ANALISI DINAMICA BASICA

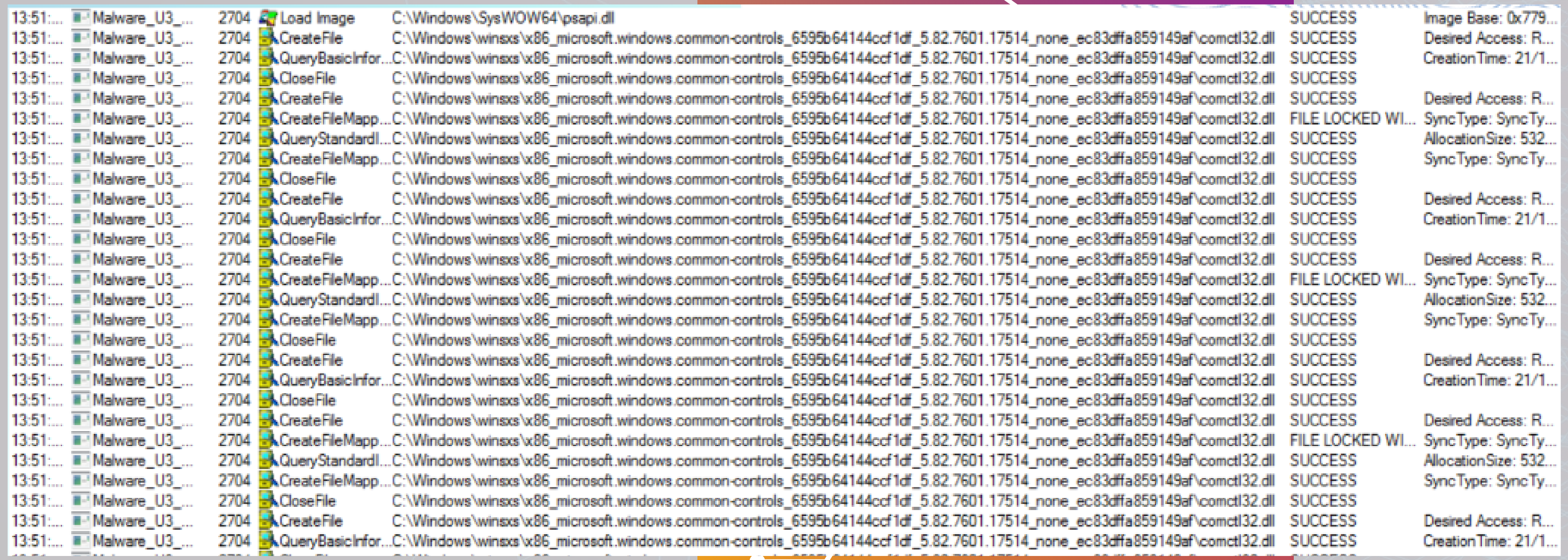
MATTIA
PASTORELLI

COMANDA:

Configurare la macchina virtuale per l’analisi dinamica (il malwaresarà effettivamente eseguito). Con riferimento al file eseguibile contenuto nella cartella «Esercizio_Pratico_U3_W2_L2» presente sul desktop della vostra macchina virtuale dedicata all’analisi dei malware, rispondere ai seguenti quesiti:

- Identificare eventuali azioni del malwaresul file systemutilizzando ProcessMonitor (procmon)
- Identificare eventuali azioni del malwaresu processi e threadutilizzando ProcessMonitor
- Modifiche del registro dopo il malware(le differenze)
- Provare a profilare il malwarein base alla correlazione tra «operation» e Path.

PROCMON

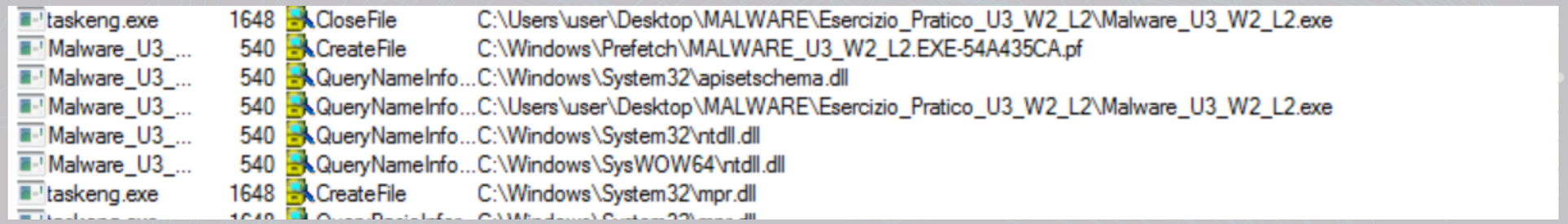


13:51:...	Malware_U3_...	2704	Load Image	C:\Windows\SysWOW64\psapi.dll	SUCCESS	Image Base: 0x779...
13:51:...	Malware_U3_...	2704	CreateFile	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll	SUCCESS	Desired Access: R...
13:51:...	Malware_U3_...	2704	QueryBasicInfor...	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll	SUCCESS	CreationTime: 21/1...
13:51:...	Malware_U3_...	2704	CloseFile	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll	SUCCESS	
13:51:...	Malware_U3_...	2704	CreateFile	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll	SUCCESS	Desired Access: R...
13:51:...	Malware_U3_...	2704	CreateFileMapp...	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll	FILE LOCKED WI...	SyncType: SyncTy...
13:51:...	Malware_U3_...	2704	QueryStandardI...	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll	SUCCESS	AllocationSize: 532...
13:51:...	Malware_U3_...	2704	CreateFileMapp...	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll	SUCCESS	SyncType: SyncTy...
13:51:...	Malware_U3_...	2704	CloseFile	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll	SUCCESS	
13:51:...	Malware_U3_...	2704	CreateFile	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll	SUCCESS	Desired Access: R...
13:51:...	Malware_U3_...	2704	QueryBasicInfor...	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll	SUCCESS	CreationTime: 21/1...
13:51:...	Malware_U3_...	2704	CloseFile	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll	SUCCESS	
13:51:...	Malware_U3_...	2704	CreateFile	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll	SUCCESS	Desired Access: R...
13:51:...	Malware_U3_...	2704	CreateFileMapp...	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll	FILE LOCKED WI...	SyncType: SyncTy...
13:51:...	Malware_U3_...	2704	QueryStandardI...	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll	SUCCESS	AllocationSize: 532...
13:51:...	Malware_U3_...	2704	CreateFileMapp...	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll	SUCCESS	SyncType: SyncTy...
13:51:...	Malware_U3_...	2704	CloseFile	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll	SUCCESS	
13:51:...	Malware_U3_...	2704	CreateFile	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll	SUCCESS	Desired Access: R...
13:51:...	Malware_U3_...	2704	QueryBasicInfor...	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll	SUCCESS	CreationTime: 21/1...
13:51:...	Malware_U3_...	2704	CloseFile	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll	SUCCESS	
13:51:...	Malware_U3_...	2704	CreateFile	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll	SUCCESS	Desired Access: R...
13:51:...	Malware_U3_...	2704	CreateFileMapp...	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll	FILE LOCKED WI...	SyncType: SyncTy...
13:51:...	Malware_U3_...	2704	QueryStandardI...	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll	SUCCESS	AllocationSize: 532...
13:51:...	Malware_U3_...	2704	CreateFileMapp...	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll	SUCCESS	SyncType: SyncTy...
13:51:...	Malware_U3_...	2704	CloseFile	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll	SUCCESS	
13:51:...	Malware_U3_...	2704	CreateFile	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll	SUCCESS	Desired Access: R...
13:51:...	Malware_U3_...	2704	QueryBasicInfor...	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll	SUCCESS	CreationTime: 21/1...

Si tratta di uno strumento di monitoraggio e analisi del sistema creato da Microsoft per il sistema operativo Windows. Procmon consente agli utenti di monitorare in tempo reale le attività del sistema, come processi, file di registro, attività di rete, registri di sistema e altro ancora. Quando si apre il programma, comparirà questa schermata.

Come funziona?

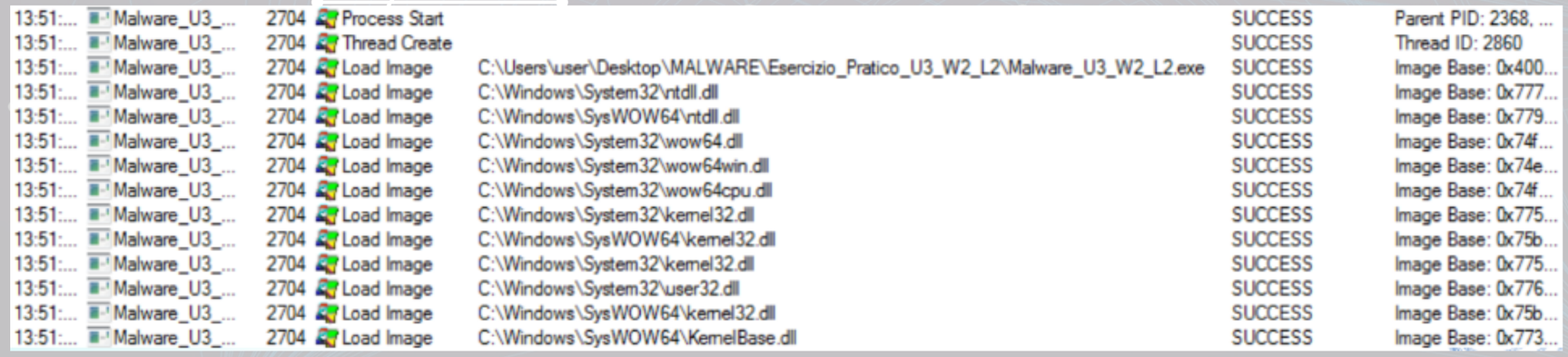
Una volta attivato, il malware inizia a generare file e varie richieste di librerie note (ad esempio, apisetschema.dll / ntdll.dll). Ciò suggerisce che il malware sta cercando di assumere il controllo delle librerie per poter operare senza essere interrotto. Attiva il servizio consent.exe per scalare i privilegi e acquisire i diritti di amministratore, consentendogli di agire sull'intero sistema.



taskeng.exe	1648	CloseFile	C:\Users\user\Desktop\MALWARE\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe
Malware_U3_...	540	CreateFile	C:\Windows\Prefetch\MALWARE_U3_W2_L2.EXE-54A435CA.pf
Malware_U3_...	540	QueryNameInfo...	C:\Windows\System32\apisetschema.dll
Malware_U3_...	540	QueryNameInfo...	C:\Users\user\Desktop\MALWARE\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe
Malware_U3_...	540	QueryNameInfo...	C:\Windows\System32\ntdll.dll
Malware_U3_...	540	QueryNameInfo...	C:\Windows\SysWOW64\ntdll.dll
taskeng.exe	1648	CreateFile	C:\Windows\System32\mpr.dll

Thread

Relativamente ai thread, si può osservare che il malware ha generato un nuovo thread con la capacità di caricare immagini da varie librerie (tra cui Kernel.dll e user32.dll). Utilizzando il thread, è in grado di eseguire diverse azioni contemporaneamente e in modo più veloce, il che porta a un insieme di azioni ravvicinate.



13:51:...	Malware_U3_...	2704	Process Start		SUCCESS	Parent PID: 2368, ...
13:51:...	Malware_U3_...	2704	Thread Create		SUCCESS	Thread ID: 2860
13:51:...	Malware_U3_...	2704	Load Image	C:\Users\user\Desktop\MALWARE\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	Image Base: 0x400...
13:51:...	Malware_U3_...	2704	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x777...
13:51:...	Malware_U3_...	2704	Load Image	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Image Base: 0x779...
13:51:...	Malware_U3_...	2704	Load Image	C:\Windows\System32\wow64.dll	SUCCESS	Image Base: 0x74f...
13:51:...	Malware_U3_...	2704	Load Image	C:\Windows\System32\wow64win.dll	SUCCESS	Image Base: 0x74e...
13:51:...	Malware_U3_...	2704	Load Image	C:\Windows\System32\wow64cpu.dll	SUCCESS	Image Base: 0x74f...
13:51:...	Malware_U3_...	2704	Load Image	C:\Windows\System32\kernel32.dll	SUCCESS	Image Base: 0x775...
13:51:...	Malware_U3_...	2704	Load Image	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Image Base: 0x75b...
13:51:...	Malware_U3_...	2704	Load Image	C:\Windows\System32\kernel32.dll	SUCCESS	Image Base: 0x775...
13:51:...	Malware_U3_...	2704	Load Image	C:\Windows\System32\user32.dll	SUCCESS	Image Base: 0x776...
13:51:...	Malware_U3_...	2704	Load Image	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Image Base: 0x75b...
13:51:...	Malware_U3_...	2704	Load Image	C:\Windows\SysWOW64\KernelBase.dll	SUCCESS	Image Base: 0x773...

Modifiche del registro post malware.

Nel momento in cui si crea un'istanza prima e dopo l'avvio del malware, sono state aggiunte nuove chiavi alla directory shell/bags. Questa directory è utilizzata da Windows per memorizzare le preferenze dell'utente e personalizzare l'esperienza di navigazione delle cartelle nell'Esplora file. Questo potrebbe indicare un tentativo di visualizzare le cartelle in modo che il malware possa infettarle tutte contemporaneamente, anziché doverle infettare singolarmente.
Inoltre, il malware ha inserito una chiave nella directory "AllFolders/ComDlg" che consente di salvare, stampare file e svolgere altre azioni simili.

```
----------------------------------
Keys added: 14
----------------------------------
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{50F8E37B-FEDF-4D76-947D-8C85793181A7}
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Mozilla\Firefox\Default Browser Agent\PingCache
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Mozilla\Firefox\Default Browser Agent\PingCache\version2
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\48\ComDlg
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\89\Shell\{5C4F28B5-F869-4E84-8E60-F1
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\ComDlg
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\ComDlg\{FBB3477E-C9E4-4B3
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\ComDlg\{FBB3477E-C9E4-4B3
HKU\S-1-5-21-3771313050-58705377-3452663501-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\48\ComDlg
HKU\S-1-5-21-3771313050-58705377-3452663501-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\89\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC
HKU\S-1-5-21-3771313050-58705377-3452663501-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\ComDlg
HKU\S-1-5-21-3771313050-58705377-3452663501-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\ComDlg\{FBB3477E-C9E4-4B3B-A2BA-D3
HKU\S-1-5-21-3771313050-58705377-3452663501-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\ComDlg\{FBB3477E-C9E4-4B3B-A2BA-D3

----------------------------------
Values added: 54
----------------------------------
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\CIDSizeMRU\3:  52 00 65 00 67 00 73 00 68 00 6
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{50F8E37B-FEDF-4D76-947D-8C85793181A7}\Wp
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{50F8E37B-FEDF-4D76-947D-8C85793181A7}\Wp
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{50F8E37B-FEDF-4D76-947D-8C85793181A7}\Wp
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{50F8E37B-FEDF-4D76-947D-8C85793181A7}\Wp
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Mozilla\Firefox\Default Browser Agent\CurrentDefault: "firefox"
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Mozilla\Firefox\Default Browser Agent\LastPingSentAt:  9D 2B 00 B2 8E 5E DA 01
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Mozilla\Firefox\Default Browser Agent\PingCurrentDefault: "firefox"
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Mozilla\Firefox\Default Browser Agent\PingCache\version2\Capacity: 0x00000002
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Mozilla\Firefox\Default Browser Agent\PingCache\version2\Front: 0x00000000
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Mozilla\Firefox\Default Browser Agent\PingCache\version2\Size: 0x00000000
```