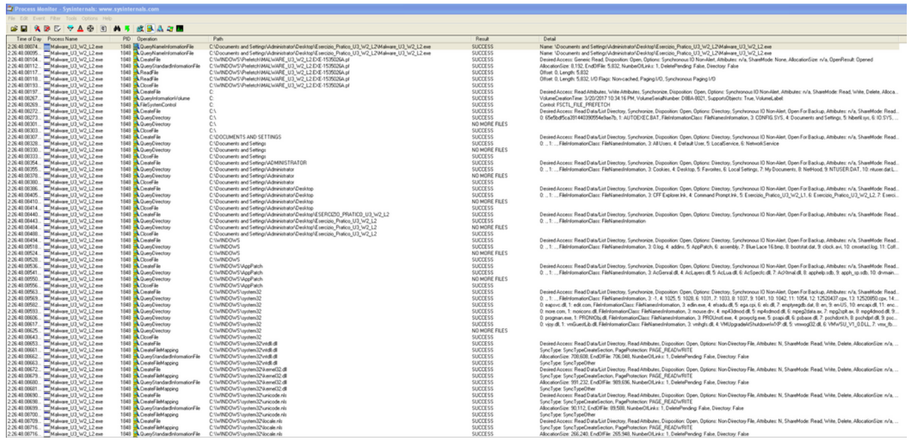
S10 L2

Analisi Dinamica Basica

Daniele Zizzi

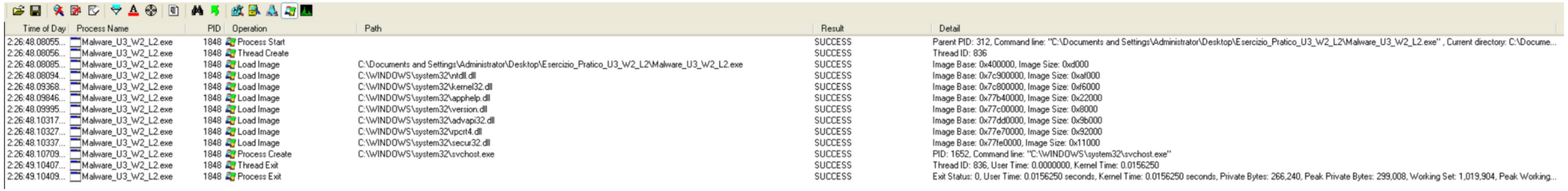
In questo esercizio, andremo a fare un’analisi di tipo dinamica basica eseguendo un file .exe infetto. Grazie all’utilizzo di process monitor e regshot, possiamo visualizzare i comandi eseguiti dal malware.

Modifiche effettuate al filesystem, tra cui creazione di file, lettura, chiusura e ricerca di cartelle. Possiamo notare come il malware vada a creare un file .log dove scrive le varie azioni dell’utente.



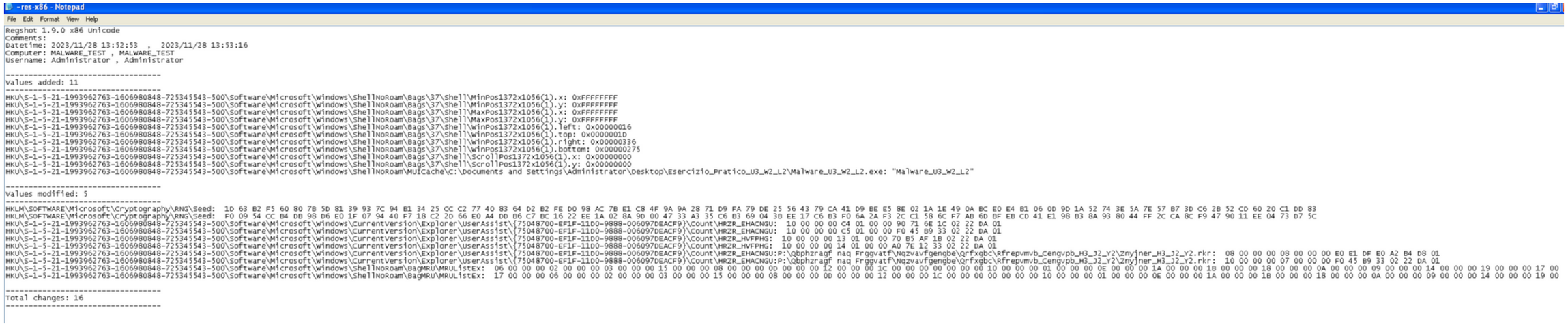
2:08:02.57467...	Malware_U3_W2_L2.exe	416	CloseFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	SUCCESS		
2:10:52.69325...	svchost.exe	1020	CreateFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log	SUCCESS	Desired Access: Generic Write, Read Attributes, Disposition: OpenIf, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: N, ShareMode: Write, AllocationSize: 0, ...
2:10:52.69330...	svchost.exe	1020	QueryStandardInformationFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log	SUCCESS	AllocationSize: 472, EndOfFile: 471, NumberOfLinks: 1, DeletePending: False, Directory: False
2:10:52.69335...	svchost.exe	1020	WriteFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log	SUCCESS	Offset: 471, Length: 12
2:10:52.69340...	svchost.exe	1020	ReadFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log	SUCCESS	Offset: 0, Length: 483, I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O
2:10:52.69347...	svchost.exe	1020	WriteFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log	SUCCESS	Offset: 483, Length: 22
2:10:52.69360...	svchost.exe	1020	WriteFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log	SUCCESS	Offset: 505, Length: 4
2:10:52.69367...	svchost.exe	1020	WriteFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log	SUCCESS	Offset: 509, Length: 1
2:10:52.69371...	svchost.exe	1020	CloseFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log	SUCCESS	
2:10:53.15847...	svchost.exe	1020	CreateFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log	SUCCESS	Desired Access: Generic Write, Read Attributes, Disposition: OpenIf, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: N, ShareMode: Write, AllocationSize: 0, ...
2:10:53.15851...	svchost.exe	1020	QueryStandardInformationFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log	SUCCESS	AllocationSize: 512, EndOfFile: 510, NumberOfLinks: 1, DeletePending: False, Directory: False
2:10:53.15854...	svchost.exe	1020	WriteFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log	SUCCESS	Offset: 510, Length: 1
2:10:53.15861...	svchost.exe	1020	CloseFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log	SUCCESS	
2:10:53.37431...	svchost.exe	1020	CreateFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log	SUCCESS	Desired Access: Generic Write, Read Attributes, Disposition: OpenIf, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: N, ShareMode: Write, AllocationSize: 0, ...
2:10:53.37434...	svchost.exe	1020	QueryStandardInformationFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log	SUCCESS	AllocationSize: 512, EndOfFile: 511, NumberOfLinks: 1, DeletePending: False, Directory: False
2:10:53.37437...	svchost.exe	1020	WriteFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log	SUCCESS	Offset: 511, Length: 1
2:10:53.37444...	svchost.exe	1020	CloseFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log	SUCCESS	
2:10:57.53099...	svchost.exe	1020	CreateFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log	SUCCESS	Desired Access: Generic Write, Read Attributes, Disposition: OpenIf, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: N, ShareMode: Write, AllocationSize: 0, ...
2:10:57.53102...	svchost.exe	1020	QueryStandardInformationFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log	SUCCESS	AllocationSize: 512, EndOfFile: 512, NumberOfLinks: 1, DeletePending: False, Directory: False
2:10:57.53106...	svchost.exe	1020	WriteFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log	SUCCESS	Offset: 512, Length: 1
2:10:57.53115...	svchost.exe	1020	CloseFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log	SUCCESS	
2:10:57.81994...	svchost.exe	1020	CreateFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log	SUCCESS	Desired Access: Generic Write, Read Attributes, Disposition: OpenIf, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: N, ShareMode: Write, AllocationSize: 0, ...
2:10:57.81997...	svchost.exe	1020	QueryStandardInformationFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log	SUCCESS	AllocationSize: 520, EndOfFile: 513, NumberOfLinks: 1, DeletePending: False, Directory: False
2:10:57.82000...	svchost.exe	1020	WriteFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log	SUCCESS	Offset: 513, Length: 1
2:10:57.82009...	svchost.exe	1020	CloseFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log	SUCCESS	
2:10:57.95993...	svchost.exe	1020	CreateFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log	SUCCESS	Desired Access: Generic Write, Read Attributes, Disposition: OpenIf, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: N, ShareMode: Write, AllocationSize: 0, ...
2:10:57.95996...	svchost.exe	1020	QueryStandardInformationFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log	SUCCESS	AllocationSize: 520, EndOfFile: 514, NumberOfLinks: 1, DeletePending: False, Directory: False
2:10:57.95999...	svchost.exe	1020	WriteFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log	SUCCESS	Offset: 514, Length: 1
2:10:57.96006...	svchost.exe	1020	CloseFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log	SUCCESS	
2:10:58.06463...	svchost.exe	1020	CreateFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log	SUCCESS	Desired Access: Generic Write, Read Attributes, Disposition: OpenIf, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: N, ShareMode: Write, AllocationSize: 0, ...
2:10:58.06466...	svchost.exe	1020	QueryStandardInformationFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log	SUCCESS	AllocationSize: 520, EndOfFile: 515, NumberOfLinks: 1, DeletePending: False, Directory: False
2:10:58.06470...	svchost.exe	1020	WriteFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log	SUCCESS	Offset: 515, Length: 1
2:10:58.06476...	svchost.exe	1020	CloseFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log	SUCCESS	

Azioni del malware su processi e thread.
All’avvio del malware, viene creato un thread. Viene caricato il malware in memoria e poi vengono effettuate le varie chiamate alle librerie di sistema. Crea un processo in svchost.exe con pid 1652, in modo da non poter essere più rimosso. In seguito chiude il thread creato in precenza in modo che non sia visibile sul task manager di windows e l’utente non posso accorgersi del keylogger.



Time of Day	Process Name	PID	Operation	Path	Result	Detail
2:26:48.08055...	Malware_U3_W2_L2.exe	1848	Process Start		SUCCESS	Parent PID: 312, Command line: "C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe" , Current directory: C:\Docume...
2:26:48.08056...	Malware_U3_W2_L2.exe	1848	Thread Create		SUCCESS	Thread ID: 836
2:26:48.08085...	Malware_U3_W2_L2.exe	1848	Load Image	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	Image Base: 0x400000, Image Size: 0xd000
2:26:48.08094...	Malware_U3_W2_L2.exe	1848	Load Image	C:\WINDOWS\system32\ntdll.dll	SUCCESS	Image Base: 0x7c900000, Image Size: 0xaf000
2:26:48.09368...	Malware_U3_W2_L2.exe	1848	Load Image	C:\WINDOWS\system32\kernel32.dll	SUCCESS	Image Base: 0x7c800000, Image Size: 0xf6000
2:26:48.09846...	Malware_U3_W2_L2.exe	1848	Load Image	C:\WINDOWS\system32\apphelp.dll	SUCCESS	Image Base: 0x77b40000, Image Size: 0x22000
2:26:48.09995...	Malware_U3_W2_L2.exe	1848	Load Image	C:\WINDOWS\system32\version.dll	SUCCESS	Image Base: 0x77c00000, Image Size: 0x8000
2:26:48.10317...	Malware_U3_W2_L2.exe	1848	Load Image	C:\WINDOWS\system32\advapi32.dll	SUCCESS	Image Base: 0x77dd0000, Image Size: 0x9b000
2:26:48.10327...	Malware_U3_W2_L2.exe	1848	Load Image	C:\WINDOWS\system32\rpcrt4.dll	SUCCESS	Image Base: 0x77e70000, Image Size: 0x92000
2:26:48.10337...	Malware_U3_W2_L2.exe	1848	Load Image	C:\WINDOWS\system32\secur32.dll	SUCCESS	Image Base: 0x77fe0000, Image Size: 0x11000
2:26:48.10709...	Malware_U3_W2_L2.exe	1848	Process Create	C:\WINDOWS\system32\svchost.exe	SUCCESS	PID: 1652, Command line: "C:\WINDOWS\system32\svchost.exe"
2:26:49.10407...	Malware_U3_W2_L2.exe	1848	Thread Exit		SUCCESS	Thread ID: 836, User Time: 0.0000000, Kernel Time: 0.0156250
2:26:49.10409...	Malware_U3_W2_L2.exe	1848	Process Exit		SUCCESS	Exit Status: 0, User Time: 0.0156250 seconds, Kernel Time: 0.0156250 seconds, Private Bytes: 266,240, Peak Private Bytes: 299,008, Working Set: 1,019,904, Peak Working...

Modifiche effettuate sul registro, utilizzando il tool regshot, dopo aver avviato il malware. Vengono create e modificate varie chiavi di registro.



```
- res-x86 - Notepad
File  Edit  Format  View  Help
Regshot 1.9.0 x86 Unicode
Comments:
Datetime: 2023/11/28 13:52:53  ,  2023/11/28 13:53:16
Computer: MALWARE_TEST , MALWARE_TEST
Username: Administrator , Administrator

----------------------------------
Values added: 11
----------------------------------
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\Bags\37\Shell\MinPos1372x1056(1).x: 0xFFFFFFFF
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\Bags\37\Shell\MinPos1372x1056(1).y: 0xFFFFFFFF
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\Bags\37\Shell\MaxPos1372x1056(1).x: 0xFFFFFFFF
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\Bags\37\Shell\MaxPos1372x1056(1).y: 0xFFFFFFFF
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\Bags\37\Shell\WinPos1372x1056(1).left: 0x00000016
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\Bags\37\Shell\WinPos1372x1056(1).top: 0x0000001D
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\Bags\37\Shell\WinPos1372x1056(1).right: 0x00000336
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\Bags\37\Shell\WinPos1372x1056(1).bottom: 0x00000275
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\Bags\37\Shell\ScrollPos1372x1056(1).x: 0x00000000
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\Bags\37\Shell\ScrollPos1372x1056(1).y: 0x00000000
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\MUICache\C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe: "Malware_U3_W2_L2"

----------------------------------
Values modified: 5
----------------------------------
HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed:  1D 63 B2 F5 60 80 7B 5D 81 39 93 7C 94 B1 34 25 CC C2 77 40 83 64 D2 B2 FE D0 98 AC 7B E1 C8 4F 9A 9A 28 71 D9 FA 79 DE 25 56 43 79 CA 41 D9 BE E5 8E 02 1A 1E 49 0A BC E0 E4 B1 06 0D 9D 1A 52 74 3E 5A 7E 57 B7 3D C6 2B 52 CD 60 20 C1 DD 83
HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed:  F0 09 54 CC B4 DB 98 D6 E0 1F 07 94 40 F7 18 C2 2D 66 E0 A4 DD B6 C7 BC 16 22 EE 1A 02 8A 9D 00 47 33 A3 35 C6 B3 69 04 3B EE 17 C6 B3 F0 6A 2A F3 2C C1 58 6C F7 AB 6D BF EB CD 41 E1 98 B3 8A 93 80 44 FF 2C CA BC F9 47 90 11 EE 04 73 D7 5C
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZR_EHACNGU:  10 00 00 00 C4 01 00 00 90 71 6E 1C 02 22 DA 01
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZR_EHACNGU:  10 00 00 00 C5 01 00 00 F0 45 B9 33 02 22 DA 01
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZR_HVFPHG:  10 00 00 00 13 01 00 00 70 B5 AF 1B 02 22 DA 01
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZR_HVFPHG:  10 00 00 00 14 01 00 00 A0 7E 12 33 02 22 DA 01
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZR_EHACNGU:P:\Qbphzragf naq Frggvatf\Nqzvavfgengbe\Qrfxgbc\Rfrepvmvb_Cengvpb_H3_J2_Y2\Znyjner_H3_J2_Y2.rkr:  08 00 00 00 08 00 00 00 E0 E1 DF E0 A2 B4 D8 01
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZR_EHACNGU:P:\Qbphzragf naq Frggvatf\Nqzvavfgengbe\Qrfxgbc\Rfrepvmvb_Cengvpb_H3_J2_Y2\Znyjner_H3_J2_Y2.rkr:  10 00 00 00 07 00 00 00 F0 45 B9 33 02 22 DA 01
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\BagMRU\MRUListEx:  06 00 00 00 02 00 00 00 03 00 00 00 15 00 00 00 08 00 00 00 0D 00 00 00 12 00 00 00 1C 00 00 00 00 00 00 00 10 00 00 00 01 00 00 00 0E 00 00 00 1A 00 00 00 1B 00 00 00 18 00 00 00 0A 00 00 00 09 00 00 00 14 00 00 00 19 00 00 00 17 00
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\BagMRU\MRUListEx:  17 00 00 00 06 00 00 00 02 00 00 00 03 00 00 00 15 00 00 00 08 00 00 00 0D 00 00 00 12 00 00 00 1C 00 00 00 00 00 00 00 10 00 00 00 01 00 00 00 0E 00 00 00 1A 00 00 00 1B 00 00 00 18 00 00 00 0A 00 00 00 09 00 00 00 14 00 00 00 19 00

----------------------------------
Total changes: 16
----------------------------------
```

Il malware in questione è un keylogger. Cattura i programmi aperti sull'host e l'input da tastiera. Molto pericoloso, poichè può catturare username e password in chiaro.