2025 16:57	\VOLUME{01dc3a60ec095701-04ec23c2}\WINDOWS\SYSTEM32\BACKGROUNDTASKHOST.EXE
10/10/2025 16:51	\VOLUME{01dc3a60ec095701-04ec23c2}\WINDOWS\SYSTEM32\BACKGROUNDTASKHOST.EXE
10/10/2025 17:32	\VOLUME{01dc3a60ec095701-04ec23c2}\WINDOWS\SYSTEM32\BACKGROUNDTASKHOST.EXE
10/10/2025 17:03	\VOLUME{01dc3a60ec095701-04ec23c2}\WINDOWS\SYSTEM32\BACKGROUNDTASKHOST.EXE
10/10/2025 16:58	\VOLUME{01dc3a60ec095701-04ec23c2}\WINDOWS\SYSTEM32\BACKGROUNDTASKHOST.EXE
10/10/2025 17:05	\VOLUME{01dc3a60ec095701-04ec23c2}\WINDOWS\SYSTEM32\BACKGROUNDTASKHOST.EXE
10/10/2025 17:28	\VOLUME{01dc3a60ec095701-04ec23c2}\WINDOWS\SYSTEM32\BACKGROUNDTRANSFERHOST.EXE
10/10/2025 17:28	\VOLUME{01dc3a60ec095701-04ec23c2}\WINDOWS\SYSTEM32\BACKGROUNDTRANSFERHOST.EXE
10/10/2025 17:28	\VOLUME{01dc3a60ec095701-04ec23c2}\WINDOWS\SYSTEM32\BACKGROUNDTRANSFERHOST.EXE
10/10/2025 16:59	\VOLUME{01dc3a60ec095701-04ec23c2}\WINDOWS\SYSTEM32\BACKGROUNDTRANSFERHOST.EXE
10/10/2025 16:59	\VOLUME{01dc3a60ec095701-04ec23c2}\WINDOWS\SYSTEM32\BACKGROUNDTRANSFERHOST.EXE
10/10/2025 17:05	\VOLUME{01dc3a60ec095701-04ec23c2}\WINDOWS\SYSTEM32\BYTECODEGENERATOR.EXE
10/10/2025 17:05	\VOLUME{01dc3a60ec095701-04ec23c2}\WINDOWS\SYSTEM32\BYTECODEGENERATOR.EXE
10/10/2025 17:37	\VOLUME{01dc3a60ec095701-04ec23c2}\WINDOWS\SYSTEM32\CMD.EXE
10/10/2025 17:37	\VOLUME{01dc3a60ec095701-04ec23c2}\WINDOWS\SYSTEM32\CMD.EXE
10/10/2025 17:37	\VOLUME{01dc3a60ec095701-04ec23c2}\WINDOWS\SYSTEM32\CMD.EXE
10/10/2025 17:37	\VOLUME{01dc3a60ec095701-04ec23c2}\WINDOWS\SYSTEM32\CMD.EXE
10/10/2025 17:37	\VOLUME{01dc3a60ec095701-04ec23c2}\WINDOWS\SYSTEM32\CMD.EXE
10/10/2025 17:37	\VOLUME{01dc3a60ec095701-04ec23c2}\WINDOWS\SYSTEM32\CMD.EXE
10/10/2025 17:39	\VOLUME{01dc3a60ec095701-04ec23c2}\WINDOWS\SYSTEM32\CONHOST.EXE
10/10/2025 17:37	\VOLUME{01dc3a60ec095701-04ec23c2}\WINDOWS\SYSTEM32\CONHOST.EXE

ATOMICSERVICE.EXE last executed at 2025-10-10 17:37:43 - confirming red team activity timestamp

Key Findings & Analysis :

1. Suspicious or Unusual Executables

ATOMICSERVICE.EXE was executed from:

⇨ **\ATOMICREDTEAM\TMP\ATOMIC-RED-TEAM ...\ATOMICS\T1543.003 \BIN\ATOMICSERVICE.EXE**

- **This path** strongly suggests **Atomic Red Team**, a **well-known adversary simulation framework** used **for testing security controls**.
- **MITRE ATT&CK Technique: T1543.003** – **Create or Modify System Process**: Windows Service

2. Powershell Activity

- **CONHOST.EXE** and **POWERSHELL.EXE** were executed **multiple times**.
- **PowerShell** is commonly **used for legitimate administration** but also **for post-exploitation** and **lateral movement.**

3. Scheduled Task Activity

SCHTASKS.EXE was launched via **CMD.EXE**, indicating **possible scheduled task creation or modification**.

4. User-Level Persistence Attempt

CMD.EXE referenced:

- ⇨ **\USERS\KR3L_DF\APPDATA\ROAMING\MICROSOFT\WINDOWS\START MENU\PROGRAMS\STARTUP\BATSTARTUP.BAT**

This is a startup script location for persistence

5. Background Tasks Hosts & DLL Hosts

Multiple instances of **BACKGROUNDTASKHOST.EXE** and **DLLHOST.EXE** were launched, some associated with:

- Content Delivery Manager
- AAD Broker Plugin
- Microsoft Office Hub
- **These are typically legitimate but can be abused for code execution.**

6. Compilation Activity

CSC.EXE (C# Compiler) and **CVTRES.EXE** (Resource Converter) were executed, suggesting on-the-fly compilation of **C# code**, often seen **in offensive toolkits**.

7. Timeline of interest

- **Most activity** occurred between **16:51** and **17:41** on **2025-10-10.**
- Multiple **CONHOST.EXE** and **DLLHOST.EXE** instances **suggest interactive** or **scripted sessions.**