

I opened the explorer and navigated to the mouse configs. This led me to the following answers.

Registry Explorer v2.0.0.0

File Tools Options Bookmarks (29/0) View Help

Registry hives (1) Available bookmarks (29/0)

Enter text to search... Find

Key name	# values	# subkeys	Last write time
C:\Users\Administrator\Downloads\files...			
ROOT	0	10	2023-01-29 16:2
AppEvents	0	2	2023-01-29 09:3
Console	48	2	2023-01-29 09:3
Control Panel	0	14	2023-01-29 09:3
Accessibility	2	13	2023-01-29 09:3
Appearance	3	2	2023-01-29 09:3
Bluetooth	0	1	2023-01-29 09:3
Colors	31	0	2023-01-29 09:3
Cursors	20	0	2023-01-29 09:3
Desktop	45	2	2023-01-29 16:2
Input Method	1	1	2023-01-29 09:3
International	40	4	2023-01-29 09:3
Keyboard	3	0	2023-01-29 10:2
Mouse	18	0	2023-01-29 09:3
Personalization	0	1	2023-01-29 09:3
PowerCfg	1	2	2023-01-29 09:3
Quick Actions	0	2	2023-01-29 09:3
Sound	2	0	2023-01-29 09:3
Environment	4	0	2023-01-29 09:3
EUDC	0	4	2023-01-29 09:3
Keyboard Layout	0	3	2023-01-29 09:3
Network	0	0	2023-01-29 09:3
Printers	0	2	2023-01-29 09:5
SOFTWARE	0	9	2023-01-29 16:2
System	0	2	2023-01-29 09:3

Values

Drag a column header here to group by that column

Value Name	Value Type	Data
ActiveWindowTracking	RegDword	0
Beep	RegSz	No
DoubleClickHeight	RegSz	4
DoubleClickSpeed	RegSz	500
DoubleClickWidth	RegSz	4
ExtendedSounds	RegSz	No
MouseHoverHeight	RegSz	4
MouseHoverTime	RegSz	400
MouseHoverWidth	RegSz	4
MouseSensitivity	RegSz	10
MouseSpeed	RegSz	1
MouseThreshold1	RegSz	6
MouseThreshold2	RegSz	10
MouseTrails	RegSz	0
SmoothMouseXCurve	RegBinary	00-00-00-00-00-00-00-00-1
SmoothMouseYCurve	RegBinary	00-00-00-00-00-00-00-00-F

Type viewer Binary viewer

Value name ActiveWindowTracking

Value type RegDword

Value 0

**Answer 1A:** As we can see the DoubleClickSpeed is 500 ms.

Registry Explorer v2.0.0.0

File Tools Options Bookmarks (29/0) View Help

Registry hives (1) Available bookmarks (29/0)

paths

Find

Key name	# values	# subkeys	Last write time
C:\Users\Administrator\Downloads\files...			
ROOT	0	10	2023-01-29 16:2
SOFTWARE	0	9	2023-01-29 16:2
Microsoft	0	62	2023-01-29 16:2
Windows	0	7	2023-01-29 09:3
CurrentVersion	0	61	2023-01-29 16:2
App Paths	0	1	2023-01-29 09:3
Explorer	12	41	2023-01-29 16:2
TypedPaths	1	0	2023-01-29 16:2

Values

Drag a column header here to group by that column

Value Name	Value Type	Data
url1	RegSz	C:\Windows\System32\calc.exe

**Answer 1B:** The most recent typedpaths is the calc.exe.

**Answer 1C:** For the malware question, I looked up the commonly changed registry keys to achieve prestistace.

This allows the malware to persist even after the system has been rebooted.

Malware achieves persistence by modifying the registry keys in one of AutoStart Extention Points (ASEPs). Below are some of the registry keys that malware mostly achieves its persistence by editing the registry keys at the User Level:

- HKEY\_CURRENT\_USERSoftwareMicrosoftWindowsCurrentVersionRun
- HKEY\_CURRENT\_USERSoftwareMicrosoftWindowsCurrentVersionRunOnce

Finding these registry keys, I see the malware.exe .

Registry Explorer v2.0.0.0  
File Tools Options Bookmarks (29/0) View Help

Registry hives (1) Available bookmarks (29/0)

run

Key name	# values	# subkeys	Last write time
C:\Users\Administrator\Downloads\files...			
ROOT	0	10	2023-01-29 16:2
SOFTWARE	0	9	2023-01-29 16:2
Microsoft	0	62	2023-01-29 16:2
Windows	0	7	2023-01-29 09:3
CurrentVersion	0	61	2023-01-29 16:2
AppHost	0	1	2023-01-29 09:3
IndexedDB	0	89	2023-01-29 11:3
Microsoft.NET.Native.Run...	1	0	2023-01-29 09:3
Microsoft.NET.Native.Run...	1	0	2023-01-29 09:3
Explorer	12	41	2023-01-29 16:2
RunRU	0	0	2023-01-29 16:1
StartupApproved	0	2	2023-01-29 16:2
Run	0	0	2023-01-29 16:2
Run	3	0	2023-01-29 16:1
RunOnce	0	0	2023-01-29 11:2
Shell	0	3	2023-01-29 09:3
Associations	1	1	2023-01-29 09:3
UnAssociations	0	99	2023-01-29 11:3
ms-holographicfirstRun	0	0	2023-01-29 09:5

Values

Drag a column header here to group by that column

Value Name	Value Type	Data	Value Slack
OneDrive	RegSz	"C:\Users\w\AppData\Local\Microsoft\OneDrive\OneDrive.exe" /background	00-00-00-00-00-00
MicrosoftEdgeAutoLaunch_C8A64D2EF681E3E50136A28FC3C44893	RegSz	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --no-startup-window	00-58-00-C7-0A-31
Malware	RegSz	C:\Users\w\Desktop\malware.exe	00-00-78-00-65-00

Type viewer Slack viewer Binary viewer

Value name OneDrive

Value type RegSz

OneDrive	RegSz	"C:\Users\w\AppData\Local\Microsoft\OneDrive\OneD
MicrosoftEdgeAutoLaunch_C8A64D2EF681E3E50136A28FC3C44893	RegSz	"C:\Program Files (x86)\Microsoft\Edge\Application\ms
Malware	RegSz	C:\Users\w\Desktop\malware.exe

Hence this is the new value added to the registry by the virus.

## Answer 2A:

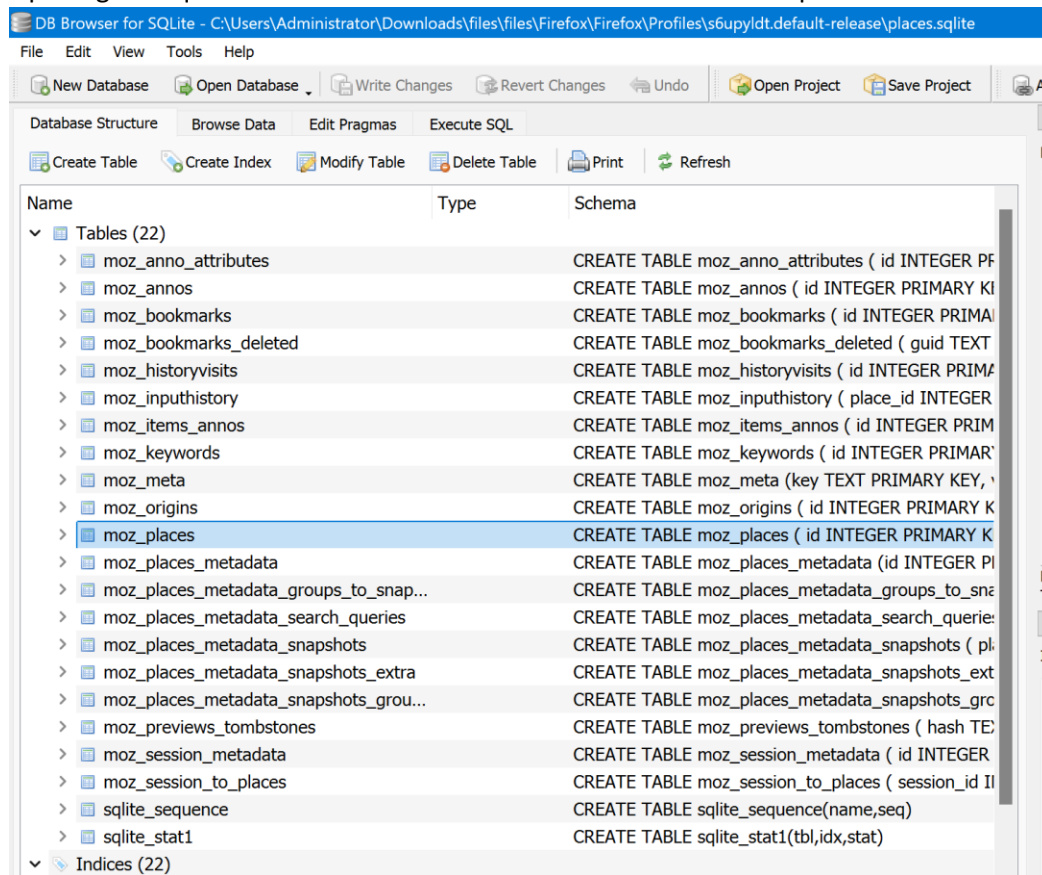
Running the decrypt tool and giving the firefox folder as an argument we see the answers.

```
PS C:\Users\Administrator\Downloads\firefox_decrypt-main\firefox_decrypt-main> python .\firefox_decrypt.py C:\Users\Administrator\Downloads\files\files\Firefox\Firefox
2024-08-27 10:37:10,905 - WARNING - Running with unsupported encoding 'locale': cp1252 - Things are likely to fail from here onwards
Select the Mozilla profile you wish to decrypt
1 -> Profiles/83bm17p1.default
2 -> Profiles/s6upyltd.default-release
2

Website: https://www.reddit.com
Username: 'hackerman'
Password: 'sup3rs3cur3p4ssw0rd'
PS C:\Users\Administrator\Downloads\firefox_decrypt-main\firefox_decrypt-main>
```

## Answer 2B:

Opening the sqlite database of in the default-release folder of the profiles.



Inside the Places.sqlite the moz\_places contains the tables for the browser history.

moz_meta	CREATE TABLE moz_meta (key TEXT PRIMARY KEY, value TEXT)
moz_origi	CREATE TABLE moz_origins ( id INTEGER PRIMARY KEY, url LONGVARCHAR, title LONGVARCHAR, rev_host LONGVARCHAR, visit_count INTEGER, hidden INTEGER, typed INTEGER, frecency INTEGER, last_visit_date INTEGER, guid TEXT, foreign_count INTEGER, url_hash INTEGER, description TEXT, preview_image_url TEXT, site_name TEXT, origin_id INTEGER)
moz_plac	CREATE TABLE moz_places ( id INTEGER PRIMARY KEY, url LONGVARCHAR, title LONGVARCHAR, rev_host LONGVARCHAR, visit_count INTEGER, hidden INTEGER, typed INTEGER, frecency INTEGER, last_visit_date INTEGER, guid TEXT, foreign_count INTEGER, url_hash INTEGER, description TEXT, preview_image_url TEXT, site_name TEXT, origin_id INTEGER)
id	INTEGER "id" INTEGER
url	LONGVARCHAR "url" LONGVARCHAR
title	LONGVARCHAR "title" LONGVARCHAR
rev_host	LONGVARCHAR "rev_host" LONGVARCHAR
visit_count	INTEGER "visit_count" INTEGER DEFAULT 0
hidden	INTEGER "hidden" INTEGER NOT NULL DEFAULT 0
typed	INTEGER "typed" INTEGER NOT NULL DEFAULT 0
frecency	INTEGER "frecency" INTEGER NOT NULL DEFAULT -1
last_visit_date	INTEGER "last_visit_date" INTEGER
guid	TEXT "guid" TEXT
foreign_count	INTEGER "foreign_count" INTEGER NOT NULL DEFAULT 0
url_hash	INTEGER "url_hash" INTEGER NOT NULL DEFAULT 0
description	TEXT "description" TEXT
preview_image_url	TEXT "preview_image_url" TEXT
site_name	TEXT "site_name" TEXT
origin_id	INTEGER "origin_id" INTEGER
moz_places_metadata	CREATE TABLE moz_places_metadata (id INTEGER PRIMARY KEY, url LONGVARCHAR, title LONGVARCHAR, rev_host LONGVARCHAR, visit_count INTEGER, hidden INTEGER, typed INTEGER, frecency INTEGER, last_visit_date INTEGER, guid TEXT, foreign_count INTEGER, url_hash INTEGER, description TEXT, preview_image_url TEXT, site_name TEXT, origin_id INTEGER)
moz_places_metadata_groups_to_snap...	CREATE TABLE moz_places_metadata_groups_to_snap (id INTEGER PRIMARY KEY, url LONGVARCHAR, title LONGVARCHAR, rev_host LONGVARCHAR, visit_count INTEGER, hidden INTEGER, typed INTEGER, frecency INTEGER, last_visit_date INTEGER, guid TEXT, foreign_count INTEGER, url_hash INTEGER, description TEXT, preview_image_url TEXT, site_name TEXT, origin_id INTEGER)
moz_places_metadata_search_queries	CREATE TABLE moz_places_metadata_search_queries (id INTEGER PRIMARY KEY, url LONGVARCHAR, title LONGVARCHAR, rev_host LONGVARCHAR, visit_count INTEGER, hidden INTEGER, typed INTEGER, frecency INTEGER, last_visit_date INTEGER, guid TEXT, foreign_count INTEGER, url_hash INTEGER, description TEXT, preview_image_url TEXT, site_name TEXT, origin_id INTEGER)

DB Browser for SQLite - C:\Users\Administrator\Downloads\files\files\Firefox\Firefox\Profiles\s6upyltd.default-release\places.sqlite

File Edit View Tools Help

New Database Open Database Write Changes Revert Changes Undo Open Project Save Project

Database Structure Browse Data Edit Pragma Execute SQL

moz\_anno\_attributes moz\_places moz\_places

Table: moz\_places

id	url	title
1	https://support.mozilla.org/products...	gro.all:
2	https://support.mozilla.org/kb/...	gro.all:
3	https://www.mozilla.org/contribute/	gro.all:
4	https://www.mozilla.org/about/	gro.all:
5	https://www.mozilla.org/privacy/...	gro.all:
6	https://www.mozilla.org/firefox/...	gro.all:
7	https://www.mozilla.org/en-US/...	Firefox Privacy Notice - Mozilla
8	https://www.amazon.com/exec/obidos/...	moc.noze
9	https://www.amazon.com/s/...	Amazon.com : BlackHat Go
10	https://www.amazon.com/s?...	Amazon.com : BlackHat Go
11	https://www.amazon.com/Black-Hat-Go-...	Amazon.com: Black Hat Go: Go ...
12	https://www.amazon.com/s/...	Amazon.com : BlackHat Python
13	https://www.amazon.com/s?...	Amazon.com : BlackHat Python
14	https://www.amazon.com/Black-Hat-...	Black Hat Python, 2nd Edition: Pytho...
15	https://www.amazon.com/s/...	Amazon.com : BlackHat GraphQL
16	https://www.amazon.com/s?...	Amazon.com : BlackHat GraphQL
17	https://www.amazon.com/Black-Hat-...	Amazon.com: Black Hat GraphQL: ...
18	https://www.reddit.com/	Reddit - Dive into anything
19	https://www.google.com/search?...	python download - Google Search
20	https://www.python.org/downloads/	Download Python   Python.org
21	https://www.python.org/ftp/python/...	python-3.11.1-amd64(1).exe
22	http://tryhackme.com/	moc.emke

From these records we see that the most visited website is amazon.com.

### Answer 2C:

In the same moz\_places table we see that the python 3.11 exe was the last downloaded file by suspect and that link was visited.

Table: moz_places			Filter in any column
	id	url	title
1	1	https://support.mozilla.org/products/firefox	Filter
2	2	https://support.mozilla.org/kb/customize-firefox-controls-buttons-and-toolbars?...	NULL
3	3	https://www.mozilla.org/contribute/	NULL
4	4	https://www.mozilla.org/about/	NULL
5	5	https://www.mozilla.org/privacy/firefox/	NULL
6	6	https://www.mozilla.org/firefox/central/	NULL
7	7	https://www.mozilla.org/en-US/privacy/firefox/	Firefox Privacy Notice - Mozilla
8	8	https://www.amazon.com/exec/obidos/external-search/?field=...	NULL
9	9	https://www.amazon.com/s/134-3609764-0992412?ie=UTF8&field=...	Amazon.com : BlackHat Go
10	10	https://www.amazon.com/s?k=BlackHat+Go&link_code=qs&sourceid=Mozilla-search&tag=mozilla-20	Amazon.com : BlackHat Go
11	11	https://www.amazon.com/Black-Hat-Go-Programming-Pentesters/dp/1593278659/ref=sr_1_1?...	Amazon.com: Black Hat Go: Go ...
12	12	https://www.amazon.com/s/ref=nb_sb_noss?url=search-alias%3Daps&field-keywords=BlackHat+Python	Amazon.com : BlackHat Python
13	13	https://www.amazon.com/s?k=BlackHat+Python&ref=nb_sb_noss	Amazon.com : BlackHat Python
14	14	https://www.amazon.com/Black-Hat-Python-2nd-Programming/dp/1718501129/ref=sr_1_1?...	Black Hat Python, 2nd Edition: Pytho
15	15	https://www.amazon.com/s/ref=nb_sb_noss_1?url=search-alias%3Daps&field=...	Amazon.com : BlackHat GraphQL
16	16	https://www.amazon.com/s?...	Amazon.com : BlackHat GraphQL
17	17	https://www.amazon.com/Black-Hat-GraphQL-Attacking-Generation/dp/1718502842/ref=sr_1_1?...	Amazon.com: Black Hat GraphQL: ...
18	23	https://www.reddit.com/	Reddit - Dive into anything
19	24	https://www.google.com/search?client=firefox-b-d&q=python+download	python download - Google Search
20	25	https://www.python.org/downloads/	Download Python   Python.org
21	26	https://www.python.org/ftp/python/3.11.1/python-3.11.1-amd64.exe	python-3.11.1-amd64(1).exe
22	27	http://tryhackme.com/	NULL
23	28	https://tryhackme.com/	TryHackMe   Cyber Security Training

### Answer 3A:

Analyzing the logs we see that the command executed is as follows:

Microsoft-Windows-PowerShell%4Operational

Number of events: 40

Act

Min

Level

Date and Time

Source

Event ID

Task Category

Verbose

1/29/2023 10:55:08 PM

PowerShell (Microsoft-Win...

4104

Execute a Remote Command

Verbose

1/29/2023 10:55:08 PM

PowerShell (Microsoft-Win...

4104

Execute a Remote Command

Verbose

1/29/2023 10:55:08 PM

PowerShell (Microsoft-Win...

4104

Execute a Remote Command

Verbose

1/29/2023 10:55:05 PM

PowerShell (Microsoft-Win...

4104

Execute a Remote Command

Verbose

1/29/2023 10:55:04 PM

PowerShell (Microsoft-Win...

4104

Execute a Remote Command

Verbose

1/29/2023 10:54:35 PM

PowerShell (Microsoft-Win...

4104

Execute a Remote Command

Verbose

1/29/2023 10:54:35 PM

PowerShell (Microsoft-Win...

4104

Execute a Remote Command

Verbose

1/29/2023 10:54:30 PM

PowerShell (Microsoft-Win...

4104

Execute a Remote Command

Event 4104, PowerShell (Microsoft-Windows-PowerShell)

General

Details

Creating Scriptblock text (1 of 1):

Invoke-WebRequest -UseBasicParsing -Uri https://raw.githubusercontent.com/vonderchild/digital-forensics-lab/main/Lab%202/files/file.ps1 -OutFile "file.ps1"

ScriptBlock ID: 1dfa7d0e-b89f-42cf-b8de-15a54a622de9

Path:

### Answer 3B:

Analyzing the logs, I see the data sent.

Level	Date and time	Source	Event ID	Task Category
Verbose	1/29/2023 10:55:08 PM	PowerShell (Microsoft-Win...	4104	Execute a Remote Command
Verbose	1/29/2023 10:55:08 PM	PowerShell (Microsoft-Win...	4104	Execute a Remote Command
Verbose	1/29/2023 10:55:08 PM	PowerShell (Microsoft-Win...	4104	Execute a Remote Command
Verbose	1/29/2023 10:55:05 PM	PowerShell (Microsoft-Win...	4104	Execute a Remote Command
Verbose	1/29/2023 10:55:04 PM	PowerShell (Microsoft-Win...	4104	Execute a Remote Command
Verbose	1/29/2023 10:54:35 PM	PowerShell (Microsoft-Win...	4104	Execute a Remote Command
Verbose	1/29/2023 10:54:35 PM	PowerShell (Microsoft-Win...	4104	Execute a Remote Command
Verbose	1/29/2023 10:54:30 PM	PowerShell (Microsoft-Win...	4104	Execute a Remote Command

Event 4104, PowerShell (Microsoft-Windows-PowerShell)	
General	Details
Creating Scriptblock text (1 of 1): \$data = "SGVsbG8slHVzZSBmbGFne2V2M250X2wwZ3NFZjByX3RoM193MW59IGFzHRoZSBhbnN3ZXlqdG8qdGhlIG9yaWdpbmFslHF1ZXN0aW9uLQ==" \$flag = [System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String(\$data)) Write-Output \$flag  ScriptBlock ID: edebd072-da14-4407-8d52-ea4b696a193c Path: C:\Users\w\file.ps1	

Decrypting it from base64:

Hello, use flag{ev3nt\_l0gs\_f0r\_th3\_w1n} as the answer to the original question.

### Answer 4:

Using the prefetch folder that is given I execute the following command to run the tool.

```
Administrator: Windows PowerShell
PS C:\Users\Administrator\Downloads\PECmd> .\PECmd.exe -d "C:\Users\Administrator\Downloads\files\files\Prefetch\Prefetch" --csv exports
```

This redirects the output to the csv format in the tools folder.

Giving the timeline file to chatgpt it gives top 3 suspicious files.

```
To locate a malicious program, I will:

1. Identify unique executable paths.
2. Highlight any that seem suspicious based on common indicators of malicious software.

Let's start by listing the unique executable paths. [-]
```

The list contains several executable paths, some of which stand out as potentially suspicious, especially those located in unusual directories such as `TEMP` or with unusual names like `DLLHOST.EXE` or `ALLO`. These could be indicators of malicious activity.

**Potentially Suspicious Entries:**

- `\USERS\WORK\APPDATA\LOCAL\TEMP\DLLHOST.EXE`
- `\WINDOWS\TEMP\385B95B7-2AE3-4D9B-AE48-E7652FF5481C\DISMHOST.EXE`
- `\WINDOWS\TEMP\{1EF7570F-AA82-441F-BDF8-8D56CF6BA8C9}\.CR\VCREDIST\_X86.EXE`

**Next steps:**

- Cross-check these executables against known malicious software databases.
- Investigate the runtime to see when these executables were run and if they align with any suspicious activities.

At row 59 we see the file which is misnamed and is run from a non standard path as it is the only one that stands out. DLLHOST instead of DLLHOST renaming error. Hence it is the malware.

52	#####	\VOLUME{01d95894c528b62b-44c53985}\WINDOWS\SYSTEM32\CONSENT.EXE				
53	#####	\VOLUME{01d95894c528b62b-44c53985}\WINDOWS\SYSTEM32\CONSENT.EXE				
54	#####	\VOLUME{01d95894c528b62b-44c53985}\WINDOWS\SYSTEM32\CONSENT.EXE				
55	#####	\VOLUME{01d95894c528b62b-44c53985}\WINDOWS\SYSTEM32\CSRSS.EXE				
56	#####	\VOLUME{01d95894c528b62b-44c53985}\WINDOWS\SYSTEM32\DASHOST.EXE				
57	#####	\VOLUME{01d95894c528b62b-44c53985}\WINDOWS\SYSTEM32\DEFRAG.EXE				
58	#####	\VOLUME{01d95894c528b62b-44c53985}\WINDOWS\TEMP\385B95B7-2AE3-4D9B-AE48-E7652FF5481C\DISMHOST.EXE				
59	#####	\VOLUME{01d95894c528b62b-44c53985}\USERS\WORK\APPDATA\LOCAL\TEMP\DLLHOST.EXE				
60	#####	\VOLUME{01d95894c528b62b-44c53985}\WINDOWS\SYSTEM32\DLLHOST.EXE				
61	#####	\VOLUME{01d95894c528b62b-44c53985}\WINDOWS\SYSTEM32\DLLHOST.EXE				
62	#####	\VOLUME{01d95894c528b62b-44c53985}\WINDOWS\SYSTEM32\DLLHOST.EXE				
63	#####	\VOLUME{01d95894c528b62b-44c53985}\WINDOWS\SYSTEM32\DLLHOST.EXE				
64	#####	\VOLUME{01d95894c528b62b-44c53985}\WINDOWS\SYSTEM32\DLLHOST.EXE				
65	#####	\VOLUME{01d95894c528b62b-44c53985}\WINDOWS\SYSTEM32\DLLHOST.EXE				
66	#####	\VOLUME{01d95894c528b62b-44c53985}\WINDOWS\SYSTEM32\DLLHOST.EXE				