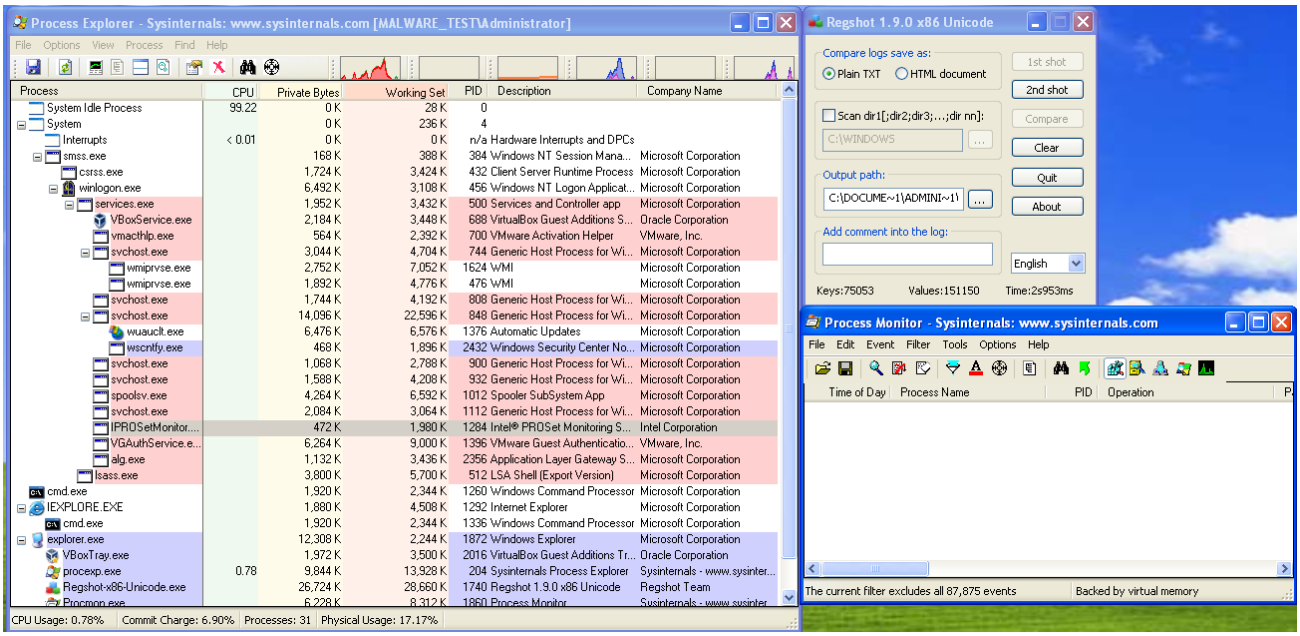
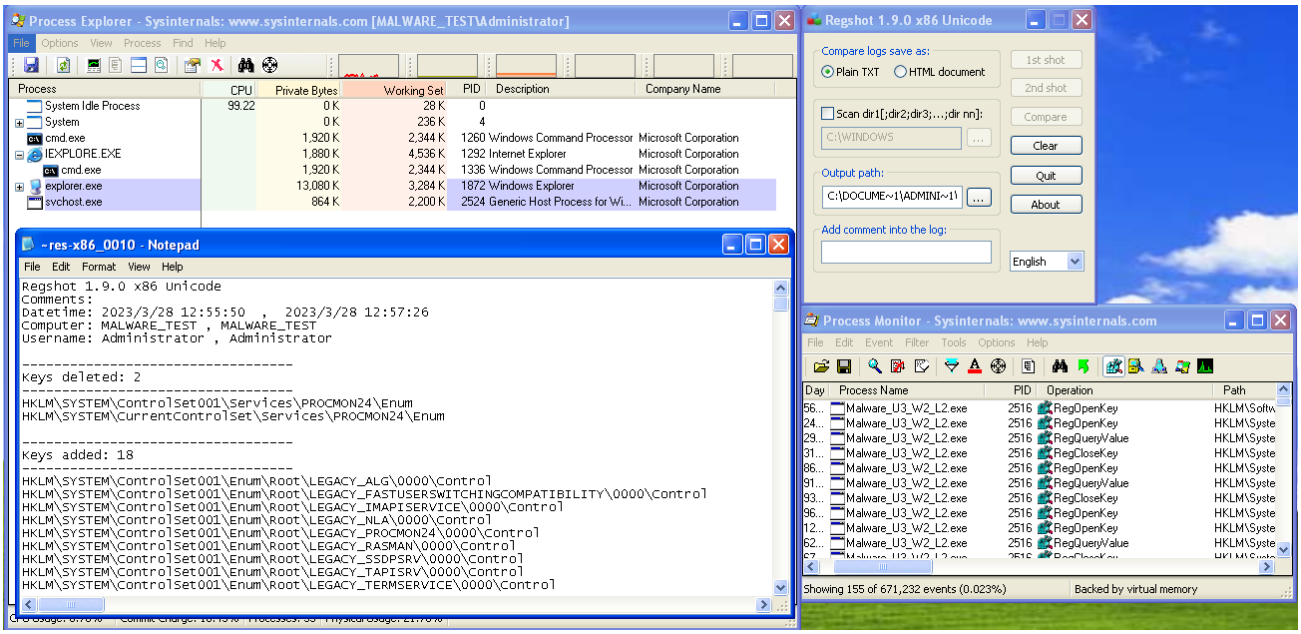
Analisi dinamica malware

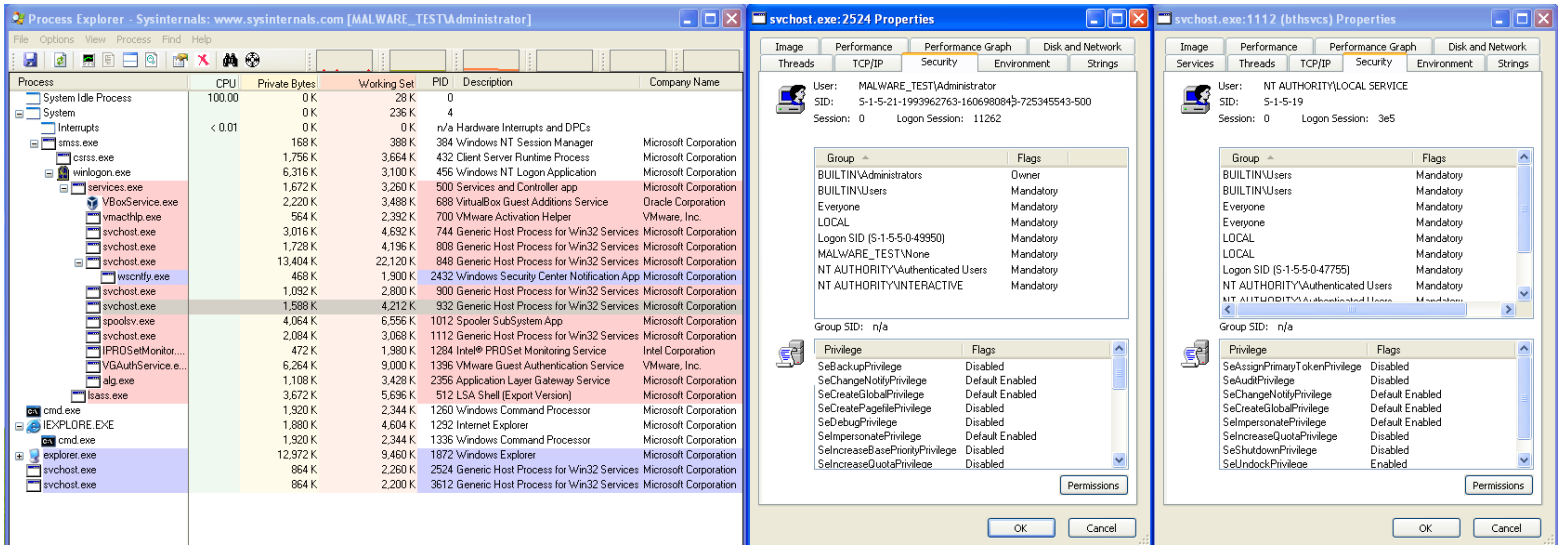
03-28-2023



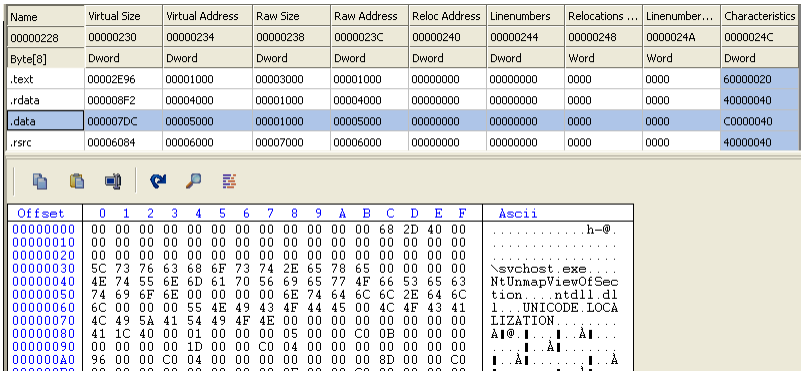
Nell' immagine sopra abbiamo una visione d'insieme di come si presenta il sistema operativo in condizioni normali, sotto invece vediamo come una volta avviato il malware le chiavi di registro dell'utente corrente e quelle della macchina locale sono state modificate, aggiunte e cancellate sotto le istruzioni dell'eseguibile malevolo.
Notiamo inoltre la presenza di un processo aggiuntivo che apparentemente sembra un normale processo di sistema che ne assicura il corretto funzionamento, quindi da non abbattere per non minare la stabilità di windows.
Oltre a questo possiamo vedere su Process Monitor 155 nuovi processi che sono andati a richiedere informazioni sulle chiavi di registro nominate prima.



Analizziamo quindi il nuovo processo comparandolo con uno identico che sappiamo essere lecito, notiamo appunto delle discrepanze sia nel gruppo che nei permessi, da non tralasciare inoltre l'utente che ha avviato i processi.



L'ennesima conferma che il processo nuovo si tratta di un falso viene dall'analisi statica dell'eseguibile che nelle sue variabili globali contiene proprio il nome del processo sotto cui si nasconderà una volta eseguito il malware.



Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations ...	Linenumber...	Characteristics
00000228	00000230	00000234	00000238	0000023C	00000240	00000244	00000248	0000024A	0000024C
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
.text	00002E96	00001000	00003000	00001000	00000000	00000000	0000	0000	60000020
.rdata	000008F2	00004000	00001000	00004000	00000000	00000000	0000	0000	40000040
.data	000007DC	00005000	00001000	00005000	00000000	00000000	0000	0000	C0000040
.rsrc	00006084	00006000	00007000	00006000	00000000	00000000	0000	0000	40000040

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii
00000000	00	00	00	00	00	00	00	00	00	00	00	00	68	2D	40	00	.....h-@.
00000010	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000030	5C	73	76	63	68	6F	73	74	2E	65	78	65	00	00	00	00	\svchost.exe....
00000040	4E	74	55	6E	6D	61	70	56	69	65	77	4F	66	53	65	63	NtUnmapViewOfSec
00000050	74	69	6F	6E	00	00	00	00	6E	74	64	6C	6C	2E	64	6C	tion....ntdll.dl
00000060	6C	00	00	00	55	4E	49	43	4F	44	45	00	4C	4F	43	41	l...UNICODE.LOCA
00000070	4C	49	5A	41	54	49	4F	4E	00	00	00	00	00	00	00	00	LIZATION.....
00000080	41	1C	40	00	01	00	00	00	05	00	00	C0	0B	00	00	00	A.@.....À....
00000090	00	00	00	00	1D	00	00	C0	04	00	00	00	00	00	00	00	.....À.....
000000A0	96	00	00	C0	04	00	00	00	00	00	00	8D	00	00	00	C0	...À.....À

Analizzando le funzioni chiamate dall'applicazione e comparandole con il risultato di Process Monitor il funzionamento del malware sembrerebbe essere la modifica di key del sistema al fine di aprire una connessione HTTP con il malintenzionato probabilmente dandogli accesso ad una shell sulla nostra macchina, oltre a questo anche le chiavi di criptazione sono state compromesse esponendo il sistema a rischi esterni, anche il servizio TermService è stato attivato e configurato dal malware il che potrebbe dargli un accesso remoto direttamente al Desktop.

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
000046B8	N/A	00004444	00004448	0000444C	00004450	00004454
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.dll	54	0000446C	00000000	00000000	000046B8	00004000

OFTs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
00004548	00004548	001B	CloseHandle
00004556	00004556	02BF	VirtualFree
00004564	00004564	0218	ReadFile
00004570	00004570	02BB	VirtualAlloc
00004580	00004580	0112	GetFileSize
0000458E	0000458E	0034	CreateFileA
0000459C	0000459C	022C	ResumeThread
000045AC	000045AC	0283	SetThreadContext
000045C0	000045C0	02E9	WriteProcessMemory
000045D6	000045D6	02BC	VirtualAllocEx
000045E8	000045E8	013E	GetProcAddress
000045FA	000045FA	0126	GetModuleHandleA
0000460E	0000460E	021C	ReadProcessMemory
00004622	00004622	0167	GetThreadContext
00004636	00004636	0044	CreateProcessA
00004648	00004648	00B6	FreeResource
00004658	00004658	0295	SizeofResource
0000466A	0000466A	01D5	LockResource
0000467A	0000467A	01C7	LoadResource
0000468A	0000468A	00A3	FindResourceA
0000469A	0000469A	0159	GetSystemDirectoryA
000046B0	000046B0	0296	Sleep
000046C6	000046C6	00CA	GetCommandLineA
000046D8	000046D8	0174	GetVersion
000046E6	000046E6	007D	ExitProcess
000046F4	000046F4	029E	TerminateProcess
00004708	00004708	00F7	GetCurrentProcess
0000471C	0000471C	02AD	UnhandledExceptionFilter
00004738	00004738	0124	GetModuleFileNameA
0000474E	0000474E	00B2	FreeEnvironmentStringsA
00004768	00004768	00B3	FreeEnvironmentStringsW

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations ...	Linenumber...	Characteristics
00000200	00000208	0000020C	00000210	00000214	00000218	0000021C	00000220	00000222	00000224
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
.rdata	000008F2	00004000	00001000	00004000	00000000	00000000	0000	0000	40000040
.data	000007DC	00005000	00001000	00005000	00000000	00000000	0000	0000	C0000040
.rsrc	00006084	00006000	00007000	00006000	00000000	00000000	0000	0000	40000040

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii
00000560	72	65	65	00	18	02	52	65	61	64	46	69	6C	65	00	00	ree..RReadFile..
00000570	BB	02	56	69	72	74	75	61	6C	41	6C	6F	63	00	00	00	»VirtualAlloc...
00000580	12	01	47	65	74	46	69	6C	65	53	69	7A	65	00	34	00	GetFileSize.4.
00000590	43	72	65	61	74	65	46	69	6C	65	41	00	2C	02	52	65	CreateFileA.,Re
000005A0	73	75	6D	65	54	68	72	65	61	64	00	00	83	02	53	65	sumeThread...Se
000005B0	74	54	68	72	65	61	64	43	6F	6E	74	65	78	74	00	00	tThreadContext..
000005C0	E9	02	57	72	69	74	65	50	72	6F	63	65	73	73	4D	65	éWriteProcessMe
000005D0	6D	6F	72	79	00	00	BC	02	56	69	72	74	75	61	6C	41	mory..¼Virtualà
000005E0	6C	6C	6F	63	45	78	00	00	3E	01	47	65	74	50	72	6F	llocEx..>GetPro
000005F0	63	41	64	64	72	65	73	73	00	00	26	01	47	65	74	4D	cAddress..&GetM
00000600	6F	64	75	6C	65	48	61	6E	64	6C	65	41	00	00	1C	02	oduleHandleA....
00000610	52	65	61	64	50	72	6F	63	65	73	73	4D	65	6D	6F	72	ReadProcessMemor
00000620	79	00	67	01	47	65	74	54	68	72	65	61	64	43	6F	6E	y.gGetThreadCon
00000630	74	65	78	74	00	00	44	00	43	72	65	61	74	65	50	72	text..D.CreatePr
00000640	6F	63	65	73	73	41	00	00	B6	00	46	72	65	65	52	65	ocessA..¶.FreeRe
00000650	73	6F	75	72	63	65	00	00	95	02	53	69	7A	65	6F	66	source...Sizeof
00000660	52	65	73	6F	75	72	63	65	00	00	D5	01	4C	6F	63	6B	Resource..ÕLock
00000670	52	65	73	6F	75	72	63	65	00	00	C7	01	4C	6F	61	64	Resource..ÇLoad
00000680	52	65	73	6F	75	72	63	65	00	00	A3	00	46	69	6E	64	Resource..£.Find
00000690	52	65	73	6F	75	72	63	65	41	00	59	01	47	65	74	53	ResourceA.YGetS
000006A0	79	73	74	65	6D	44	69	72	65	63	74	6F	72	79	41	00	ystemDirectoryA.
000006B0	96	02	53	6C	65	65	70	00	4B	45	52	4E	45	4C	33	32	..Sleep.KERNEL32
000006C0	2E	64	6C	6C	00	00	CA	00	47	65	74	43	6F	6D	6D	61	.dll..ÊGetComma
000006D0	6E	64	4C	69	6E	65	41	00	74	01	47	65	74	56	65	72	ndLineA.tGetVer
000006E0	73	69	6F	6E	00	00	7D	00	45	78	69	74	50	72	6F	63	sion..}.ExitProc
000006F0	65	73	73	00	9E	02	54	65	72	6D	69	6E	61	74	65	50	ess..TerminateP
00000700	72	6F	63	65	73	73	00	00	F7	00	47	65	74	43	75	72	rocess..÷.GetCur
00000710	72	65	6E	74	50	72	6F	63	65	73	73	00	AD	02	55	6E	rentProcess.-Un
00000720	68	61	6E	64	6C	65	64	45	78	63	65	70	74	69	6F	6E	handledException
00000730	46	69	6C	74	65	72	00	00	24	01	47	65	74	4D	6F	64	Filter..$GetMod
00000740	75	6C	65	46	69	6C	65	4E	61	6D	65	41	00	00	B2	00	uleFileNameA..²
00000750	46	72	65	65	45	6E	76	69	72	6F	6E	6D	65	6E	74	53	FreeEnvironmentS
00000760	74	72	69	6E	67	73	41	00	B3	00	46	72	65	65	45	6E	tringsA.³.FreeEn
00000770	76	69	72	6F	6E	6D	65	6E	74	53	74	72	69	6E	67	73	vironmentStrings
00000780	57	00	D2	02	57	69	64	65	43	68	61	72	54	6F	4D	75	W.ÒWideCharToMu
00000790	6C	74	69	42	79	74	65	00	06	01	47	65	74	45	6E	76	ltiByte..GetEnv
000007A0	69	72	6F	6E	6D	65	6E	74	53	74	72	69	6E	67	73	00	ironmentStrings.
000007B0	08	01	47	65	74	45	6E	76	69	72	6F	6E	6D	65	6E	74	..GetEnvironment
000007C0	53	74	72	69	6E	67	73	57	00	00	6D	02	53	65	74	48	StringsW..mSetH
000007D0	61	6E	64	6C	65	43	6F	75	6E	74	00	00	52	01	47	65	andleCount..RGe
000007E0	74	53	74	64	48	61	6E	64	6C	65	00	00	15	01	47	65	tStdHandle...Ge
000007F0	74	46	69	6C	65	54	79	70	65	00	50	01	47	65	74	53	tFileType.PGetS
00000800	74	61	72	74	75	70	49	6E	66	6F	41	00	9D	01	48	65	tartupInfoA..He
00000810	61	70	44	65	73	74	72	6F	79	00	9B	01	48	65	61	70	apDestroy..Heap
00000820	43	72	65	61	74	65	00	00	9F	01	48	65	61	70	46	72	Create...HeapFr
00000830	65	65	00	00	2F	02	52	74	6C	55	6E	77	69	6E	64	00	ee../RtlUnwind.
00000840	DF	02	57	72	69	74	65	46	69	6C	65	00	99	01	48	65	ß.WriteFile..He

Time of Day	Process Name	PID	Operation	Path	Result	Detail
1:34:47.82173...	Malware_U3_W2_L2.exe	1232	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Malware_U3_W2_L2.exe	NAME NOT FOUND	Desired Access: Read
1:34:47.82313...	Malware_U3_W2_L2.exe	1232	RegOpenKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS	Desired Access: Read
1:34:47.82318...	Malware_U3_W2_L2.exe	1232	RegQueryValue	HKLM\System\CurrentControlSet\Control\Terminal Server\TSAppCompat	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
1:34:47.82321...	Malware_U3_W2_L2.exe	1232	RegCloseKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS	
1:34:47.82860...	Malware_U3_W2_L2.exe	1232	RegOpenKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS	Desired Access: Read
1:34:47.82864...	Malware_U3_W2_L2.exe	1232	RegQueryValue	HKLM\System\CurrentControlSet\Control\Terminal Server\TSAppCompat	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
1:34:47.82883...	Malware_U3_W2_L2.exe	1232	RegCloseKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS	
1:34:47.83017...	Malware_U3_W2_L2.exe	1232	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager\AppCertDlls	NAME NOT FOUND	Desired Access: Query Value
1:34:47.83020...	Malware_U3_W2_L2.exe	1232	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager\AppCompatibility	SUCCESS	Desired Access: Query Value
1:34:47.83024...	Malware_U3_W2_L2.exe	1232	RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\AppCompatibility\DisableAppCompat	NAME NOT FOUND	Length: 20
1:34:47.83027...	Malware_U3_W2_L2.exe	1232	RegCloseKey	HKLM\System\CurrentControlSet\Control\Session Manager\AppCompatibility	SUCCESS	
1:34:47.83268...	Malware_U3_W2_L2.exe	1232	RegOpenKey	HKLM\System\CurrentControlSet\Control\SafeBoot\Option	NAME NOT FOUND	Desired Access: Query Value, Set Value
1:34:47.83271...	Malware_U3_W2_L2.exe	1232	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	SUCCESS	Desired Access: Query Value
1:34:47.83274...	Malware_U3_W2_L2.exe	1232	RegQueryValue	HKLM\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers\TransparentEnabled	SUCCESS	Type: REG_DWORD, Length: 4, Data: 1
1:34:47.83277...	Malware_U3_W2_L2.exe	1232	RegCloseKey	HKLM\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers	SUCCESS	
1:34:47.83280...	Malware_U3_W2_L2.exe	1232	RegOpenKey	HKCU\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	NAME NOT FOUND	Desired Access: Query Value
1:34:47.83332...	Malware_U3_W2_L2.exe	1232	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Apphelp.dll	NAME NOT FOUND	Desired Access: Read
1:34:47.83334...	Malware_U3_W2_L2.exe	1232	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\ntdll.dll	NAME NOT FOUND	Desired Access: Read
1:34:47.83336...	Malware_U3_W2_L2.exe	1232	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\kernel32.dll	NAME NOT FOUND	Desired Access: Read
1:34:47.83483...	Malware_U3_W2_L2.exe	1232	RegOpenKey	HKLM\System\WPA\TabletPC	NAME NOT FOUND	Desired Access: Query Value, WOW64_64Key
1:34:47.83485...	Malware_U3_W2_L2.exe	1232	RegOpenKey	HKLM\SYSTEM\WPA\MediaCenter	SUCCESS	Desired Access: Query Value, WOW64_64Key
1:34:47.83492...	Malware_U3_W2_L2.exe	1232	RegQueryValue	HKLM\SYSTEM\WPA\MediaCenter\Installed	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
1:34:47.83495...	Malware_U3_W2_L2.exe	1232	RegCloseKey	HKLM\SYSTEM\WPA\MediaCenter	SUCCESS	
1:34:47.83803...	Malware_U3_W2_L2.exe	1232	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers	NAME NOT FOUND	Desired Access: Read, WOW64_64Key
1:34:47.83807...	Malware_U3_W2_L2.exe	1232	RegOpenKey	HKCU\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers	SUCCESS	Desired Access: Read, WOW64_64Key
1:34:47.83811...	Malware_U3_W2_L2.exe	1232	RegQueryValue	HKCU\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers\C:\WINDOWS\system32\svchost.exe	NAME NOT FOUND	Length: 1,024
1:34:47.83815...	Malware_U3_W2_L2.exe	1232	RegCloseKey	HKCU\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers	SUCCESS	
1:34:47.83816...	Malware_U3_W2_L2.exe	1232	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Custom\svchost.exe	NAME NOT FOUND	Desired Access: Read, WOW64_64Key
1:34:47.83864...	Malware_U3_W2_L2.exe	1232	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Query Value
1:34:47.83869...	Malware_U3_W2_L2.exe	1232	RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\SafeDllSearchMode	NAME NOT FOUND	Length: 16
1:34:47.83872...	Malware_U3_W2_L2.exe	1232	RegCloseKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	
1:34:47.83904...	Malware_U3_W2_L2.exe	1232	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\VERSION.dll	NAME NOT FOUND	Desired Access: Read
1:34:47.84163...	Malware_U3_W2_L2.exe	1232	RegOpenKey	HKCU	SUCCESS	Desired Access: Maximum Allowed
1:34:47.84166...	Malware_U3_W2_L2.exe	1232	RegOpenKey	HKCU\Software\Policies\Microsoft\Control Panel\Desktop	NAME NOT FOUND	Desired Access: Read
1:34:47.84168...	Malware_U3_W2_L2.exe	1232	RegOpenKey	HKCU\Control Panel\Desktop	SUCCESS	Desired Access: Read
1:34:47.84171...	Malware_U3_W2_L2.exe	1232	RegQueryValue	HKCU\Control Panel\Desktop\MultiUILanguageId	NAME NOT FOUND	Length: 256
1:34:47.84174...	Malware_U3_W2_L2.exe	1232	RegCloseKey	HKCU\Control Panel\Desktop	SUCCESS	
1:34:47.84176...	Malware_U3_W2_L2.exe	1232	RegCloseKey	HKCU	SUCCESS	
1:34:47.84555...	Malware_U3_W2_L2.exe	1232	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags	NAME NOT FOUND	Desired Access: Read, WOW64_64Key
1:34:47.84558...	Malware_U3_W2_L2.exe	1232	RegOpenKey	HKCU\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags	SUCCESS	Desired Access: Read, WOW64_64Key
1:34:47.84562...	Malware_U3_W2_L2.exe	1232	RegQueryValue	HKCU\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\{9321dd42-0077-4508-9895-b08d86772699}	NAME NOT FOUND	Length: 1,024
1:34:47.84565...	Malware_U3_W2_L2.exe	1232	RegCloseKey	HKCU\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags	SUCCESS	
1:34:47.84812...	Malware_U3_W2_L2.exe	1232	RegOpenKey	HKLM\System\CurrentControlSet\Control\SafeBoot\Option	NAME NOT FOUND	Desired Access: Query Value, Set Value
1:34:47.84814...	Malware_U3_W2_L2.exe	1232	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	SUCCESS	Desired Access: Query Value
1:34:47.84818...	Malware_U3_W2_L2.exe	1232	RegQueryValue	HKLM\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers\TransparentEnabled	SUCCESS	Type: REG_DWORD, Length: 4, Data: 1
1:34:47.84819...	Malware_U3_W2_L2.exe	1232	RegQueryValue	HKLM\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers\AuthenticodeEnabled	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
1:34:47.84822...	Malware_U3_W2_L2.exe	1232	RegCloseKey	HKLM\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers	SUCCESS	
1:34:47.84907...	Malware_U3_W2_L2.exe	1232	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Secur32.dll	NAME NOT FOUND	Desired Access: Read
1:34:47.84912...	Malware_U3_W2_L2.exe	1232	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\RPCRT4.dll	NAME NOT FOUND	Desired Access: Read
1:34:47.84915...	Malware_U3_W2_L2.exe	1232	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\ADVAPI32.DLL	NAME NOT FOUND	Desired Access: Read
1:34:47.84918...	Malware_U3_W2_L2.exe	1232	RegOpenKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS	Desired Access: Read
1:34:47.84921...	Malware_U3_W2_L2.exe	1232	RegQueryValue	HKLM\System\CurrentControlSet\Control\Terminal Server\TSAppCompat	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
1:34:47.84923...	Malware_U3_W2_L2.exe	1232	RegQueryValue	HKLM\System\CurrentControlSet\Control\Terminal Server\TSUserEnabled	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
1:34:47.84926...	Malware_U3_W2_L2.exe	1232	RegCloseKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS	

3:11:41.41260...	svchost.exe	2424	CreateFile	C:\WINDOWS\system32\vpcrt4.dll	SUCCESS	Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-Directory File, Attributes: N, ShareMode: Read,
3:11:41.41279...	svchost.exe	2424	CreateFileMapping	C:\WINDOWS\system32\vpcrt4.dll	SUCCESS	SyncType: SyncTypeCreateSection, PageProtection: PAGE_READWRITE
3:11:41.41281...	svchost.exe	2424	QueryStandardInformationFile	C:\WINDOWS\system32\vpcrt4.dll	SUCCESS	AllocationSize: 585,728, EndOfFile: 584,704, NumberOfLinks: 1, DeletePending: False, Directory: False
3:11:41.41284...	svchost.exe	2424	CreateFileMapping	C:\WINDOWS\system32\vpcrt4.dll	SUCCESS	SyncType: SyncTypeOther
3:11:41.41309...	svchost.exe	2424	CreateFile	C:\WINDOWS\system32\secur32.dll	SUCCESS	Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-Directory File, Attributes: N, ShareMode: Read,
3:11:41.41328...	svchost.exe	2424	CreateFileMapping	C:\WINDOWS\system32\secur32.dll	SUCCESS	SyncType: SyncTypeCreateSection, PageProtection: PAGE_READWRITE
3:11:41.41330...	svchost.exe	2424	QueryStandardInformationFile	C:\WINDOWS\system32\secur32.dll	SUCCESS	AllocationSize: 57,344, EndOfFile: 56,320, NumberOfLinks: 1, DeletePending: False, Directory: False
3:11:41.41334...	svchost.exe	2424	CreateFileMapping	C:\WINDOWS\system32\secur32.dll	SUCCESS	SyncType: SyncTypeOther
3:11:41.41360...	svchost.exe	2424	CreateFile	C:\WINDOWS\system32\winmm.dll	SUCCESS	Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-Directory File, Attributes: N, ShareMode: Read,
3:11:41.41380...	svchost.exe	2424	CreateFileMapping	C:\WINDOWS\system32\winmm.dll	SUCCESS	SyncType: SyncTypeCreateSection, PageProtection: PAGE_READWRITE
3:11:41.41381...	svchost.exe	2424	QueryStandardInformationFile	C:\WINDOWS\system32\winmm.dll	SUCCESS	AllocationSize: 176,128, EndOfFile: 176,128, NumberOfLinks: 1, DeletePending: False, Directory: False
3:11:41.41385...	svchost.exe	2424	CreateFileMapping	C:\WINDOWS\system32\winmm.dll	SUCCESS	SyncType: SyncTypeOther
3:11:41.41410...	svchost.exe	2424	CreateFile	C:\WINDOWS\system32\ole32.dll	SUCCESS	Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-Directory File, Attributes: N, ShareMode: Read,
3:11:41.41429...	svchost.exe	2424	CreateFileMapping	C:\WINDOWS\system32\ole32.dll	SUCCESS	SyncType: SyncTypeCreateSection, PageProtection: PAGE_READWRITE
3:11:41.41431...	svchost.exe	2424	QueryStandardInformationFile	C:\WINDOWS\system32\ole32.dll	SUCCESS	AllocationSize: 1,290,240, EndOfFile: 1,287,168, NumberOfLinks: 1, DeletePending: False, Directory: False
3:11:41.41435...	svchost.exe	2424	CreateFileMapping	C:\WINDOWS\system32\ole32.dll	SUCCESS	SyncType: SyncTypeOther
3:11:41.41460...	svchost.exe	2424	CreateFile	C:\WINDOWS\system32\msvcrt.dll	SUCCESS	Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-Directory File, Attributes: N, ShareMode: Read,
3:11:41.41498...	svchost.exe	2424	CreateFileMapping	C:\WINDOWS\system32\msvcrt.dll	SUCCESS	SyncType: SyncTypeCreateSection, PageProtection: PAGE_READWRITE
3:11:41.41499...	svchost.exe	2424	QueryStandardInformationFile	C:\WINDOWS\system32\msvcrt.dll	SUCCESS	AllocationSize: 344,064, EndOfFile: 343,040, NumberOfLinks: 1, DeletePending: False, Directory: False
3:11:41.41503...	svchost.exe	2424	CreateFileMapping	C:\WINDOWS\system32\msvcrt.dll	SUCCESS	SyncType: SyncTypeOther
3:11:41.41528...	svchost.exe	2424	CreateFile	C:\WINDOWS\system32\oleaut32.dll	SUCCESS	Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-Directory File, Attributes: N, ShareMode: Read,
3:11:41.41550...	svchost.exe	2424	CreateFileMapping	C:\WINDOWS\system32\oleaut32.dll	SUCCESS	SyncType: SyncTypeCreateSection, PageProtection: PAGE_READWRITE
3:11:41.41551...	svchost.exe	2424	QueryStandardInformationFile	C:\WINDOWS\system32\oleaut32.dll	SUCCESS	AllocationSize: 552,960, EndOfFile: 551,936, NumberOfLinks: 1, DeletePending: False, Directory: False
3:11:41.41555...	svchost.exe	2424	CreateFileMapping	C:\WINDOWS\system32\oleaut32.dll	SUCCESS	SyncType: SyncTypeOther
3:11:41.41580...	svchost.exe	2424	CreateFile	C:\WINDOWS\system32\msacm32.dll	SUCCESS	Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-Directory File, Attributes: N, ShareMode: Read,
3:11:41.41599...	svchost.exe	2424	CreateFileMapping	C:\WINDOWS\system32\msacm32.dll	SUCCESS	SyncType: SyncTypeCreateSection, PageProtection: PAGE_READWRITE
3:11:41.41601...	svchost.exe	2424	QueryStandardInformationFile	C:\WINDOWS\system32\msacm32.dll	SUCCESS	AllocationSize: 73,728, EndOfFile: 71,680, NumberOfLinks: 1, DeletePending: False, Directory: False
3:11:41.41604...	svchost.exe	2424	CreateFileMapping	C:\WINDOWS\system32\msacm32.dll	SUCCESS	SyncType: SyncTypeOther
3:11:41.41629...	svchost.exe	2424	CreateFile	C:\WINDOWS\system32\version.dll	SUCCESS	Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-Directory File, Attributes: N, ShareMode: Read,
3:11:41.41650...	svchost.exe	2424	CreateFileMapping	C:\WINDOWS\system32\version.dll	SUCCESS	SyncType: SyncTypeCreateSection, PageProtection: PAGE_READWRITE
3:11:41.41651...	svchost.exe	2424	QueryStandardInformationFile	C:\WINDOWS\system32\version.dll	SUCCESS	AllocationSize: 20,480, EndOfFile: 18,944, NumberOfLinks: 1, DeletePending: False, Directory: False
3:11:41.41655...	svchost.exe	2424	CreateFileMapping	C:\WINDOWS\system32\version.dll	SUCCESS	SyncType: SyncTypeOther
3:11:41.41680...	svchost.exe	2424	CreateFile	C:\WINDOWS\system32\shell32.dll	SUCCESS	Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-Directory File, Attributes: N, ShareMode: Read,
3:11:41.41699...	svchost.exe	2424	CreateFileMapping	C:\WINDOWS\system32\shell32.dll	SUCCESS	SyncType: SyncTypeCreateSection, PageProtection: PAGE_READWRITE
3:11:41.41700...	svchost.exe	2424	QueryStandardInformationFile	C:\WINDOWS\system32\shell32.dll	SUCCESS	AllocationSize: 8,462,336, EndOfFile: 8,461,312, NumberOfLinks: 1, DeletePending: False, Directory: False
3:11:41.41704...	svchost.exe	2424	CreateFileMapping	C:\WINDOWS\system32\shell32.dll	SUCCESS	SyncType: SyncTypeOther
3:11:41.41723...	svchost.exe	2424	CreateFile	C:\WINDOWS\system32\shlwapi.dll	SUCCESS	Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-Directory File, Attributes: N, ShareMode: Read,
3:11:41.41749...	svchost.exe	2424	CreateFileMapping	C:\WINDOWS\system32\shlwapi.dll	SUCCESS	SyncType: SyncTypeCreateSection, PageProtection: PAGE_READWRITE
3:11:41.41751...	svchost.exe	2424	QueryStandardInformationFile	C:\WINDOWS\system32\shlwapi.dll	SUCCESS	AllocationSize: 475,136, EndOfFile: 474,112, NumberOfLinks: 1, DeletePending: False, Directory: False
3:11:41.41755...	svchost.exe	2424	CreateFileMapping	C:\WINDOWS\system32\shlwapi.dll	SUCCESS	SyncType: SyncTypeOther
3:11:41.41780...	svchost.exe	2424	CreateFile	C:\WINDOWS\system32\userenv.dll	SUCCESS	Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-Directory File, Attributes: N, ShareMode: Read,
3:11:41.41799...	svchost.exe	2424	CreateFileMapping	C:\WINDOWS\system32\userenv.dll	SUCCESS	SyncType: SyncTypeCreateSection, PageProtection: PAGE_READWRITE
3:11:41.41801...	svchost.exe	2424	QueryStandardInformationFile	C:\WINDOWS\system32\userenv.dll	SUCCESS	AllocationSize: 729,088, EndOfFile: 727,040, NumberOfLinks: 1, DeletePending: False, Directory: False
3:11:41.41804...	svchost.exe	2424	CreateFileMapping	C:\WINDOWS\system32\userenv.dll	SUCCESS	SyncType: SyncTypeOther
3:11:41.41840...	svchost.exe	2424	CreateFile	C:\WINDOWS\system32\uxtheme.dll	SUCCESS	Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-Directory File, Attributes: N, ShareMode: Read,
3:11:41.41861...	svchost.exe	2424	CreateFileMapping	C:\WINDOWS\system32\uxtheme.dll	SUCCESS	SyncType: SyncTypeCreateSection, PageProtection: PAGE_READWRITE
3:11:41.41862...	svchost.exe	2424	QueryStandardInformationFile	C:\WINDOWS\system32\uxtheme.dll	SUCCESS	AllocationSize: 221,184, EndOfFile: 218,624, NumberOfLinks: 1, DeletePending: False, Directory: False
3:11:41.41866...	svchost.exe	2424	CreateFileMapping	C:\WINDOWS\system32\uxtheme.dll	SUCCESS	SyncType: SyncTypeOther
3:11:41.41891...	svchost.exe	2424	CreateFile	C:\WINDOWS\system32\ctype.nls	SUCCESS	Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-Directory File, Attributes: N, ShareMode: Read,
3:11:41.41910...	svchost.exe	2424	CreateFileMapping	C:\WINDOWS\system32\ctype.nls	SUCCESS	SyncType: SyncTypeCreateSection, PageProtection: PAGE_READWRITE
3:11:41.41911...	svchost.exe	2424	QueryStandardInformationFile	C:\WINDOWS\system32\ctype.nls	SUCCESS	AllocationSize: 12,288, EndOfFile: 8,386, NumberOfLinks: 1, DeletePending: False, Directory: False
3:11:41.41915...	svchost.exe	2424	CreateFileMapping	C:\WINDOWS\system32\ctype.nls	SUCCESS	SyncType: SyncTypeOther
3:11:41.41940...	svchost.exe	2424	CreateFile	C:\WINDOWS\system32\sortkey.nls	SUCCESS	Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-Directory File, Attributes: N, ShareMode: Read,
3:11:41.41960...	svchost.exe	2424	CreateFileMapping	C:\WINDOWS\system32\sortkey.nls	SUCCESS	SyncType: SyncTypeCreateSection, PageProtection: PAGE_READWRITE