

Malware Dynamic Analysis Report



INTRODUCTION



The purpose of this report is to document the dynamic analysis performed on an executable malware sample located in the folder Esercizio_Pratico_U3_W2_L2 on the desktop of the virtual machine dedicated to malware analysis. The primary objectives of this analysis were:

- Detect registry changes after malware execution.
- Identify malware actions related to processes and threads using Process Monitor (Procmon).
- Track file system modifications caused by the malware using Process Monitor (Procmon).
- Profile the malware by analyzing the correlation between Operation and Path in logged events.

Virtual Machine Setup

To begin, I configured a Windows 7 virtual machine (VM). To ensure system recovery in case of issues, I created a snapshot of the VM using VirtualBox. This step is critical for quickly restoring the system to its initial state if the malware severely compromises system integrity.

Tools Used

Process Monitor (Procmon):

Process Monitor is an advanced tool for real-time monitoring of file system, registry, process, and thread activity. It is part of the Sysinternals suite and provides detailed information about each event, including operations performed, paths involved, results, and process details. The main features include:

- Monitoring of file system, registry, network, and process/thread operations.
- Filtering and searching for specific events to simplify analysis.
- Detailed view of each event with process information, duration, and result.

Analysis Procedure

- **Monitoring Tools Initialization:**

I launched Process Monitor (Procmon) to track all file system, process, and thread operations. I configured Procmon filters to specifically capture malware-related activities.

- **Malware Execution:**

I executed the malware and allowed it to run for a sufficient period to record all its activities. During this time, Procmon logged all operations performed by the malware.

- **Capture Termination and Data Analysis:**

After collecting enough data, I stopped the capture in Procmon and began a detailed analysis of the recorded operations. I used Procmon's filtering features to identify relevant actions, such as:

- File creation
- Registry key access
- Process creation

10:37:...	Malware_U3_...	2836	QueryNameInfo... C:\Windows\SysWOW64\svchost.exe	SUCCESS	Name: \Windows\...
10:37:...	Malware_U3_...	2836	Process Create C:\Windows\SysWOW64\svchost.exe	SUCCESS	PID: 2860, Comm...
10:37:...	svchost.exe	2860	Process Start	SUCCESS	Parent PID: 2836, ...
10:37:...	svchost.exe	2860	Thread Create	SUCCESS	Thread ID: 2864
10:37:00.6023318	je_U3_...	2836	RegOpenKey HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: Q...
10:37:...	Malware_U3_...	2836	RegOpenKey HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Desired Access: Q...
10:37:...	Malware_U3_...	2836	RegOpenKey HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: Q...
10:37:...	Malware_U3_...	2836	RegOpenKey HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Desired Access: Q...
10:37:...	Malware_U3_...	2836	RegOpenKey HKLM\Software\Wow6432Node\Polic...	REPARSE	Desired Access: Q...
10:37:...	Malware_U3_...	2836	RegOpenKey HKLM\SOFTWARE\Policies\Microsoft\...	SUCCESS	Desired Access: Q...
10:37:...	Malware_U3_...	2836	RegOpenKey HKLM\SOFTWARE\Policies\Microsoft\...	SUCCESS	KeySetInformation...
10:37:...	Malware_U3_...	2836	RegQueryValue HKLM\SOFTWARE\Policies\Microsoft\...	NAME NOT FOUND	Length: 80
10:37:...	Malware_U3_...	2836	RegQueryValue HKLM\SOFTWARE\Policies\Microsoft\...	SUCCESS	Type: REG_DWO...
10:37:...	Malware_U3_...	2836	RegCloseKey HKLM\SOFTWARE\Policies\Microsoft\...	SUCCESS	
10:37:...	Malware_U3_...	2836	RegOpenKey HKCU\Software\Policies\Microsoft\Win...	NAME NOT FOUND	Desired Access: Q...
10:37:...	Malware_U3_...	2836	RegOpenKey HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: Q...
10:37:...	Malware_U3_...	2836	RegOpenKey HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Desired Access: Q...
10:37:...	Malware_U3_...	2836	RegOpenKey HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: Q...
10:37:...	Malware_U3_...	2836	RegOpenKey HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Desired Access: Q...
10:37:...	Malware_U3_...	2836	RegOpenKey HKLM\Software\Wow6432Node\Polic...	REPARSE	Desired Access: Q...
10:37:...	Malware_U3_...	2836	RegOpenKey HKLM\SOFTWARE\Policies\Microsoft\...	NAME NOT FOUND	Desired Access: Q...
10:37:...	Malware_U3_...	2836	RegQueryValue HKLM\SOFTWARE\Policies\Microsoft\...	NAME NOT FOUND	Length: 80
10:37:...	Malware_U3_...	2836	RegQueryValue HKLM\SOFTWARE\Policies\Microsoft\...	SUCCESS	
10:37:...	Malware_U3_...	2836	RegCloseKey HKLM\SOFTWARE\Policies\Microsoft\...	SUCCESS	
10:37:...	Malware_U3_...	2836	RegOpenKey HKCU\Software\Policies\Microsoft\Win...	NAME NOT FOUND	Desired Access: Q...
10:37:...	Malware_U3_...	2836	RegOpenKey HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: Q...
10:37:...	Malware_U3_...	2836	RegOpenKey HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Desired Access: Q...
10:37:...	Malware_U3_...	2836	RegOpenKey HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: Q...
10:37:...	Malware_U3_...	2836	RegOpenKey HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Desired Access: Q...
10:37:...	Malware_U3_...	2836	RegOpenKey HKLM\Software\Wow6432Node\Polic...	REPARSE	Desired Access: Q...
10:37:...	Malware_U3_...	2836	RegOpenKey HKLM\SOFTWARE\Policies\Microsoft\...	NAME NOT FOUND	Desired Access: Q...
10:37:...	Malware_U3_...	2836	RegQueryValue HKLM\SOFTWARE\Policies\Microsoft\...	NAME NOT FOUND	Length: 80
10:37:...	Malware_U3_...	2836	RegQueryValue HKLM\SOFTWARE\Policies\Microsoft\...	SUCCESS	
10:37:...	Malware_U3_...	2836	RegCloseKey HKLM\SOFTWARE\Policies\Microsoft\...	SUCCESS	
10:37:...	Malware_U3_...	2836	QueryBasicInfor... C:\Windows\SysWOW64\svchost.exe	SUCCESS	Information: Owner...
10:37:...	Malware_U3_...	2836	CreateFile C:\Windows\SysWOW64\apphelp.dll	SUCCESS	CreationTime: 14/0...
10:37:...	Malware_U3_...	2836	QueryBasicInfor... C:\Windows\SysWOW64\apphelp.dll	SUCCESS	Desired Access: R...
10:37:...	Malware_U3_...	2836	CloseFile C:\Windows\SysWOW64\apphelp.dll	SUCCESS	CreationTime: 21/1...
10:37:...	Malware_U3_...	2836	CreateFile C:\Windows\SysWOW64\apphelp.dll	SUCCESS	Desired Access: R...
10:37:...	Malware_U3_...	2836	CreateFileMapp... C:\Windows\SysWOW64\apphelp.dll	SUCCESS	FILE LOCKED WI... SyncType: SyncTy...
10:37:...	Malware_U3_...	2836	CreateFileMapp... C:\Windows\SysWOW64\apphelp.dll	SUCCESS	SyncType: SyncTy...
10:37:...	Malware_U3_...	2836	Load Image C:\Windows\SysWOW64\apphelp.dll	SUCCESS	Image Base: 0x74a...
10:37:...	Malware_U3_...	2836	CloseFile C:\Windows\SysWOW64\apphelp.dll	SUCCESS	
10:37:...	Malware_U3_...	2836	Load Image C:\Windows\SysWOW64\svchost.exe	SUCCESS	
10:37:...	Malware_U3_...	2836	CreateFile C:\Windows\AppPatch\sysmain.sdb	SUCCESS	Desired Access: G...
10:37:...	Malware_U3_...	2836	QueryStandard... C:\Windows\AppPatch\sysmain.sdb	SUCCESS	AllocationSize: 4.0...
10:37:...	Malware_U3_...	2836	CreateFileMapp... C:\Windows\AppPatch\sysmain.sdb	FILE LOCKED WI...	SyncType: SyncTy...
10:37:...	Malware_U3_...	2836	QueryStandard... C:\Windows\AppPatch\sysmain.sdb	SUCCESS	AllocationSize: 4.0...
10:37:...	Malware_U3_...	2836	CreateFileMapp... C:\Windows\AppPatch\sysmain.sdb	SUCCESS	SyncType: SyncTy...
10:37:...	Malware_U3_...	2836	QueryStandard... C:\Windows\AppPatch\sysmain.sdb	SUCCESS	AllocationSize: 4.0...
10:37:...	Malware_U3_...	2836	CreateFile C:\Windows\SysWOW64	SUCCESS	Desired Access: R...
10:37:...	Malware_U3_...	2836	QueryDirectory C:\Windows\SysWOW64\svchost.exe	SUCCESS	Desired Access: R...
10:37:...	Malware_U3_...	2836	CloseFile C:\Windows\SysWOW64	SUCCESS	Filter: svchost.exe, ...

The screenshot shows the Process Monitor interface with a list of captured events and an open 'Event Properties' dialog. The main window displays a table of events with columns: Time, Process Name, PID, Operation, Path, Result, and Detail. The 'Detail' column provides specific information about each operation, such as file paths and registry keys. The 'Event Properties' dialog is open for a specific event, showing details like Date (11/06/2024 10:37:00.60113%), Thread (2840), Class (File System), Operation (CreateFile), Result (SUCCESS), Path (C:\Windows), and Duration (0.0000074). It also lists Desired Access, Disposition, Options, Attributes, ShareMode, AllocationSize, and OpenResult. The bottom right of the dialog has buttons for Copy All and Close.

Analysis Results PT1

Malware File System Actions:

The malware performed numerous file creation, read, and write operations. Below are some significant examples:

- **CreateFile:** The malware created files in critical directories such as C:\Windows\SysWOW64 and C:\Windows\System32.
- **ReadFile/WriteFile:** It read from and wrote to existing files, potentially modifying system file contents.

A notable example is the CreateFile operation in C:\Windows\SysWOW64, which may indicate an attempt at persistence or system file tampering.

Malware Process and Thread Actions:

The malware created new processes and threads. Observed operations include:

- **Process Create:** Spawned new processes, including multiple svchost.exe instances that could be used to conceal malicious activity.
- **Thread Create:** Created new threads within existing processes, suggesting potential code injection into legitimate processes to execute operations.

Analysis Results PT2

Registry Modifications After Malware Execution

Using Process Monitor (Procmon), I identified multiple registry operations indicating significant changes:

- RegSetValue and RegCreateKey:

The malware created and modified registry keys to:

- Enable automatic execution at system startup
- Potentially alter security configurations

- Added keys under:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run

(Ensures malware persistence via auto-start)

- Modified security configuration keys under:

- HKCU\Software\Microsoft\Windows\CurrentVersion\Policies

(Suggests attempts to weaken system defenses)

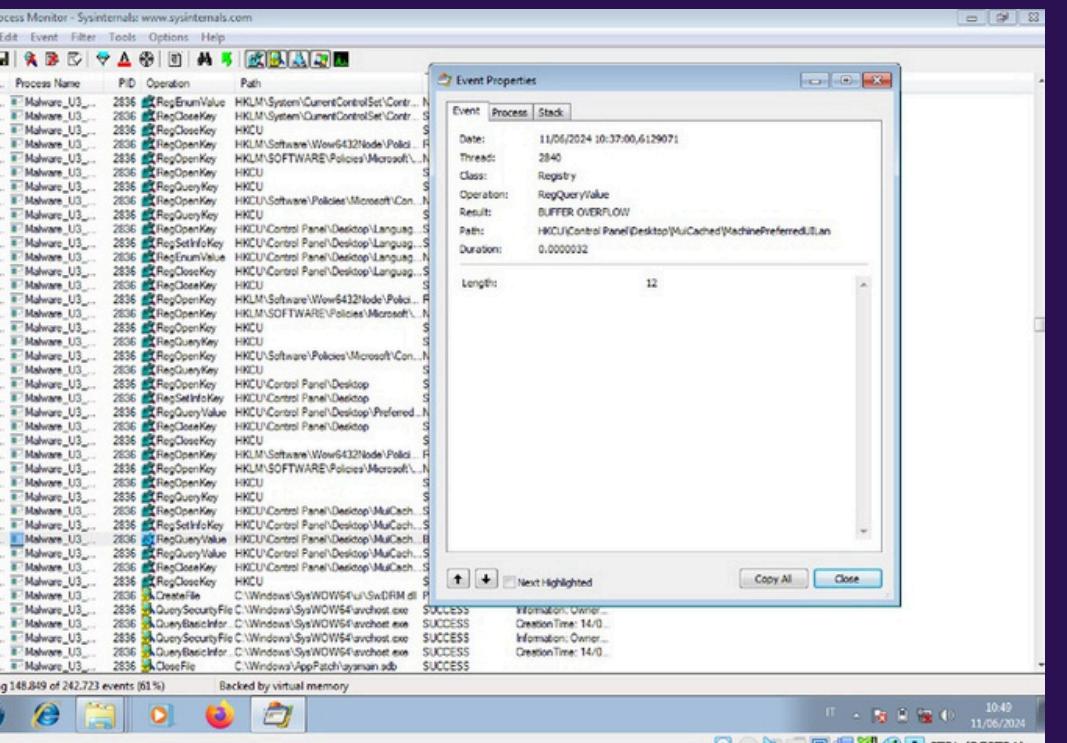
Malware Profiling

I correlated operations (CreateFile, ReadFile, WriteFile, Process Create) with specific paths:

- CreateFile in C:\Windows\SysWOW64:
Indicates attempts to tamper with/replace system files.
- Process Create spawning svchost.exe:
Suggests code execution under a legitimate system process to evade detection.
- Registry modifications for persistence:
Confirms the malware maintains execution capability after system reboot.

10.37...	Malware_U3...	2836	RegOpenKey	HKEY\SYSTEM\CurrentControlSet\Contro...	REPARSE	Desired Access: R...
10.37...	Malware_U3...	2836	RegOpenKey	HKEY\SYSTEM\CurrentControlSet\Contro...	SUCCESS	Desired Access: R...
10.37...	Malware_U3...	2836	RegSetInfoKey	HKEY\SYSTEM\CurrentControlSet\Contro...	SUCCESS	KeySetInformation...
10.37...	Malware_U3...	2836	RegQueryValue	HKEY\SYSTEM\CurrentControlSet\Contro...	NAME NOT FOUND Length: 548	
10.37...	Malware_U3...	2836	RegQueryValue	HKEY\SYSTEM\CurrentControlSet\Contro...	SUCCESS	Type: REG_DWO...
10.37...	Malware_U3...	2836	RegCloseKey	HKEY\SYSTEM\CurrentControlSet\Contro...	SUCCESS	
10.37...	Malware_U3...	2836	RegOpenKey	HKEY\SYSTEM\CurrentControlSet\Contro...	REPARSE	Desired Access: Q...
10.37...	Malware_U3...	2836	RegOpenKey	HKEY\SYSTEM\CurrentControlSet\Contro...	NAME NOT FOUND	Desired Access: Q...
10.37...	Malware_U3...	2836	RegOpenKey	HKEY\SYSTEM\CurrentControlSet\Contro...	REPARSE	Desired Access: R...
10.37...	Malware_U3...	2836	RegOpenKey	HKEY\SYSTEM\CurrentControlSet\Contro...	NAME NOT FOUND	Desired Access: R...
10.37...	Malware_U3...	2836	RegOpenKey	HKEY\Software\Wow64Node\Policy\...	REPARSE	Desired Access: Q...
10.37...	Malware_U3...	2836	RegOpenKey	HKEY\SOFTWARE\Policies\Microsoft\...	SUCCESS	Desired Access: Q...
10.37...	Malware_U3...	2836	RegSetInfoKey	HKEY\SOFTWARE\Policies\Microsoft\...	SUCCESS	KeySetInformation...
10.37...	Malware_U3...	2836	RegQueryValue	HKEY\SOFTWARE\Policies\Microsoft\...	NAME NOT FOUND Length: 80	
10.37...	Malware_U3...	2836	RegQueryValue	HKEY\SOFTWARE\Policies\Microsoft\...	SUCCESS	
10.37...	Malware_U3...	2836	RegCloseKey	HKEY\SOFTWARE\Policies\Microsoft\...	SUCCESS	
10.37...	Malware_U3...	2836	RegOpenKey	HKEY\Software\Policies\Microsoft\Win...	NAME NOT FOUND	Desired Access: Q...
10.37...	Malware_U3...	2836	RegOpenKey	HKEY\SYSTEM\CurrentControlSet\Contro...	REPARSE	Desired Access: R...
10.37...	Malware_U3...	2836	RegSetInfoKey	HKEY\SYSTEM\CurrentControlSet\Contro...	SUCCESS	KeySetInformation...
10.37...	Malware_U3...	2836	RegQueryValue	HKEY\SYSTEM\CurrentControlSet\Contro...	SUCCESS	Type: REG_SZ, Le...
10.37...	Malware_U3...	2836	ReadFile	C:\Users\user\Desktop\MALWARE\Ea...	SUCCESS	Offset: 40,950, Len...
10.37...	Malware_U3...	2836	ReadFile	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Offset: 259,072, Le...
10.37...	Malware_U3...	2836	ReadFile	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Offset: 43,296, Le...
10.37...	Malware_U3...	2836	RegOpenKey	HKEY\SYSTEM\CurrentControlSet\Contro...	REPARSE	Desired Access: Q...
10.37...	Malware_U3...	2836	RegOpenKey	HKEY\SYSTEM\CurrentControlSet\Contro...	SUCCESS	Desired Access: Q...
10.37...	Malware_U3...	2836	RegSetInfoKey	HKEY\SYSTEM\CurrentControlSet\Contro...	SUCCESS	KeySetInformation...
10.37...	Malware_U3...	2836	RegQueryValue	HKEY\SYSTEM\CurrentControlSet\Contro...	NAME NOT FOUND Length: 16	
10.37...	Malware_U3...	2836	CreateFile	C:\Windows\SysWOW64\svchost.exe	SUCCESS	Desired Access: R...
10.37...	Malware_U3...	2836	CreateFileMapping...	C:\Windows\SysWOW64\svchost.exe	FILE LOCKED WI...	SyncType: SyncTy...
10.37...	Malware_U3...	2836	QueryStandardI...	C:\Windows\SysWOW64\svchost.exe	SUCCESS	AllocationSize: 24...
10.37...	Malware_U3...	2836	ReadFile	C:\Windows\SysWOW64\svchost.exe	SUCCESS	Offset: 0, Length: 4...
10.37...	Malware_U3...	2836	ReadFile	C:\Windows\SysWOW64\svchost.exe	SUCCESS	Offset: 19,968, Len...
10.37...	Malware_U3...	2836	CreateFileMapping...	C:\Windows\SysWOW64\svchost.exe	SUCCESS	SyncType: SyncTy...
10.37...	Malware_U3...	2836	RegOpenKey	HKEY\SOFTWARE\Microsoft\WIN_...	NAME NOT FOUND	Desired Access: Q...
10.37...	Malware_U3...	2836	QuerySecurityFile	C:\Windows\SysWOW64\svchost.exe	SUCCESS	Information: Label
10.37...	Malware_U3...	2836	ReadFile	C:\Windows\SysWOW64\svchost.exe	SUCCESS	Offset: 1,024, Len...
10.37...	Malware_U3...	2836	ReadFile	C:\Windows\SysWOW64\svchost.exe	SUCCESS	Offset: 17,408, Len...
10.37...	Malware_U3...	2836	QueryNameInfo...	C:\Windows\SysWOW64\svchost.exe	SUCCESS	Name: '\Windows\'...
10.37...	Malware_U3...	2836	Process Create	C:\Windows\SysWOW64\svchost.exe	SUCCESS	PID: 2860, Comma...

U3...	2836	QueryDirectory	C:\Windows	SUCCESS	Filter: Windows, 1:...
U3...	2836	QueryDirectory	C:\Windows	SUCCESS	Filter: system32, 1:...
U3...	2836	CreateFile	C:\Windows	SUCCESS	Desired Access: R...
U3...	2836	QueryDirectory	C:\Windows\SysWOW64\avchost.exe	SUCCESS	Desired Access: R...
U3...	2836	CloseFile	C:\Windows	SUCCESS	Filter: avchost.exe, ...
U3...	2836	CreateFile	C:\Windows\SysWOW64	SUCCESS	Desired Access: R...
U3...	2836	QueryDirectory	C:\Windows\SysWOW64\avchost.exe	SUCCESS	Desired Access: R...
U3...	2836	CloseFile	C:\Windows	SUCCESS	Filter: avchost.exe, ...
U3...	2836	RegOpenKey	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	SUCCESS	Desired Access: Q...
U3...	2836	RegSetInfoKey	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	SUCCESS	KeySetInformation...
U3...	2836	RegQueryValue	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	SUCCESS	Type: REG_SZ, Le...
U3...	2836	RegCloseKey	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	SUCCESS	
U3...	2836	RegOpenKey	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run	NAME NOT FOUND	Desired Access: R...
U3...	2836	RegOpenKey	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run	NAME NOT FOUND	Desired Access: R...
U3...	2836	RegOpenKey	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run	NAME NOT FOUND	Desired Access: R...
U3...	2836	CreateFile	C:\Windows\SysWOW64	SUCCESS	Desired Access: R...
U3...	2836	QueryDirectory	C:\Windows\SysWOW64*\	SUCCESS	Filter: *, 1:...
U3...	2836	QueryDirectory	C:\Windows\SysWOW64	SUCCESS	0: ..., 1: 0410, 2: 12...
U3...	2836	QueryDirectory	C:\Windows\SysWOW64	SUCCESS	0: apda.dll, 1: apm...
U3...	2836	QueryDirectory	C:\Windows\SysWOW64	SUCCESS	0: apime-win-core...
U3...	2836	QueryDirectory	C:\Windows\SysWOW64	SUCCESS	0: atmfld.dll, 1: atm...
U3...	2836	QueryDirectory	C:\Windows\SysWOW64	SUCCESS	0: bcryptprimitives...
U3...	2836	QueryDirectory	C:\Windows\SysWOW64	SUCCESS	0: catdrvps.dll, 1: c...
U3...	2836	QueryDirectory	C:\Windows\SysWOW64	SUCCESS	0: cleanmgr.exe, 1:...
U3...	2836	QueryDirectory	C:\Windows\SysWOW64	SUCCESS	0: compact.exe, 1: ...
U3...	2836	QueryDirectory	C:\Windows\SysWOW64	SUCCESS	0: csobj.dll, 1: csd...
U3...	2836	QueryDirectory	C:\Windows\SysWOW64	SUCCESS	0: C_1148.NLS, 1: ...
U3...	2836	QueryDirectory	C:\Windows\SysWOW64	SUCCESS	0: C_20423.NLS, 1: ...
U3...	2836	QueryDirectory	C:\Windows\SysWOW64	SUCCESS	0: C_855.NLS, 1: ...
U3...	2836	QueryDirectory	C:\Windows\SysWOW64	SUCCESS	0: d3dxof.dll, 1: d...
U3...	2836	QueryDirectory	C:\Windows\SysWOW64	SUCCESS	0: DevicePinningWA...
U3...	2836	QueryDirectory	C:\Windows\SysWOW64	SUCCESS	0: Dism.exe, 1: dis...
U3...	2836	QueryDirectory	C:\Windows\SysWOW64	SUCCESS	0: dot3c.dll, 1: dot...
U3...	2836	QueryDirectory	C:\Windows\SysWOW64	SUCCESS	0: dsksquid.dll, 1: ...
U3...	2836	QueryDirectory	C:\Windows\SysWOW64	SUCCESS	0: efsaud.dll, 1: efa...
U3...	2836	QueryDirectory	C:\Windows\SysWOW64	SUCCESS	0: expv.dll, 1: edr...
U3...	2836	QueryDirectory	C:\Windows\SysWOW64	SUCCESS	0: format.com, 1: fp...
U3...	2836	QueryDirectory	C:\Windows\SysWOW64	SUCCESS	0: gppmed.dll, 1: g...
U3...	2836	QueryDirectory	C:\Windows\SysWOW64	SUCCESS	0: iss.dll, 1: issocct...
U3...	2836	QueryDirectory	C:\Windows\SysWOW64	SUCCESS	0: leapfir.dll, 1: led...
U3...	2836	QueryDirectory	C:\Windows\SysWOW64	SUCCESS	0: infocardapi.dll, 1: ...



The screenshot shows the Windows 7 - malware analysis [In esecuzione] - Oracle VM VirtualBox interface at the top. Below it is the Process Monitor application window from Sysinternals.

Process Monitor - Sysinternals: www.sysinternals.com

The main table lists numerous file system operations (CreateFile, QueryFile, OpenFile, etc.) performed by the process **Malware_U3_** (PID: 2836). The operations involve paths such as **C:\Windows\Temp\app-patch\sysmain sub**, **C:\Windows\Temp\app-patch\sysmain sub**, **C:\Windows\SysWOW64**, and various registry keys under **HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run**.

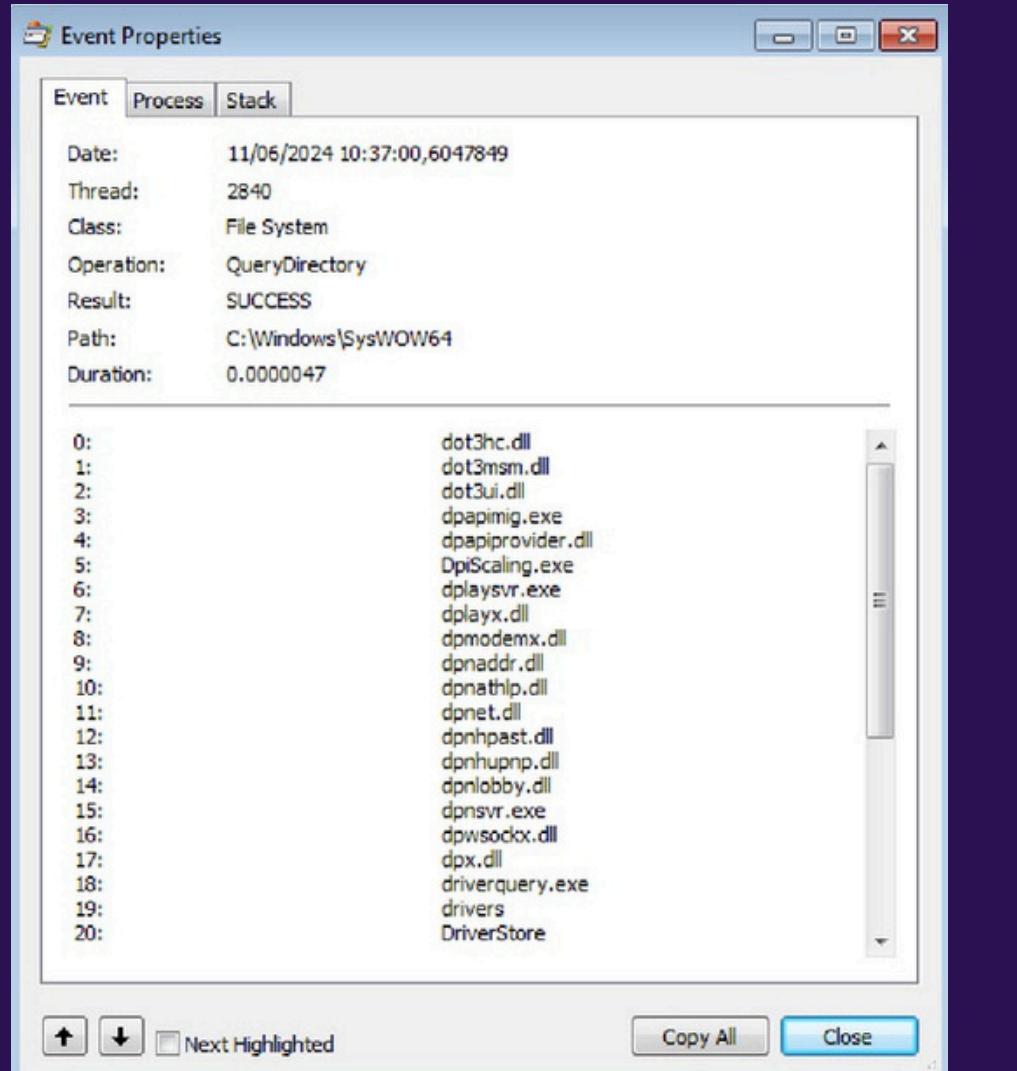
Event Properties dialog box (Event tab) details:

- Date: 11/06/2024 10:37:00,6037059
- Thread: 2840
- Class: File System
- Operations: CreateFile
- Result: SUCCESS
- Path: C:\Windows\SysWOW64
- Duration: 0.0000065

Event Properties dialog box (Details tab) details:

- Desired Access: Read Data/List Directory, Synchronize
- Disposition: Open
- Options: Directory, Synchronous IO Non-Alert
- Attributes: n/a
- ShareMode: Read, Write
- AllocationSize: n/a
- OpenResult: Opened

Buttons at the bottom of the dialog box include: Next Highlighted, Copy All, and Close.



Conclusion



The dynamic analysis revealed that the malware performs various malicious operations including modification of system files, creation of suspicious processes, and registry modifications to ensure persistence. The techniques employed by the malware involve alteration of critical directories and the use of legitimate processes to conceal its activities. Using tools like Procmon is critical for monitoring and analyzing such behaviors in order to develop effective defense measures against similar threats. This report provides a detailed overview of the malware's activities and the techniques used to identify and analyze them, serving as a practical example of how to conduct dynamic analysis in a controlled environment.