Anubis - Analysis Report

Analysis Report for file

MD5: f2e926746faccc7a1e8174fdf0cb0535

Summary:

Description	Risk
Write to foreign memory areas: This executable tampers with the execution of another process.	high
Performs File Modification and Destruction: The executable modifies and destructs files which are not temporary.	low
Changes security settings of Internet Explorer: This system alteration could seriously affect safety surfing the World Wide Web.	low
Creates files in the Windows system directory: Malware often keeps copies of itself in the Windows directory to stay undetected by users.	medium
Spawns Processes: The executable produces processes during the execution.	low
Execution did not terminate correctly: The executable crashed.	medium
Modify system files: This executable modifies files in the windows system directories.	medium
Performs Registry Activities: The executable creates and/or modifies registry entries.	low

Dependency overview:

- **file.exe** C:\file.exe
  Analysis reason: Primary Analysis Subject
  - **Explorer.EXE** C:\WINDOWS\Explorer.EXE
    Analysis reason: file.exe wrote to the virtual memory of this process
  - **cmd.exe** C:\WINDOWS\system32\cmd.exe
    Analysis reason: Started by file.exe
    - **attrib.exe** C:\WINDOWS\system32\attrib.exe
      Analysis reason: Started by cmd.exe

Table of Contents:

1. General Information

Information about Anubis' invocation	
Time needed:	256 s
Report created:	11/01/12, 14:04:21 UTC
Termination reason:	Timeout
Program version:	1.76.3886

2. file.exe

General information about this executable	
Analysis Reason:	Primary Analysis Subject
Filename:	file.exe
MD5:	f2e926746faccc7a1e8174fdf0cb0535
SHA-1:	11b6ed3b5107ca2379a267a91bedb0dd74429229
File Size:	205824
Command Line:	"C:\file.exe"
Process-status at analysis end:	dead
Exit Code:	0

Load-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\ntdll.dll	0x7C900000	0x000AF000
C:\WINDOWS\system32\kernel32.dll	0x7C800000	0x000F6000
C:\WINDOWS\system32\USER32.dll	0x7E410000	0x00091000
C:\WINDOWS\system32\GDI32.dll	0x77F10000	0x00049000

Run-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\dfrgnet.dll	0x10000000	0x00011000
C:\WINDOWS\system32\netapi32.dll	0x5B860000	0x00055000
C:\WINDOWS\system32\comctl32.dll	0x5D090000	0x0009A000
C:\WINDOWS\system32\MSISIP.DLL	0x605F0000	0x00007000
C:\WINDOWS\system32\rsaenh.dll	0x68000000	0x00036000
C:\WINDOWS\system32\MSCTF.dll	0x74720000	0x0004C000
C:\WINDOWS\system32\PSAPI.DLL	0x76BF0000	0x0000B000
C:\WINDOWS\system32\WINTRUST.dll	0x76C30000	0x0002E000
C:\WINDOWS\system32\IMAGEHLP.dll	0x76C90000	0x00028000
C:\WINDOWS\system32\CLBCATQ.DLL	0x76FD0000	0x0007F000
C:\WINDOWS\system32\COMRes.dll	0x77050000	0x000C5000
C:\WINDOWS\system32\OLEAUT32.dll	0x77120000	0x0008B000
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll	0x773D0000	0x00103000
C:\WINDOWS\system32\ole32.dll	0x774E0000	0x0013D000
C:\WINDOWS\system32\SETUPAPI.dll	0x77920000	0x000F3000
C:\WINDOWS\system32\CRYPT32.dll	0x77A80000	0x00095000
C:\WINDOWS\system32\MSASN1.dll	0x77B20000	0x00012000
C:\WINDOWS\system32\Apphelp.dll	0x77B40000	0x00022000
C:\WINDOWS\system32\VERSION.dll	0x77C00000	0x00008000
C:\WINDOWS\system32\msvcrt.dll	0x77C10000	0x00058000
C:\WINDOWS\system32\ADVAPI32.dll	0x77DD0000	0x0009B000
C:\WINDOWS\system32\RPCRT4.dll	0x77E70000	0x00092000
C:\WINDOWS\system32\SHLWAPI.dll	0x77F60000	0x00076000
C:\WINDOWS\system32\Secur32.dll	0x77FE0000	0x00011000
C:\WINDOWS\system32\SHELL32.dll	0x7C9C0000	0x00817000
C:\WINDOWS\system32\wshext.dll	0x7DFA0000	0x00016000
C:\WINDOWS\system32\urlmon.dll	0x7E1E0000	0x000A2000

2.a) file.exe - Registry Activities

Registry Keys Created:

HKLM\System\CurrentControlSet\Control\Session Manager\AppCertDlls

Registry Values Modified:

Key	Name	New Value
HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	Common Desktop	C:\Documents and Settings\All Users\Desktop
HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	Common Documents	C:\Documents and Settings\All Users\Documents
HKLM\System\CurrentControlSet\Control\Session Manager\AppCertDlls	mqtgstat	C:\WINDOWS\system32\dfrgnet.dll
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{a1094da8-30a0-11dd-817b-806d6172696f}\	BaseClass	Drive
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{a1094daa-30a0-11dd-817b-806d6172696f}\	BaseClass	Drive
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	Cache	C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	Cookies	C:\Documents and Settings\Administrator\Cookies
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	Desktop	C:\Documents and Settings\Administrator\Desktop
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	Personal	C:\Documents and Settings\Administrator\My Documents
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\	IntranetName	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\	ProxyBypass	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\	UNCAsIntranet	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\ShellNoRoam\MUICache\	C:\439687.bat	439687

Registry Values Read:

Key	Name	Value	Times
HKLM\SOFTWARE\CLASSES\.ASP		aspfile	1
HKLM\SOFTWARE\CLASSES\.BAT		batfile	3
HKLM\SOFTWARE\CLASSES\BATFILE\SHELL\OPEN\COMMAND		"%1" %*	2
HKLM\SOFTWARE\CLASSES\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\INPROCSERVER32		%SystemRoot%\system32\SHELL32.dll	1
HKLM\SOFTWARE\CLASSES\CLSID\{7B8A2D94-0AC9-11D1-896C-00C04FB6BFC4}\INPROCSERVER32		C:\WINDOWS\system32\urlmon.dll	2
HKLM\SOFTWARE\CLASSES\CLSID\{7B8A2D94-0AC9-11D1-896C-00C04FB6BFC4}\INPROCSERVER32	ThreadingModel	Both	1
HKLM\SOFTWARE\CLASSES\CLSID\{AEB6717E-7E19-11D0-97EE-00C04FD91972}\INPROCSERVER32		shell32.dll	1
HKLM\SOFTWARE\CLASSES\DIRECTORY	AlwaysShowExt		1
HKLM\SOFTWARE\CLASSES\DRIVE\SHELLEX\FOLDEREXTENSIONS\{FBEB8A05-BEEE-4442-804E-409D6C4515E9}	DriveMask	32	1
HKLM\SOFTWARE\Microsoft\CTF\SystemShared\	CUAS	0	1
HKLM\SOFTWARE\Microsoft\Cryptography\Defaults\Provider Types\Type 001	Name	Microsoft Strong Cryptographic Provider	4
HKLM\SOFTWARE\Microsoft\Cryptography\Defaults\Provider\Microsoft Strong Cryptographic Provider	Image Path	rsaenh.dll	4

Registry Values Read:

Key	Name	Value	Times
HKLM\SOFTWARE\Microsoft\Cryptography\Defaults\Provider\Microsoft Strong Cryptographic Provider	Type	1	1
HKLM\SYSTEM\CurrentControlSet\Control\Session Manager	CriticalSectionTimeout	2592000	1
HKLM\SYSTEM\Setup	OsLoaderPath	\	2
HKLM\SYSTEM\Setup	SystemPartition	\Device\HarddiskVolume1	2
HKLM\SYSTEM\Setup	SystemSetupInProgres	0	1
HKLM\SYSTEM\WPA\MediaCenter	Installed	0	1
HKLM\Software\Microsoft\COM3	Com+Enabled	1	2
HKLM\Software\Microsoft\COM3	REGDBVersion	0x0b00000000000000	2
HKLM\Software\Microsoft\Cryptography	MachineGuid	4604e8cc-5b9c-4ffb-a374-a62e6d0494fc	4
HKLM\Software\Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDllIsMyFileType2\{000C10F1-0000-0000-C000-000000000046}	Dll	MSISIP.DLL	2
HKLM\Software\Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDllIsMyFileType2\{000C10F1-0000-0000-C000-000000000046}	FuncName	MsiSIPIsMyTypeOfFile	2
HKLM\Software\Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDllIsMyFileType2\{06C9E010-38CE-11D4-A2A3-00104BD35090}	Dll	C:\WINDOWS\system32\wshext.dll	2
HKLM\Software\Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDllIsMyFileType2\{06C9E010-38CE-11D4-A2A3-00104BD35090}	FuncName	IsFileSupportedName	2
HKLM\Software\Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDllIsMyFileType2\{1629F04E-2799-4DB5-8FE5-ACE10F17EBAB}	Dll	C:\WINDOWS\system32\wshext.dll	2
HKLM\Software\Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDllIsMyFileType2\{1629F04E-2799-4DB5-8FE5-ACE10F17EBAB}	FuncName	IsFileSupportedName	2
HKLM\Software\Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDllIsMyFileType2\{1A610570-38CE-11D4-A2A3-00104BD35090}	Dll	C:\WINDOWS\system32\wshext.dll	2
HKLM\Software\Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDllIsMyFileType2\{1A610570-38CE-11D4-A2A3-00104BD35090}	FuncName	IsFileSupportedName	2
HKLM\Software\Microsoft\Cryptography\Providers\Trust\CertCheck\{00AAC56B-CD44-11D0-8CC2-00C04FC295EE}	$DLL	WINTRUST.DLL	1
HKLM\Software\Microsoft\Cryptography\Providers\Trust\CertCheck\{00AAC56B-CD44-11D0-8CC2-00C04FC295EE}	$Function	SoftpubCheckCert	1
HKLM\Software\Microsoft\Cryptography\Providers\Trust\Certificate\{00AAC56B-CD44-11D0-8CC2-00C04FC295EE}	$DLL	WINTRUST.DLL	1
HKLM\Software\Microsoft\Cryptography\Providers\Trust\Certificate\{00AAC56B-CD44-11D0-8CC2-00C04FC295EE}	$Function	WintrustCertificateTrust	1
HKLM\Software\Microsoft\Cryptography\Providers\Trust\Cleanup\{00AAC56B-CD44-11D0-8CC2-00C04FC295EE}	$DLL	WINTRUST.DLL	1
HKLM\Software\Microsoft\Cryptography\Providers\Trust\Cleanup\{00AAC56B-CD44-11D0-8CC2-00C04FC295EE}	$Function	SoftpubCleanup	1
HKLM\Software\Microsoft\Cryptography\Providers\Trust\FinalPolicy\{00AAC56B-CD44-11D0-8CC2-00C04FC295EE}	$DLL	WINTRUST.DLL	1
HKLM\Software\Microsoft\Cryptography\Providers\Trust\FinalPolicy\{00AAC56B-CD44-11D0-8CC2-00C04FC295EE}	$Function	SoftpubAuthenticode	1
HKLM\Software\Microsoft\Cryptography\Providers\Trust\Initialization\{00AAC56B-CD44-11D0-8CC2-00C04FC295EE}	$DLL	WINTRUST.DLL	1
HKLM\Software\Microsoft\Cryptography\Providers\Trust\Initialization\{00AAC56B-CD44-11D0-8CC2-00C04FC295EE}	$Function	SoftpubInitialize	1

Registry Values Read:

Key	Name	Value	Times
HKLM\Software\Microsoft\Cryptography\Providers\Trust\Message\{00AAC56B-CD44-11D0-8CC2-00C04FC295EE}	$DLL	WINTRUST.DLL	1
HKLM\Software\Microsoft\Cryptography\Providers\Trust\Message\{00AAC56B-CD44-11D0-8CC2-00C04FC295EE}	$Function	SoftpubLoadMessage	1
HKLM\Software\Microsoft\Cryptography\Providers\Trust\Signature\{00AAC56B-CD44-11D0-8CC2-00C04FC295EE}	$DLL	WINTRUST.DLL	1
HKLM\Software\Microsoft\Cryptography\Providers\Trust\Signature\{00AAC56B-CD44-11D0-8CC2-00C04FC295EE}	$Function	SoftpubLoadSignature	1
HKLM\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_BEHAVIORS	*	1	1
HKLM\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_DISABLE_MK_PROTOCOL	*	1	1
HKLM\Software\Microsoft\Windows\CurrentVersion	DevicePath	%SystemRoot%\inf	1
HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\FileAssociation	CutList	0x4100700070006c0069006300610074006669006f006e002000460069006c00	2
HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellExecuteHooks	{AEB6717E-7E19-11d0		1
HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	Common Desktop	%ALLUSERSPROFILE%\Desktop	1
HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	Common Documents	%ALLUSERSPROFILE%\Documents	1
HKLM\Software\Microsoft\Windows\CurrentVersion\Setup	DriverCachePath	%SystemRoot%\Driver Cache	2
HKLM\Software\Microsoft\Windows\CurrentVersion\Setup	LogLevel	0	2
HKLM\Software\Microsoft\Windows\CurrentVersion\Setup	ServicePackCachePath	c:\windows\ServicePackFiles\ServicePackCache	2
HKLM\Software\Microsoft\Windows\CurrentVersion\Setup	ServicePackSourcePat	D:\	2
HKLM\Software\Microsoft\Windows\CurrentVersion\Setup	SourcePath	D:\	2
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	AuthenticodeEnabled	0	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	DefaultLevel	262144	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	ExecutableTypes	0x4100440045000000410044005000000042004100530000004200410053000000420041005400	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	PolicyScope	0	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	TransparentEnabled	1	3
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{349d35ab-37b5-462f-9b89-edd5fbde1328}	HashAlg	32771	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{349d35ab-37b5-462f-9b89-edd5fbde1328}	ItemData	0x5eab304f957a49896a006c1c31154015	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{349d35ab-37b5-462f-9b89-edd5fbde1328}	ItemSize	779	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{349d35ab-37b5-462f-9b89-edd5fbde1328}	SaferFlags	0	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{7fb9cd2e-3076-4df9-a57b-b813f72dbb91}	HashAlg	32771	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{7fb9cd2e-3076-4df9-a57b-b813f72dbb91}	ItemData	0x67b0d48b343a3fd3bce9dc646704f394	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{7fb9cd2e-3076-4df9-a57b-b813f72dbb91}	ItemSize	517	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{7fb9cd2e-3076-4df9-a57b-b813f72dbb91}	SaferFlags	0	1

Registry Values Read:

Key	Name	Value	Times
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f}	HashAlg	32771	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f}	ItemData	0x327802dcfef8c893dc8ab006dd847d1d	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f}	ItemSize	918	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f}	SaferFlags	0	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}	HashAlg	32771	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}	ItemData	0xbd9a2adb42ebd8560e250e4df8162f67	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}	ItemSize	229	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}	SaferFlags	0	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{dc971ee5-44eb-4fe4-ae2e-b91490411bfc}	HashAlg	32771	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{dc971ee5-44eb-4fe4-ae2e-b91490411bfc}	ItemData	0x386b085f84ecf669d36b956a22c01e80	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{dc971ee5-44eb-4fe4-ae2e-b91490411bfc}	ItemSize	370	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{dc971ee5-44eb-4fe4-ae2e-b91490411bfc}	SaferFlags	0	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Paths\{dda3f824-d8cb-441b-834d-be2efd2c1a33}	ItemData	%HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cache%OLK*	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Paths\{dda3f824-d8cb-441b-834d-be2efd2c1a33}	SaferFlags	0	1
HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName	ComputerName	PC	2
HKLM\System\CurrentControlSet\Control\Session Manager\AppCertDlls	mqtgstat	C:\WINDOWS\system32\dfrgnet.dll	1
HKLM\System\CurrentControlSet\Control\Terminal Server	TSUserEnabled	0	1
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	Domain		1
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	Hostname	pc	1
HKLM\System\Setup	SystemSetupInProgres	0	2
HKLM\System\WPA\PnP	seed	1274198464	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Keyboard Layout\Toggle	Language Hotkey	1	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\Keyboard Layout\Toggle	Layout Hotkey	2	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Internet Explorer\Security	Safety Warning Level	Query	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\	ShellState	0x240000003808000000000000000000000000000000010000000d0000000000	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	DontPrettyPath	0	1

Registry Values Read:

Key	Name	Value	Times
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	Filter	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	Hidden	1	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	HideFileExt	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	HideIcons	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	MapNetDrvBtn	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	NoNetCrawling	1	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	SeparateProcess	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	ShowCompColor	1	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	ShowInfoTip	1	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	ShowSuperHidden	1	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	WebView	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{a1094da8-30a0-11dd-817b-806d6172696f}\	Data	0x000000005c005c003f005c00490044004450023004300640052006f006d00	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{a1094da8-30a0-11dd-817b-806d6172696f}\	Generation	1	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{a1094daa-30a0-11dd-817b-806d6172696f}\	Data	0x000000005c005c003f005c00530054004 4f00520041004700450023005600	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{a1094daa-30a0-11dd-817b-806d6172696f}\	Generation	1	5
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	Cache	C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	Cache	%USERPROFILE%\Local Settings\Temporary Internet Files	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	Cookies	%USERPROFILE%\Cookies	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	Desktop	%USERPROFILE%\Desktop	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	Personal	%USERPROFILE%\My Documents	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0	1806	0	1

Registry Values Read:

Key	Name	Value	Times
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0	Flags	33	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1	Flags	219	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\2	Flags	71	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3	Flags	1	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4	Flags	3	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing	State	146432	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\ShellNoRoam\MUICache	LangID	0x0904	1

Monitored Registry Keys:

Key Name	Watch subtree	Notify Filter	Count
HKLM\Software\Classes	1	Key Change,Value Change	3
HKLM\Software\Classes\CLSID	1	Key Change,Value Change	2
HKLM\Software\Microsoft\COM3	1	Key Change,Value Change	6
HKU	1	Key Change,Value Change	3

2.b) file.exe - File Activities

Files Created:

C:\439687.bat
C:\WINDOWS\system32\dfrgnet.dll

Files Read:

C:\439687.bat
C:\Documents and Settings\Administrator\My Documents\desktop.ini
C:\Documents and Settings\All Users\Documents\desktop.ini
C:\WINDOWS\Registration\R000000000000b.clb
C:\WINDOWS\system32\rsaenh.dll
PIPE\lsarpc
PIPE\wkssvc

Files Modified:

C:\439687.bat
C:\WINDOWS\system32\dfrgnet.dll
MountPointManager
PIPE\lsarpc
PIPE\wkssvc

File System Control Communication:

File	Control Code	Times
C:\Program Files\Common Files\	0x00090028	1
PIPE\lsarpc	0x0011C017	14
PIPE\wkssvc	0x0011C017	1

Device Control Communication:

File	Control Code	Times
\Device\KsecDD	0x00390008	8
IDE#CdRomQEMU_QEMU_CD-ROM_____0.9.____#4d513030303020332020202020202020200202020#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}	0x004D0008	1
MountPointManager	0x006D0008	2
STORAGE#Volume#1&30a96598&0&SignatureB15FB15FOffset7E00Length13F2918000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}	0x004D0008	1
MountPointManager	0x006D0034	4

Memory Mapped Files:

File Name
C:\439687.bat
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
C:\WINDOWS\WindowsShell.Manifest
C:\WINDOWS\system32\Apphelp.dll
C:\WINDOWS\system32\CLBCATQ.DLL
C:\WINDOWS\system32\COMRes.dll
C:\WINDOWS\system32\MSCTF.dll
C:\WINDOWS\system32\MSISIP.DLL
C:\WINDOWS\system32\PSAPI.DLL
C:\WINDOWS\system32\SETUPAPI.dll
C:\WINDOWS\system32\SHELL32.dll
C:\WINDOWS\system32\cmd.exe
C:\WINDOWS\system32\comctl32.dll
C:\WINDOWS\system32\dfrgnet.dll
C:\WINDOWS\system32\imm32.dll
C:\WINDOWS\system32\rpcss.dll
C:\WINDOWS\system32\rsaenh.dll
C:\WINDOWS\system32\urlmon.dll
C:\WINDOWS\system32\wshext.dll
C:\Windows\AppPatch\sysmain.sdb
C:\439687.bat

2.c) file.exe - Process Activities

Processes Created:

Executable	Command Line
C:\WINDOWS\system32\cmd.exe	
	"C:\439687.bat" "C:\file.exe"

Remote Threads Created:

Affected Process
C:\WINDOWS\explorer.exe
C:\WINDOWS\system32\cmd.exe

Foreign Memory Regions Read:

Process: C:\WINDOWS\explorer.exe
Process: C:\WINDOWS\system32\cmd.exe

Foreign Memory Regions Written:

Process: C:\WINDOWS\explorer.exe
Process: C:\WINDOWS\system32\cmd.exe

3. Explorer.EXE

General information about this executable

Analysis Reason:	file.exe wrote to the virtual memory of this process
Filename:	Explorer.EXE
MD5:	12896823fb95bfb3dc9b46bcaedc9923
SHA-1:	9d2bf84874abc5b6e9a2744b7865c193c08d362f
File Size:	1033728
Command Line:	C:\WINDOWS\Explorer.EXE
Process-status at analysis end:	alive
Exit Code:	0

Load-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\ntdll.dll	0x7C900000	0x000AF000
C:\WINDOWS\system32\kernel32.dll	0x7C800000	0x000F6000
C:\WINDOWS\system32\ADVAPI32.dll	0x77DD0000	0x0009B000
C:\WINDOWS\system32\RPCRT4.dll	0x77E70000	0x00092000
C:\WINDOWS\system32\Secur32.dll	0x77FE0000	0x00011000
C:\WINDOWS\system32\BROWSEUI.dll	0x75F80000	0x000FD000
C:\WINDOWS\system32\GDI32.dll	0x77F10000	0x00049000
C:\WINDOWS\system32\USER32.dll	0x7E410000	0x00091000
C:\WINDOWS\system32\msvcrt.dll	0x77C10000	0x00058000
C:\WINDOWS\system32\ole32.dll	0x774E0000	0x0013D000
C:\WINDOWS\system32\SHLWAPI.dll	0x77F60000	0x00076000
C:\WINDOWS\system32\OLEAUT32.dll	0x77120000	0x0008B000
C:\WINDOWS\system32\SHDOCVW.dll	0x7E290000	0x00171000
C:\WINDOWS\system32\CRYPT32.dll	0x77A80000	0x00095000
C:\WINDOWS\system32\MSASN1.dll	0x77B20000	0x00012000
C:\WINDOWS\system32\CRYPTUI.dll	0x754D0000	0x00080000
C:\WINDOWS\system32\NETAPI32.dll	0x5B860000	0x00055000
C:\WINDOWS\system32\VERSION.dll	0x77C00000	0x00008000
C:\WINDOWS\system32\WININET.dll	0x771B0000	0x000AA000
C:\WINDOWS\system32\WINTRUST.dll	0x76C30000	0x0002E000
C:\WINDOWS\system32\IMAGEHLP.dll	0x76C90000	0x00028000
C:\WINDOWS\system32\WLDAP32.dll	0x76F60000	0x0002C000
C:\WINDOWS\system32\SHELL32.dll	0x7C9C0000	0x00817000
C:\WINDOWS\system32\UxTheme.dll	0x5AD70000	0x00038000
C:\WINDOWS\system32\ShimEng.dll	0x5CB70000	0x00026000
C:\WINDOWS\AppPatch\AcGenral.DLL	0x6F880000	0x001CA000
C:\WINDOWS\system32\WINMM.dll	0x76B40000	0x0002D000
C:\WINDOWS\system32\MSACM32.dll	0x77BE0000	0x00015000
C:\WINDOWS\system32\USERENV.dll	0x769C0000	0x000B4000
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll	0x773D0000	0x00103000
C:\WINDOWS\system32\comctl32.dll	0x5D090000	0x0009A000
C:\WINDOWS\system32\appHelp.dll	0x77B40000	0x00022000
C:\WINDOWS\system32\CLBCATQ.DLL	0x76FD0000	0x0007F000
C:\WINDOWS\system32\COMRes.dll	0x77050000	0x000C5000
C:\WINDOWS\System32\cscui.dll	0x77A20000	0x00054000
C:\WINDOWS\System32\CSCDLL.dll	0x76600000	0x0001D000
C:\WINDOWS\system32\themeui.dll	0x5BA60000	0x00071000
C:\WINDOWS\system32\MSIMG32.dll	0x76380000	0x00005000
C:\WINDOWS\system32\xpsp2res.dll	0x00AC0000	0x002C5000
C:\WINDOWS\system32\actxprxy.dll	0x71D40000	0x0001B000
C:\WINDOWS\system32\msutb.dll	0x5FC10000	0x00033000
C:\WINDOWS\system32\MSCTF.dll	0x74720000	0x0004C000
C:\WINDOWS\system32\urlmon.dll	0x7E1E0000	0x000A2000
C:\WINDOWS\system32\LINKINFO.dll	0x76980000	0x00008000
C:\WINDOWS\system32\ntshrui.dll	0x76990000	0x00025000

Load-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\ATL.DLL	0x76B20000	0x00011000
C:\WINDOWS\system32\rsaenh.dll	0x68000000	0x00036000
C:\WINDOWS\system32\msi.dll	0x7D1E0000	0x002BC000
C:\WINDOWS\system32\WINSTA.dll	0x76360000	0x00010000
C:\WINDOWS\system32\webcheck.dll	0x74B30000	0x00046000
C:\WINDOWS\system32\WSOCK32.dll	0x71AD0000	0x00009000
C:\WINDOWS\system32\WS2_32.dll	0x71AB0000	0x00017000
C:\WINDOWS\system32\WS2HELP.dll	0x71AA0000	0x00008000
C:\WINDOWS\system32\stobject.dll	0x76280000	0x00021000
C:\WINDOWS\system32\BatMeter.dll	0x74AF0000	0x0000A000
C:\WINDOWS\system32\POWRPROF.dll	0x74AD0000	0x00008000
C:\WINDOWS\system32\SETUPAPI.dll	0x77920000	0x000F3000
C:\WINDOWS\system32\WTSAPI32.dll	0x76F50000	0x00008000
C:\WINDOWS\system32\NETSHELL.dll	0x76400000	0x001A5000
C:\WINDOWS\system32\credui.dll	0x76C00000	0x0002E000
C:\WINDOWS\system32\dot3api.dll	0x478C0000	0x0000A000
C:\WINDOWS\system32\rtutils.dll	0x76E80000	0x0000E000
C:\WINDOWS\system32\dot3dlg.dll	0x736D0000	0x00006000
C:\WINDOWS\system32\OneX.DLL	0x5DCA0000	0x00028000
C:\WINDOWS\system32\eappcfg.dll	0x745B0000	0x00022000
C:\WINDOWS\system32\MSVCP60.dll	0x76080000	0x00065000
C:\WINDOWS\system32\eappprxy.dll	0x5DCD0000	0x0000E000
C:\WINDOWS\system32\iphlpapi.dll	0x76D60000	0x00019000
C:\WINDOWS\system32\MPR.dll	0x71B20000	0x00012000
C:\WINDOWS\System32\drprov.dll	0x75F60000	0x00007000
C:\WINDOWS\System32\ntlanman.dll	0x71C10000	0x0000E000
C:\WINDOWS\System32\NETUI0.dll	0x71CD0000	0x00017000
C:\WINDOWS\System32\NETUI1.dll	0x71C90000	0x00040000
C:\WINDOWS\System32\NETRAP.dll	0x71C80000	0x00007000
C:\WINDOWS\System32\SAMLIB.dll	0x71BF0000	0x00013000
C:\WINDOWS\System32\davclnt.dll	0x75F70000	0x0000A000
C:\WINDOWS\system32\comdlg32.dll	0x763B0000	0x00049000
C:\WINDOWS\system32\MSGINA.dll	0x75970000	0x000F8000
C:\WINDOWS\system32\ODBC32.dll	0x74320000	0x0003D000
C:\WINDOWS\system32\odbcint.dll	0x01350000	0x00017000
C:\WINDOWS\system32\browselc.dll	0x71600000	0x00012000
C:\WINDOWS\system32\shdoclc.dll	0x71800000	0x00088000

Run-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\dfrgnet.dll	0x10000000	0x00011000
C:\WINDOWS\system32\PSAPI.DLL	0x76BF0000	0x0000B000

3.a) Explorer.EXE - File Activities

Files Deleted:

- C:\Documents and Settings\Administrator\Cookies\administrator@adobe[1].txt
- C:\Documents and Settings\Administrator\Cookies\administrator@google[1].txt
- C:\Documents and Settings\Administrator\Cookies\administrator@java[1].txt
- C:\Documents and Settings\Administrator\Cookies\administrator@promotion.adobe[1].txt
- C:\Documents and Settings\Administrator\Cookies\administrator@sun[1].txt
- C:\Documents and Settings\Administrator\Cookies\administrator@walkernews[1].txt
- C:\Documents and Settings\Administrator\Local Settings\History\History.IE5\MSHist012011021720110218\index.dat
- C:\Documents and Settings\Administrator\Local Settings\History\History.IE5\MSHist012011021820110219\index.dat
- C:\Documents and Settings\Administrator\Local Settings\History\History.IE5\desktop.ini

Files Deleted:
C:\Documents and Settings\Administrator\Local Settings\History\desktop.ini
C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\4X23OP2B\desktop.ini
C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\GPURSX23\desktop.ini
C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\ODM3O1U3\desktop.ini
C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\WDUF49AN\[1]
C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\WDUF49AN\[2]
C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\WDUF49AN\desktop.ini
C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\desktop.ini
C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\desktop.ini

Files Read:
PIPE\lsarpc

Files Modified:
PIPE\lsarpc

File System Control Communication:

File	Control Code	Times
PIPE\lsarpc	0x0011C017	4

Memory Mapped Files:

File Name
C:\WINDOWS\system32\PSAPI.DLL
C:\WINDOWS\system32\dfrgnet.dll

3.b) Explorer.EXE - Other Activities

Mutexes Created:
{571F48A6-C7CD-C6C8-3A87-0EAB7C517015}

Keyboard Keys Monitored:

Virtual Key Code	Times
VK_LBUTTON (1)	80

4. cmd.exe

General information about this executable

Analysis Reason:	Started by file.exe
Filename:	cmd.exe
MD5:	6d778e0f95447e6546553eeea709d03c
SHA-1:	811a005cf787c6ccbe0d9f1c36c1d49a9cb71fd1
File Size:	389120
Command Line:	cmd /c ""C:\439687.bat" "C:\file.exe""
Process-status at analysis end:	dead
Exit Code:	1

Load-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\ntdll.dll	0x7C900000	0x000AF000
C:\WINDOWS\system32\kernel32.dll	0x7C800000	0x000F6000
C:\WINDOWS\system32\msvcrt.dll	0x77C10000	0x00058000
C:\WINDOWS\system32\USER32.dll	0x7E410000	0x00091000
C:\WINDOWS\system32\GDI32.dll	0x77F10000	0x00049000

Run-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\dfrgnet.dll	0x10000000	0x00011000
C:\WINDOWS\system32\PSAPI.DLL	0x76BF0000	0x0000B000
C:\WINDOWS\system32\Apphelp.dll	0x77B40000	0x00022000
C:\WINDOWS\system32\VERSION.dll	0x77C00000	0x00008000
C:\WINDOWS\system32\ADVAPI32.dll	0x77DD0000	0x0009B000
C:\WINDOWS\system32\RPCRT4.dll	0x77E70000	0x00092000
C:\WINDOWS\system32\Secur32.dll	0x77FE0000	0x00011000

4.a) cmd.exe - Registry Activities

Registry Values Read:

Key	Name	Value	Times
HKLM\SYSTEM\WPA\MediaCenter	Installed	0	1
HKLM\Software\Microsoft\Command Processor	AutoRun		1
HKLM\Software\Microsoft\Command Processor	CompletionChar	64	1
HKLM\Software\Microsoft\Command Processor	DefaultColor	0	1
HKLM\Software\Microsoft\Command Processor	EnableExtensions	1	1
HKLM\Software\Microsoft\Command Processor	PathCompletionChar	64	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	AuthenticodeEnabled	0	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	DefaultLevel	262144	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	PolicyScope	0	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	TransparentEnabled	1	2
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{349d35ab-37b5-462f-9b89-edd5fbde1328}	HashAlg	32771	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{349d35ab-37b5-462f-9b89-edd5fbde1328}	ItemData	0x5eab304f957a49896a006c1c31154015	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{349d35ab-37b5-462f-9b89-edd5fbde1328}	ItemSize	779	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{349d35ab-37b5-462f-9b89-edd5fbde1328}	SaferFlags	0	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{7fb9cd2e-3076-4df9-a57b-b813f72dbb91}	HashAlg	32771	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{7fb9cd2e-3076-4df9-a57b-b813f72dbb91}	ItemData	0x67b0d48b343a3fd3bce9dc646704f394	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{7fb9cd2e-3076-4df9-a57b-b813f72dbb91}	ItemSize	517	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{7fb9cd2e-3076-4df9-a57b-b813f72dbb91}	SaferFlags	0	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f}	HashAlg	32771	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f}	ItemData	0x327802dcfef8c893dc8ab006dd847d1d	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f}	ItemSize	918	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f}	SaferFlags	0	1

Registry Values Read:

Key	Name	Value	Times
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}	HashAlg	32771	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}	ItemData	0xbd9a2adb42ebd8560e250e4df8162f67	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}	ItemSize	229	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}	SaferFlags	0	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{dc971ee5-44eb-4fe4-ae2e-b91490411bfc}	HashAlg	32771	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{dc971ee5-44eb-4fe4-ae2e-b91490411bfc}	ItemData	0x386b085f84ecf669d36b956a22c01e80	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{dc971ee5-44eb-4fe4-ae2e-b91490411bfc}	ItemSize	370	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{dc971ee5-44eb-4fe4-ae2e-b91490411bfc}	SaferFlags	0	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Paths\{dda3f824-d8cb-441b-834d-be2efd2c1a33}	ItemData	%HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cache%OLK*	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Paths\{dda3f824-d8cb-441b-834d-be2efd2c1a33}	SaferFlags	0	1
HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName	ComputerName	PC	1
HKLM\System\CurrentControlSet\Control\Nls\Language Groups	1	1	1
HKLM\System\CurrentControlSet\Control\Nls\Locale	00000C07	1	1
HKLM\System\CurrentControlSet\Control\Session Manager\AppCertDlls	mqtgstat	C:\WINDOWS\system32\dfrgnet.dll	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Command Processor	CompletionChar	9	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Command Processor	DefaultColor	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Command Processor	EnableExtensions	1	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	Cache	C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files	1

4.b) cmd.exe - File Activities

Files Deleted:

C:\439687.bat

C:\file.exe

Files Read:

C:\439687.bat

PIPE\lsarpc

Files Modified:

PIPE\lsarpc

File System Control Communication:

File	Control Code	Times
C:\Program Files\Common Files	0x00090028	1
PIPE\lsarpc	0x0011C017	4

Memory Mapped Files:

File Name
C:\439687.bat
C:\WINDOWS\system32\Apphelp.dll
C:\WINDOWS\system32\PSAPI.DLL
C:\WINDOWS\system32\attrib.exe
C:\WINDOWS\system32\dfrgnet.dll
C:\Windows\AppPatch\sysmain.sdb

4.c) cmd.exe - Process Activities

Processes Created:

Executable	Command Line
C:\WINDOWS\system32\attrib.exe	
C:\WINDOWS\system32\attrib.exe	attrib -r -s -h"C:\file.exe"

Remote Threads Created:

Affected Process
C:\WINDOWS\system32\attrib.exe

Foreign Memory Regions Read:

Process: C:\WINDOWS\system32\attrib.exe

Foreign Memory Regions Written:

Process: C:\WINDOWS\system32\attrib.exe

5. attrib.exe

General information about this executable

Analysis Reason:	Started by cmd.exe
Filename:	attrib.exe
MD5:	e6d680494c812b82a15600fd23c94424
SHA-1:	6be7cccf384b1b05b08b7fc5ae5bc3bb3365cc55
File Size:	12288
Command Line:	attrib -r -s -h"C:\file.exe"
Process-status at analysis end:	dead
Exit Code:	0

Load-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\ntdll.dll	0x7C900000	0x000AF000
C:\WINDOWS\system32\kernel32.dll	0x7C800000	0x000F6000
C:\WINDOWS\system32\ulib.dll	0x71FA0000	0x00045000
C:\WINDOWS\system32\msvcrt.dll	0x77C10000	0x00058000
C:\WINDOWS\system32\USER32.dll	0x7E410000	0x00091000
C:\WINDOWS\system32\GDI32.dll	0x77F10000	0x00049000
C:\WINDOWS\system32\ADVAPI32.dll	0x77DD0000	0x0009B000
C:\WINDOWS\system32\RPCRT4.dll	0x77E70000	0x00092000
C:\WINDOWS\system32\Secur32.dll	0x77FE0000	0x00011000
C:\WINDOWS\system32\ShimEng.dll	0x5CB70000	0x00026000

Load-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\AppPatch\AcGenral.DLL	0x6F880000	0x001CA000
C:\WINDOWS\system32\WINMM.dll	0x76B40000	0x0002D000
C:\WINDOWS\system32\ole32.dll	0x774E0000	0x0013D000
C:\WINDOWS\system32\OLEAUT32.dll	0x77120000	0x0008B000
C:\WINDOWS\system32\MSACM32.dll	0x77BE0000	0x00015000
C:\WINDOWS\system32\VERSION.dll	0x77C00000	0x00008000
C:\WINDOWS\system32\SHELL32.dll	0x7C9C0000	0x00817000
C:\WINDOWS\system32\SHLWAPI.dll	0x77F60000	0x00076000
C:\WINDOWS\system32\USERENV.dll	0x769C0000	0x000B4000
C:\WINDOWS\system32\UxTheme.dll	0x5AD70000	0x00038000
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll	0x773D0000	0x00103000
C:\WINDOWS\system32\comctl32.dll	0x5D090000	0x0009A000

5.a) attrib.exe - Registry Activities

Registry Values Read:

Key	Name	Value	Times
HKLM\SYSTEM\CurrentControlSet\Control\Session Manager	CriticalSectionTimeout	2592000	1
HKLM\SYSTEM\Setup	SystemSetupInProgres	0	1
HKLM\SYSTEM\WPA\MediaCenter	Installed	0	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.iac2	aFormatTagCache	0x010000001000000002040000014000000	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.iac2	cFilterTags	0	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.iac2	cFormatTags	2	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.iac2	fdwSupport	1	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.imaadpcm	aFormatTagCache	0x010000001000000011000000014000000	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.imaadpcm	cFilterTags	0	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.imaadpcm	cFormatTags	2	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.imaadpcm	fdwSupport	1	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.l3acm	aFormatTagCache	0x010000001000000005500000001e000000	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.l3acm	cFilterTags	0	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.l3acm	cFormatTags	2	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.l3acm	fdwSupport	1	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msadpcm	aFormatTagCache	0x010000001000000002000000032000000	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msadpcm	cFilterTags	0	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msadpcm	cFormatTags	2	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msadpcm	fdwSupport	1	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msaudio1	aFormatTagCache	0x010000001200000060010000160000006610100001c000000	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msaudio1	cFilterTags	0	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msaudio1	cFormatTags	3	1

Registry Values Read:

Key	Name	Value	Times
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msaudio1	fdwSupport	1	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msg711	aFormatTagCache	0x0100000010000000060000001200000000700000012000000	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msg711	cFilterTags	0	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msg711	cFormatTags	3	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msg711	fdwSupport	1	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msg723	aFormatTagCache	0x010000001000000042000000 1c000000	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msg723	cFilterTags	0	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msg723	cFormatTags	2	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msg723	fdwSupport	1	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msgsm610	aFormatTagCache	0x0100000010000000310000001400000 0	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msgsm610	cFilterTags	0	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msgsm610	cFormatTags	2	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msgsm610	fdwSupport	1	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.sl_anet	aFormatTagCache	0x0100000010000000300100001600000 0	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.sl_anet	cFilterTags	0	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.sl_anet	cFormatTags	2	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.sl_anet	fdwSupport	1	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.trspch	aFormatTagCache	0x0100000010000000220000003200000 0	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.trspch	cFilterTags	0	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.trspch	cFormatTags	2	1
HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.trspch	fdwSupport	1	1
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	midimapper		2
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	msacm.iac2	C:\WINDOWS\system32\iac25_32.ax	2
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	msacm.imaadpcm	imaadp32.acm	3
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	msacm.l3acm		2
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	msacm.msadpcm		3
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	msacm.msaudio1		3
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	msacm.msg711		3
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	msacm.msg723	msg723.acm	3
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	msacm.msgsm610		3
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	msacm.sl_anet		2
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	msacm.trspch		3

Registry Values Read:

Key	Name	Value	Times
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	vidc.I420		2
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	vidc.M261		2
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	vidc.M263		2
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	vidc.cvid		2
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	vidc.iv31		2
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	vidc.iv32		2
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	vidc.iv41		2
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	vidc.iv50		1
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	vidc.iyuv		2
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	vidc.mrle		2
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	vidc.msvc		2
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	vidc.uyvy		2
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	vidc.yuy2		2
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	vidc.yvu9		2
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	vidc.yvyu		2
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32	wavemapper		2
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	TransparentEnabled	1	1
HKLM\System\CurrentControlSet\Control\MediaProperties\PrivateProperties\Joystick\Winmm	wheel	1	1
HKLM\System\CurrentControlSet\Control\Nls\Language Groups	1	1	1
HKLM\System\CurrentControlSet\Control\Nls\Locale	00000C07	1	1
HKLM\System\CurrentControlSet\Control\ProductOptions	ProductType	WinNT	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Multimedia\Audio	SystemFormats	CD Quality,Radio Quality,Telephone Quality	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	Local Settings	%USERPROFILE%\Local Settings	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	Personal	%USERPROFILE%\My Documents	1

5.b) attrib.exe - File Activities

File System Control Communication:

File	Control Code	Times
C:\Program Files\Common Files	0x00090028	1

Device Control Communication:

File	Control Code	Times
\Device\KsecDD	0x00390008	1

Memory Mapped Files:

File Name
C:\WINDOWS\AppPatch\AcGenral.DLL
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
C:\WINDOWS\WindowsShell.Manifest
C:\WINDOWS\system32\MSACM32.dll
C:\WINDOWS\system32\SHELL32.dll
C:\WINDOWS\system32\ShimEng.dll
C:\WINDOWS\system32\UxTheme.dll
C:\WINDOWS\system32\WINMM.dll
C:\WINDOWS\system32\comctl32.dll
C:\WINDOWS\system32\ulib.dll
C:\Windows\AppPatch\sysmain.sdb