



# Anubis - Analysis Report



## Analysis Report for zeusbin\_c83014c71b71747d5ab628011e2cc91e.exe

MD5: c83014c71b71747d5ab628011e2cc91e

### Summary:

Description	Risk
<b>Autostart capabilities:</b> This executable registers processes to be executed at system start. This could result in unwanted actions to be performed automatically.	● medium
<b>Changes security settings of Internet Explorer:</b> This system alteration could seriously affect safety surfing the World Wide Web.	● medium
<b>Creates files in the Windows system directory:</b> Malware often keeps copies of itself in the Windows directory to stay undetected by users.	● medium
<b>Performs File Modification and Destruction:</b> The executable modifies and destructs files which are not temporary.	● high
<b>Performs Registry Activities:</b> The executable reads and modifies register values. It also creates and monitors register keys.	● low

## Dependency overview:

 **zeusbin\_c83014c71b71747d5ab628011e2cc91e.exe** C:\zeusbin\_c83014c71b71747d5ab628011e2cc91e.exe

Analysis reason: Primary Analysis Subject

 **winlogon.exe** \\?\C:\WINDOWS\system32\winlogon.exe

Analysis reason: zeusbin\_c83014c71b71747d5ab628011e2cc91e.exe wrote to the virtual memory of this process

 **svchost.exe** C:\WINDOWS\system32\svchost.exe

Analysis reason: winlogon.exe wrote to the virtual memory of this process

 **System** System

Analysis reason: svchost.exe wrote to the virtual memory of this process

 **services.exe** C:\WINDOWS\system32\services.exe

Analysis reason: svchost.exe wrote to the virtual memory of this process

 **lsass.exe** C:\WINDOWS\system32\lsass.exe

Analysis reason: svchost.exe wrote to the virtual memory of this process

 **svchost.exe** C:\WINDOWS\system32\svchost.exe

Analysis reason: svchost.exe wrote to the virtual memory of this process

 **svchost.exe** C:\WINDOWS\System32\svchost.exe

Analysis reason: svchost.exe wrote to the virtual memory of this process

 **svchost.exe** C:\WINDOWS\system32\svchost.exe

Analysis reason: svchost.exe wrote to the virtual memory of this process

 **svchost.exe** C:\WINDOWS\system32\svchost.exe

Analysis reason: svchost.exe wrote to the virtual memory of this process

 **spoolsv.exe** C:\WINDOWS\system32\spoolsv.exe

Analysis reason: svchost.exe wrote to the virtual memory of this process

## **Table of Contents:**

1. General Information.....	4
2. zeusbin_c83014c71b71747d5ab628011e2cc91e.exe.....	4
a) Registry Activities.....	4
b) File Activities.....	5
c) Process Activities.....	5
3. winlogon.exe.....	6
a) Registry Activities.....	7
b) File Activities.....	7
c) Process Activities.....	8
4. svchost.exe.....	8
a) Registry Activities.....	9
b) File Activities.....	12
c) Process Activities.....	14
d) Network Activities.....	14
5. System.....	14
6. services.exe.....	14
a) Registry Activities.....	15
b) File Activities.....	18
7. lsass.exe.....	18
a) Registry Activities.....	20
b) File Activities.....	20
8. svchost.exe.....	21
a) Registry Activities.....	22
b) File Activities.....	23
9. svchost.exe.....	24
a) Registry Activities.....	26
b) File Activities.....	30
10. svchost.exe.....	30
a) Registry Activities.....	31
b) File Activities.....	31
11. svchost.exe.....	32
a) Registry Activities.....	33
b) File Activities.....	33
12. spoolsv.exe.....	33
a) File Activities.....	35



## 1. General Information

### Information about Anubis' invocation

Time needed:	241 s
Report created:	03/08/10, 23:33:33 UTC
Termination reason:	Timeout
Program version:	1.74.2603

## 2. zeusbin\_c83014c71b71747d5ab628011e2cc91e.exe

### General information about this executable

Analysis Reason:	Primary Analysis Subject
Filename:	zeusbin_c83014c71b71747d5ab628011e2cc91e.exe
MD5:	c83014c71b71747d5ab628011e2cc91e
SHA-1:	f35e03cff860908331936bc591f24b0415055d6f
File Size:	134656
Command Line:	"C:\zeusbin_c83014c71b71747d5ab628011e2cc91e.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\ADVAPI32.dll	0x77DD0000	0x0009B000
C:\WINDOWS\system32\RPCRT4.dll	0x77E70000	0x00092000
C:\WINDOWS\system32\Secur32.dll	0x77FE0000	0x00011000
C:\WINDOWS\system32\SHLWAPI.dll	0x77F60000	0x00076000
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

### Run-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\WS2HELP.dll	0x71AA0000	0x00008000
C:\WINDOWS\system32\WS2_32.dll	0x71AB0000	0x00017000
C:\WINDOWS\system32\PSAPI.DLL	0x76BF0000	0x0000B000
C:\WINDOWS\system32\OLEAUT32.dll	0x77120000	0x0008B000
C:\WINDOWS\system32\WININET.dll	0x771B0000	0x000AA000
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll	0x773D0000	0x00103000
C:\WINDOWS\system32\CRYPT32.dll	0x77A80000	0x00095000
C:\WINDOWS\system32\MSASN1.dll	0x77B20000	0x00012000
C:\WINDOWS\system32\SHELL32.dll	0x7C9C0000	0x00817000

### Ikarus Virus Scanner

Packed.Win32.Krap (Sig-Id:38174524)

## 2.a) zeusbin\_c83014c71b71747d5ab628011e2cc91e.exe - Registry Activities

### Registry Values Modified:

Key	Name	New Value
HKLM\software\microsoft\windows nt\currentversion\winlogon	userinit	C:\WINDOWS\system32\userinit.exe,C:\WINDOWS\system32\sdra64.exe,



Registry Values Read:

Key	Name	Value	Times
HKLM\SYSTEM\CurrentControlSet\Control\Session Manager	CriticalSectionTimeout	2592000	1
HKLM\SYSTEM\Setup	SystemSetupInProgress	0	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodelIdentifiers	TransparentEnabled	1	1
HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName	ComputerName	PC	1
HKLM\software\microsoft\windows nt\currentversion\winlogon	userinit	C:\WINDOWS\system32\userinit.exe,	2

**2.b) zeusbin\_c83014c71b71747d5ab628011e2cc91e.exe - File Activities**

Files Created:

C:\WINDOWS\system32\sdra64.exe

Files Read:

C:\WINDOWS\win.ini  
PIPE\lsarpc

Files Modified:

C:\WINDOWS\system32\sdra64.exe  
PIPE\lsarpc

File System Control Communication:

File	Control Code	Times
PIPE\lsarpc	0x0011C017	10

Device Control Communication:

File	Control Code	Times
\Device\KsecDD	0x00390008	1

Memory Mapped Files:

File Name
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\PSAPI.DLL
C:\WINDOWS\system32\SHELL32.dll
C:\WINDOWS\system32\WININET.dll
C:\WINDOWS\system32\WS2HELP.dll
C:\WINDOWS\system32\WS2_32.dll
C:\zeusbin_c83014c71b71747d5ab628011e2cc91e.exe

**2.c) zeusbin\_c83014c71b71747d5ab628011e2cc91e.exe - Process Activities**

Remote Threads Created:

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

Foreign Memory Regions Read:

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

Foreign Memory Regions Written:

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



### 3. winlogon.exe

#### General information about this executable

Analysis Reason:	zeusbin_c83014c71b71747d5ab628011e2cc91e.exe wrote to the virtual memory of this process
Filename:	winlogon.exe
Command Line:	winlogon.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\AUTHZ.dll	0x776C0000	0x00012000
C:\WINDOWS\system32\msvcrt.dll	0x77C10000	0x00058000
C:\WINDOWS\system32\CRYPT32.dll	0x77A80000	0x00095000
C:\WINDOWS\system32\MSASN1.dll	0x77B20000	0x00012000
C:\WINDOWS\system32\USER32.dll	0x7E410000	0x00091000
C:\WINDOWS\system32\GDI32.dll	0x77F10000	0x00049000
C:\WINDOWS\system32\NDdeApi.dll	0x75940000	0x00008000
C:\WINDOWS\system32\PROFMAP.dll	0x75930000	0x0000A000
C:\WINDOWS\system32\NETAPI32.dll	0x5B860000	0x00055000
C:\WINDOWS\system32\USERENV.dll	0x769C0000	0x000B4000
C:\WINDOWS\system32\PSAPI.DLL	0x76BF0000	0x0000B000
C:\WINDOWS\system32\REGAPI.dll	0x76BC0000	0x0000F000
C:\WINDOWS\system32\SETUPAPI.dll	0x77920000	0x000F3000
C:\WINDOWS\system32\VERSION.dll	0x77C00000	0x00008000
C:\WINDOWS\system32\WINSTA.dll	0x76360000	0x00010000
C:\WINDOWS\system32\WINTRUST.dll	0x76C30000	0x0002E000
C:\WINDOWS\system32\IMAGEHELP.dll	0x76C90000	0x00028000
C:\WINDOWS\system32\WS2_32.dll	0x71AB0000	0x00017000
C:\WINDOWS\system32\WS2HELP.dll	0x71AA0000	0x00008000
C:\WINDOWS\system32\MSGINA.dll	0x75970000	0x000F8000
C:\WINDOWS\system32\COMCTL32.dll	0x5D090000	0x0009A000
C:\WINDOWS\system32\ODBC32.dll	0x74320000	0x0003D000
C:\WINDOWS\system32\comdlg32.dll	0x763B0000	0x00049000
C:\WINDOWS\system32\SHELL32.dll	0x7C9C0000	0x00817000
C:\WINDOWS\system32\SHLWAPI.dll	0x77F60000	0x00076000
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll	0x773D0000	0x00103000
C:\WINDOWS\system32\odbcint.dll	0x00930000	0x00017000
C:\WINDOWS\system32\SHSVCS.dll	0x776E0000	0x00023000
C:\WINDOWS\system32\sfc.dll	0x76BB0000	0x00005000
C:\WINDOWS\system32\sfc_os.dll	0x76C60000	0x0002A000
C:\WINDOWS\system32\ole32.dll	0x774E0000	0x0013D000
C:\WINDOWS\system32\Aphhelp.dll	0x77B40000	0x00022000
C:\WINDOWS\system32\WINSCARD.DLL	0x723D0000	0x0001C000
C:\WINDOWS\system32\WTSAPI32.dll	0x76F50000	0x00008000
C:\WINDOWS\system32\WINMM.dll	0x76B40000	0x0002D000
C:\WINDOWS\system32\uxtheme.dll	0x5AD70000	0x00038000
C:\WINDOWS\system32\cscdll.dll	0x76600000	0x0001D000
C:\WINDOWS\System32\dimsntfy.dll	0x47020000	0x00008000
C:\WINDOWS\system32\WNotify.dll	0x75950000	0x0001A000
C:\WINDOWS\system32\MPR.dll	0x71B20000	0x00012000



Load-time Dlls		
Module Name	Base Address	Size
C:\WINDOWS\system32\WINSPOOL.DRV	0x73000000	0x00026000
C:\WINDOWS\system32\rsaenh.dll	0x68000000	0x00036000
C:\WINDOWS\system32\SAMLIB.dll	0x71BF0000	0x00013000
C:\WINDOWS\system32\sxs.dll	0x7E720000	0x000B0000
C:\WINDOWS\system32\msv1_0.dll	0x77C70000	0x00024000
C:\WINDOWS\system32\iphlpapi.dll	0x76D60000	0x00019000
C:\WINDOWS\system32\wdap32.dll	0x76F60000	0x0002C000
C:\WINDOWS\system32\cscui.dll	0x77A20000	0x00054000
C:\WINDOWS\system32\xpsp2res.dll	0x016E0000	0x002C5000
C:\WINDOWS\system32\COMRes.dll	0x77050000	0x000C5000
C:\WINDOWS\system32\OLEAUT32.dll	0x77120000	0x0008B000
C:\WINDOWS\system32\CLBCATQ.DLL	0x76FD0000	0x0007F000
C:\WINDOWS\system32\NTMARTA.DLL	0x77690000	0x00021000

Run-time Dlls		
Module Name	Base Address	Size
C:\WINDOWS\system32\WININET.dll	0x771B0000	0x000AA000

### 3.a) winlogon.exe - Registry Activities

Registry Values Read:			
Key	Name	Value	Times
HKLM\software\microsoft\windows nt\currentversion\winlogon	userinit	C:\WINDOWS\system32\userinit.exe,C:\WINDOWS\system32\sdra64.exe,	362

### 3.b) winlogon.exe - File Activities

Files Created:
C:\WINDOWS\system32\lowsec
C:\WINDOWS\system32\lowsec\local.ds
C:\WINDOWS\system32\lowsec\user.ds
pipe\_AVIRA_2109

Files Read:
PIPE\sarpc
pipe\_AVIRA_2109

Files Modified:
PIPE\sarpc
pipe\_AVIRA_2109

Directories Created:
C:\WINDOWS\system32\lowsec

File System Control Communication:		
File	Control Code	Times
PIPE\sarpc	0x0011C017	38
pipe\_AVIRA_2109	0x00110004	5
pipe\_AVIRA_2109	0x00110008	4

Memory Mapped Files:
File Name
C:\WINDOWS\system32\WININET.dll



## Directories Monitored:

Directory	Watch subtree	Notify Filter	Count
C:\WINDOWS\system32	0	File Name Change,Directory Name Change,Name Change,Size Change,Last Write Change,Creation Change,Stream Size Change,Stream Write Change	3

**3.c) winlogon.exe - Process Activities**

## Remote Threads Created:

**Affected Process**

C:\WINDOWS\system32\svchost.exe

## Foreign Memory Regions Read:

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

## Foreign Memory Regions Written:

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

**4. svchost.exe**

## General information about this executable

Analysis Reason:	winlogon.exe wrote to the virtual memory of this process
Filename:	svchost.exe
Command Line:	C:\WINDOWS\system32\svchost -k DcomLaunch
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\ShimEng.dll	0x5CB70000	0x00026000
C:\WINDOWS\AppPatch\AcGeneral.DLL	0x6F880000	0x001CA000
C:\WINDOWS\system32\USER32.dll	0x7E410000	0x00091000
C:\WINDOWS\system32\GDI32.dll	0x77F10000	0x00049000
C:\WINDOWS\system32\WINMM.dll	0x76B40000	0x0002D000
C:\WINDOWS\system32\ole32.dll	0x774E0000	0x0013D000
C:\WINDOWS\system32\msvcrt.dll	0x77C10000	0x00058000
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
C:\WINDOWS\system32\NTMARTA.DLL	0x77690000	0x00021000
C:\WINDOWS\system32\SAMLIB.dll	0x71BF0000	0x00013000
C:\WINDOWS\system32\WLDAP32.dll	0x76F60000	0x0002C000
c:\windows\system32\rpcss.dll	0x76A80000	0x00064000
c:\windows\system32\WS2_32.dll	0x71AB0000	0x00017000



## Load-time Dlls

Module Name	Base Address	Size
c:\windows\system32\WS2HELP.dll	0x71AA0000	0x00008000
C:\WINDOWS\system32\xpsp2res.dll	0x005F0000	0x002C5000
c:\windows\system32\termsrv.dll	0x760F0000	0x00053000
c:\windows\system32\ICAAPI.dll	0x74F70000	0x00006000
c:\windows\system32\SETUPAPI.dll	0x77920000	0x000F3000
C:\WINDOWS\system32\WINTRUST.dll	0x76C30000	0x0002E000
C:\WINDOWS\system32\CRYPT32.dll	0x77A80000	0x00095000
C:\WINDOWS\system32\MSASN1.dll	0x77B20000	0x00012000
C:\WINDOWS\system32\IMAGEHLP.dll	0x76C90000	0x00028000
c:\windows\system32\AUTHZ.dll	0x776C0000	0x00012000
c:\windows\system32\mstlsapi.dll	0x75110000	0x0001F000
c:\windows\system32\ACTIVEDS.dll	0x77CC0000	0x00032000
c:\windows\system32\adslrpc.dll	0x76E10000	0x00025000
C:\WINDOWS\system32\NETAPI32.dll	0x5B860000	0x00055000
c:\windows\system32\ATL.DLL	0x76B20000	0x00011000
C:\WINDOWS\system32\REGAPI.dll	0x76BC0000	0x0000F000
C:\WINDOWS\system32\rsaenh.dll	0x68000000	0x00036000
C:\WINDOWS\system32\CLBCATQ.DLL	0x76FD0000	0x0007F000
C:\WINDOWS\system32\COMRes.dll	0x77050000	0x000C5000
C:\WINDOWS\system32\Apphelp.dll	0x77B40000	0x00022000

## Run-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\hnetcfg.dll	0x662B0000	0x00058000
C:\WINDOWS\system32\mswsock.dll	0x71A50000	0x0003F000
C:\WINDOWS\System32\wshtcpip.dll	0x71A90000	0x00008000
C:\WINDOWS\system32\wsock32.dll	0x71AD0000	0x00009000
C:\WINDOWS\system32\sensapi.dll	0x722B0000	0x00005000
C:\WINDOWS\system32\PSAPI.DLL	0x76BF0000	0x0000B000
C:\WINDOWS\system32\rtutils.dll	0x76E80000	0x0000E000
C:\WINDOWS\system32\rasman.dll	0x76E90000	0x00012000
C:\WINDOWS\system32\TAPI32.dll	0x76EB0000	0x0002F000
C:\WINDOWS\system32\RASAPI32.DLL	0x76EE0000	0x0003C000
C:\WINDOWS\system32\WININET.dll	0x771B0000	0x000AA000
C:\WINDOWS\system32\urlmon.dll	0x7E1E0000	0x000A2000

**4.a) svchost.exe - Registry Activities**

## Registry Keys Created:

HKU\S-1-5-18\software\microsoft\windows\currentversion\explorer\{43BF8CD1-C5D5-2230-7BB2-98F22C2B7DC6}

## Registry Values Modified:

Key	Name	New Value
HKLM\SYSTEM\CURRENTCONTROLSET\HARDWARE PROFILES \CURRENT\Software\Microsoft\windows\CurrentVersion\Internet Settings	ProxyEnable	0
HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ Cache\Paths	Directory	C:\WINDOWS\system32\config\systemprofile \Local Settings\Temporary Internet Files\ Content.IE5
HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ Cache\Paths	Paths	4
HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ Cache\Paths\Path1	CacheLimit	40852
HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ Cache\Paths\Path1	CachePath	C:\WINDOWS\system32\config\systemprofile \Local Settings\Temporary Internet Files\ Content.IE5\Cache1





## Registry Values Read:

Key	Name	Value	Times
HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile	EnableFirewall	0	1
HKLM\SYSTEM\CurrentControlSet\Services\Winsock\Parameters	Transports	0x5400630070006900700000004e00650077400420049004f005300000000000	2
HKLM\Software\Classes\CLSID\{304CE942-6E39-40D8-943A-B913C40C9CD4}\InprocServer32		C:\WINDOWS\system32\hnetcfg.dll	1
HKLM\Software\Classes\CLSID\{304CE942-6E39-40D8-943A-B913C40C9CD4}\InprocServer32	ThreadingModel	Both	1
HKLM\Software\Microsoft\COM3	Com+Enabled	1	2
HKLM\Software\Microsoft\COM3	REGDBVersion	0x0700000000000000	2
HKLM\Software\Microsoft\Cryptography	MachineGuid	4604e8cc-5b9c-4ffb-a374-a62e6d0494fc	40
HKLM\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_BEHAVIORS	*	1	2
HKLM\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_DISABLE_MK_PROTOCOL	*	1	2
HKLM\Software\Microsoft\Tracing	EnableConsoleTracing	0	1
HKLM\Software\Microsoft\Tracing\RASAPI32	ConsoleTracingMask	4294901760	2
HKLM\Software\Microsoft\Tracing\RASAPI32	EnableConsoleTracing	0	2
HKLM\Software\Microsoft\Tracing\RASAPI32	EnableFileTracing	0	2
HKLM\Software\Microsoft\Tracing\RASAPI32	FileDirectory	%windir%\tracing	4
HKLM\Software\Microsoft\Tracing\RASAPI32	FileTracingMask	4294901760	2
HKLM\Software\Microsoft\Tracing\RASAPI32	MaxFileSize	1048576	2
HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName	ComputerName	PC	1
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Winsock	HelperDllName	%SystemRoot%\System32\wshtcpip.dll	1
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Winsock	Mapping	0x0b00000003000000020000001000000006000000020000000100000000000	1
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Winsock	MaxSockaddrLength	16	1
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Winsock	MinSockaddrLength	16	1
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Winsock	UseDelayedAcceptance	0	1
HKLM\System\Setup	SystemSetupInProgress	0	2
HKU\S-1-5-18\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings	EnableNegotiate	1	1
HKU\S-1-5-18\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings	User Agent	Mozilla/4.0 (compatible; MSIE 6.0; Win32)	2
HKU\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	Cache	%USERPROFILE%\Local Settings\Temporary Internet Files	3
HKU\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	Cookies	%USERPROFILE%\Cookies	3
HKU\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	History	%USERPROFILE%\Local Settings\History	3
HKU\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache	Signature	Client UrlCache MMF Ver 5.2	2
HKU\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content	CacheLimit	163410	1
HKU\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content	CachePrefix		2
HKU\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content	PerUserItem	1	1
HKU\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies	CacheLimit	8192	1
HKU\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies	CachePrefix	Cookie:	2
HKU\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies	PerUserItem	1	1





**Files Created:**

C:\WINDOWS\system32\lowsec\local.ds  
pipe\\_AVIRA\_2108

**Files Read:**

PIPE\lsarpc  
pipe\\_AVIRA\_2108  
pipe\\_AVIRA\_2109

**Files Modified:**

C:\WINDOWS\system32\lowsec\local.ds  
PIPE\lsarpc  
\Device\Afd\Endpoint  
pipe\\_AVIRA\_2108  
pipe\\_AVIRA\_2109

**File System Control Communication:**

File	Control Code	Times
PIPE\lsarpc	0x0011C017	22
pipe\_AVIRA_2108	0x00110004	10
pipe\_AVIRA_2108	0x00110008	9

**Device Control Communication:**

File	Control Code	Times
\Device\Afd\Endpoint	AFD_GET_INFO (0x0001207B)	2
\Device\Afd\Endpoint	AFD_SET_CONTEXT (0x00012047)	7
\Device\Afd\Endpoint	AFD_BIND (0x00012003)	1
\Device\Afd\Endpoint	AFD_GET_TDI_HAND (0x00012037)	2
\Device\Afd\Endpoint	AFD_GET SOCK_NAI (0x0001202F)	1
\Device\Afd\Endpoint	AFD_CONNECT (0x00012007)	1
unnamed file	0x00120028	1
\Device\Afd\Endpoint	AFD_SEND (0x0001201F)	1
\Device\Afd\Endpoint	AFD_RECV (0x00012017)	15

**Memory Mapped Files:**

File Name
C:\WINDOWS\System32\wshtcpip.dll
C:\WINDOWS\system32\PSAPI.DLL
C:\WINDOWS\system32\RASAPI32.DLL
C:\WINDOWS\system32\TAPI32.dll
C:\WINDOWS\system32\WININET.dll
C:\WINDOWS\system32\hnetcfg.dll
C:\WINDOWS\system32\msock.dll
C:\WINDOWS\system32\rasman.dll
C:\WINDOWS\system32\rtutils.dll
C:\WINDOWS\system32\sensapi.dll
C:\WINDOWS\system32\urlmon.dll
C:\WINDOWS\system32\wsock32.dll
C:\WINDOWS\system32\config\systemprofile\Cookies\index.dat



## Memory Mapped Files:

## File Name

C:\WINDOWS\system32\config\systemprofile\Local Settings\History\History.IE5\index.dat  
 C:\WINDOWS\system32\config\systemprofile\Local Settings\Temporary Internet Files\Content.IE5\index.dat

**4.c) svchost.exe - Process Activities**

## Remote Threads Created:

## Affected Process

C:\WINDOWS\system32\services.exe  
 C:\WINDOWS\system32\lsass.exe  
 C:\WINDOWS\system32\svchost.exe  
 C:\WINDOWS\system32\svchost.exe  
 C:\WINDOWS\system32\svchost.exe  
 C:\WINDOWS\system32\svchost.exe  
 C:\WINDOWS\system32\spoolsv.exe

## Foreign Memory Regions Written:

Process:  
 Process: C:\WINDOWS\system32\lsass.exe  
 Process: C:\WINDOWS\system32\services.exe  
 Process: C:\WINDOWS\system32\spoolsv.exe  
 Process: C:\WINDOWS\system32\svchost.exe

**4.d) svchost.exe - Network Activity**

## HTTP Conversations:

From ANUBIS:1038 to 193.104.27.139:80 - [193.104.27.139]

Request: GET /cfg2-newnew2.bin

Response: 200 "OK"

**5. System**

## General information about this executable

Analysis Reason:	svchost.exe wrote to the virtual memory of this process
Filename:	System
Process-status at analysis end:	alive
Exit Code:	0

## Load-time DLLs

Module Name	Base Address	Size
C:\WINDOWS\system32\ntdll.dll	0x7C900000	0x000AF000

**6. services.exe**

## General information about this executable

Analysis Reason:	svchost.exe wrote to the virtual memory of this process
Filename:	services.exe
MD5:	0e776ed5f7cc9f94299e70461b7b8185
SHA-1:	cb5a33cec4c7b8ef4bd5dc8c241005b66b26cbbf
File Size:	108544
Command Line:	C:\WINDOWS\system32\services.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\msvcrt.dll	0x77C10000	0x00058000
C:\WINDOWS\system32\NCObjAPI.DLL	0x5F770000	0x0000C000
C:\WINDOWS\system32\MSVCP60.dll	0x76080000	0x00065000
C:\WINDOWS\system32\SCEserv.dll	0x7DBD0000	0x00051000
C:\WINDOWS\system32\AUTHZ.dll	0x776C0000	0x00012000
C:\WINDOWS\system32\USER32.dll	0x7E410000	0x00091000
C:\WINDOWS\system32\GDI32.dll	0x77F10000	0x00049000
C:\WINDOWS\system32\USERENV.dll	0x769C0000	0x000B4000
C:\WINDOWS\system32\umpnpmgr.dll	0x7DBA0000	0x00021000
C:\WINDOWS\system32\WINSTA.dll	0x76360000	0x00010000
C:\WINDOWS\system32\NETAPI32.dll	0x5B860000	0x00055000
C:\WINDOWS\system32\ShimEng.dll	0x5CB70000	0x00026000
C:\WINDOWS\AppPatch\AcAdProc.dll	0x47260000	0x0000F000
C:\WINDOWS\system32\Apphelp.dll	0x77B40000	0x00022000
C:\WINDOWS\system32\VERSION.dll	0x77C00000	0x00008000
C:\WINDOWS\system32\eventlog.dll	0x77B70000	0x00011000
C:\WINDOWS\system32\PSAPI.DLL	0x76BF0000	0x0000B000
C:\WINDOWS\system32\WS2_32.dll	0x71AB0000	0x00017000
C:\WINDOWS\system32\WS2HELP.dll	0x71AA0000	0x00008000
C:\WINDOWS\system32\wtsapi32.dll	0x76F50000	0x00008000

## Run-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\comctl32.dll	0x5D090000	0x0009A000
C:\WINDOWS\system32\pstorec.dll	0x5E0C0000	0x0000D000
C:\WINDOWS\system32\rsaenh.dll	0x68000000	0x00036000
C:\WINDOWS\system32\ATL.DLL	0x76B20000	0x00011000
C:\WINDOWS\system32\OLEAUT32.dll	0x77120000	0x0008B000
C:\WINDOWS\system32\WININET.dll	0x771B0000	0x000AA000
C:\WINDOWS\system32\ole32.dll	0x774E0000	0x0013D000
C:\WINDOWS\system32\CRYPT32.dll	0x77A80000	0x00095000
C:\WINDOWS\system32\MSASN1.dll	0x77B20000	0x00012000
C:\WINDOWS\system32\SHLWAPI.dll	0x77F60000	0x00076000
C:\WINDOWS\system32\SHELL32.dll	0x7C9C0000	0x00817000

## 6.a) services.exe - Registry Activities

## Registry Values Modified:

Key	Name	New Value
HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	Common AppData	C:\Documents and Settings\All Users\Application Data
HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths	Directory	C:\Documents and Settings\LocalService\Local Settings\Temporary Internet Files\Content.IE5
HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths	Paths	4
HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths\Path1	CacheLimit	40852
HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths\Path1	CachePath	C:\Documents and Settings\LocalService\Local Settings\Temporary Internet Files\Content.IE5\Cache1



## Registry Values Modified:

Key	Name	New Value
HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths\Path2	CacheLimit	40852
HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths\Path2	CachePath	C:\Documents and Settings\LocalService\Local Settings\Temporary Internet Files\Content.IE5\Cache2
HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths\Path3	CacheLimit	40852
HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths\Path3	CachePath	C:\Documents and Settings\LocalService\Local Settings\Temporary Internet Files\Content.IE5\Cache3
HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths\Path4	CacheLimit	40852
HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths\Path4	CachePath	C:\Documents and Settings\LocalService\Local Settings\Temporary Internet Files\Content.IE5\Cache4
HKU\S-1-5-18\Software\Microsoft\Windows NT\CurrentVersion\Winlogon	ParseAutoexec	1
HKU\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	AppData	C:\Documents and Settings\LocalService\Application Data
HKU\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	Cache	C:\Documents and Settings\LocalService\Local Settings\Temporary Internet Files
HKU\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	Cookies	C:\Documents and Settings\LocalService\Cookies
HKU\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	History	C:\Documents and Settings\LocalService\Local Settings\History

## Registry Values Read:

Key	Name	Value	Times
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
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	SystemSetupInProgress	0	1
HKLM\Software\Microsoft\Cryptography	MachineGuid	4604e8cc-5b9c-4ffb-a374-a62e6d0494fc	4
HKLM\Software\Microsoft\Cryptography\OID\EncodingType 0\CertDllOpenStoreProv\#16	Dll	cryptnet.dll	1
HKLM\Software\Microsoft\Cryptography\OID\EncodingType 0\CertDllOpenStoreProv\#16	FuncName	LdapProvOpenStore	1
HKLM\Software\Microsoft\Cryptography\OID\EncodingType 0\CertDllOpenStoreProv\Ldap	Dll	cryptnet.dll	1
HKLM\Software\Microsoft\Cryptography\OID\EncodingType 0\CertDllOpenStoreProv\Ldap	FuncName	LdapProvOpenStore	1
HKLM\Software\Microsoft\Windows NT\CurrentVersion\ProfileList	AllUsersProfile	All Users	1
HKLM\Software\Microsoft\Windows NT\CurrentVersion\ProfileList	DefaultUserProfile	Default User	1
HKLM\Software\Microsoft\Windows NT\CurrentVersion\ProfileList	ProfilesDirectory	%SystemDrive%\Documents and Settings	2
HKLM\Software\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-18	ProfileImagePath	%systemroot%\system32\config\systemprofile	1
HKLM\Software\Microsoft\Windows\CurrentVersion	CommonFilesDir	C:\Program Files\Common Files	1
HKLM\Software\Microsoft\Windows\CurrentVersion	ProgramFilesDir	C:\Program Files	2
HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	Common AppData	%ALLUSERSPROFILE%\Application Data	1
HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName	ComputerName	PC	1
HKLM\System\CurrentControlSet\Control\Session Manager\Environment	ComSpec	%SystemRoot%\system32\cmd.exe	2



## Registry Values Read:

Key	Name	Value	Times
HKLM\System\CurrentControlSet\Control\Session Manager\Environment	FP_NO_HOST_CHECK	NO	2
HKLM\System\CurrentControlSet\Control\Session Manager\Environment	NUMBER_OF_PROCESSORS	1	2
HKLM\System\CurrentControlSet\Control\Session Manager\Environment	OS	Windows_NT	2
HKLM\System\CurrentControlSet\Control\Session Manager\Environment	PATHEXT	.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH	2
HKLM\System\CurrentControlSet\Control\Session Manager\Environment	PROCESSOR_ARCHITECTURE	x86	2
HKLM\System\CurrentControlSet\Control\Session Manager\Environment	PROCESSOR_IDENTIFIER	x86 Family 6 Model 3 Stepping 3, GenuineIntel	2
HKLM\System\CurrentControlSet\Control\Session Manager\Environment	PROCESSOR_LEVEL	6	2
HKLM\System\CurrentControlSet\Control\Session Manager\Environment	PROCESSOR_REVISION	0303	2
HKLM\System\CurrentControlSet\Control\Session Manager\Environment	Path	%SystemRoot%\system32;%SystemRoot%;%SystemRoot%\System32\Wbem	2
HKLM\System\CurrentControlSet\Control\Session Manager\Environment	TEMP	%SystemRoot%\TEMP	2
HKLM\System\CurrentControlSet\Control\Session Manager\Environment	TMP	%SystemRoot%\TEMP	2
HKLM\System\CurrentControlSet\Control\Session Manager\Environment	windir	%SystemRoot%	2
HKLM\System\CurrentControlSet\Services\ProtectedStorage	DependOnService	0x5200700063005300730000000000	2
HKLM\System\CurrentControlSet\Services\ProtectedStorage	DisplayName	Protected Storage	2
HKLM\System\CurrentControlSet\Services\ProtectedStorage	ErrorControl	1	2
HKLM\System\CurrentControlSet\Services\ProtectedStorage	ImagePath	%SystemRoot%\system32\sass.exe	2
HKLM\System\CurrentControlSet\Services\ProtectedStorage	ObjectName	LocalSystem	2
HKLM\System\CurrentControlSet\Services\ProtectedStorage	Start	2	2
HKLM\System\CurrentControlSet\Services\ProtectedStorage	Type	288	2
HKLM\System\Setup	SystemSetupInProgress	0	1
HKLM\software\microsoft\windows nt\currentversion\network	UID	pc5_7875768F3D3DB1CC	1
HKU\S-1-5-18\Environment	TEMP	%USERPROFILE%\Local Settings\Temp	2
HKU\S-1-5-18\Environment	TMP	%USERPROFILE%\Local Settings\Temp	2
HKU\S-1-5-18\Software\Microsoft\Windows NT\CurrentVersion\Winlogon	ParseAutoexec	1	1
HKU\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	AppData	%USERPROFILE%\Application Data	2
HKU\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	Cache	%USERPROFILE%\Local Settings\Temporary Internet Files	3
HKU\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	Cookies	%USERPROFILE%\Cookies	3
HKU\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	History	%USERPROFILE%\Local Settings\History	3
HKU\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache	Signature	Client UrlCache MMF Ver 5.2	2
HKU\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content	CacheLimit	163410	1
HKU\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content	CachePrefix		2
HKU\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content	PerUserItem	1	1
HKU\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies	CacheLimit	8192	1



## Registry Values Read:

Key	Name	Value	Times
HKU\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies	CachePrefix	Cookie:	2
HKU\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies	PerUserItem	1	1
HKU\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\ExtensibleCache\MSHist012008060220080603	CacheLimit	8192	1
HKU\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\ExtensibleCache\MSHist012008060220080603	CacheOptions	11	1
HKU\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\ExtensibleCache\MSHist012008060220080603	CachePath	%USERPROFILE%\Local Settings\History\History.IE5\MSHist012008060220080603\	2
HKU\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\ExtensibleCache\MSHist012008060220080603	CachePrefix	:2008060220080603:	2
HKU\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\ExtensibleCache\MSHist012008060220080603	CacheRepair	0	1
HKU\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History	CacheLimit	8192	1
HKU\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History	CachePrefix	Visited:	2
HKU\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History	PerUserItem	1	1

**6.b) services.exe - File Activities**

## Files Read:

C:\WINDOWS\system32\rsaenh.dll  
 PIPE\lsarpc  
 c:\autoexec.bat  
 pipe\\_AVIRA\_2108  
 pipe\\_AVIRA\_2109

## Files Modified:

C:\WINDOWS\system32\lowsec\user.ds  
 PIPE\lsarpc  
 pipe\\_AVIRA\_2108  
 pipe\\_AVIRA\_2109

## File System Control Communication:

File	Control Code	Times
PIPE\lsarpc	0x0011C017	14
\DosDevices\pipe\	0x00110018	5

## Memory Mapped Files:

File Name
C:\WINDOWS\system32\ATL.DLL
C:\WINDOWS\system32\SHELL32.dll
C:\WINDOWS\system32\WININET.dll
C:\WINDOWS\system32\comctl32.dll
C:\WINDOWS\system32\pstorec.dll
C:\WINDOWS\system32\rpcss.dll
C:\WINDOWS\system32\rsaenh.dll

**7. lsass.exe**



## General information about this executable

Analysis Reason:	svchost.exe wrote to the virtual memory of this process
Filename:	lsass.exe
MD5:	bf2466b3e18e970d8a976fb95fc1ca85
SHA-1:	de5a73cbb5f51f64c53fb4277ef2c23e70db123f
File Size:	13312
Command Line:	C:\WINDOWS\system32\lsass.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\LSASRV.dll	0x75730000	0x000B5000
C:\WINDOWS\system32\MPR.dll	0x71B20000	0x00012000
C:\WINDOWS\system32\USER32.dll	0x7E410000	0x00091000
C:\WINDOWS\system32\GDI32.dll	0x77F10000	0x00049000
C:\WINDOWS\system32\MSASN1.dll	0x77B20000	0x00012000
C:\WINDOWS\system32\msvcrt.dll	0x77C10000	0x00058000
C:\WINDOWS\system32\NETAPI32.dll	0x5B860000	0x00055000
C:\WINDOWS\system32\NTDSAPI.dll	0x767A0000	0x00013000
C:\WINDOWS\system32\DNSAPI.dll	0x76F20000	0x00027000
C:\WINDOWS\system32\WS2_32.dll	0x71AB0000	0x00017000
C:\WINDOWS\system32\WS2HELP.dll	0x71AA0000	0x00008000
C:\WINDOWS\system32\WLDAP32.dll	0x76F60000	0x0002C000
C:\WINDOWS\system32\SAMLIB.dll	0x71BF0000	0x00013000
C:\WINDOWS\system32\SAMSRV.dll	0x74440000	0x0006A000
C:\WINDOWS\system32\cryptdll.dll	0x76790000	0x0000C000
C:\WINDOWS\system32\ShimEng.dll	0x5CB70000	0x00026000
C:\WINDOWS\AppPatch\AcGeneral.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
C:\WINDOWS\system32\msprivs.dll	0x4D200000	0x0000E000
C:\WINDOWS\system32\kerberos.dll	0x71CF0000	0x0004C000
C:\WINDOWS\system32\msv1_0.dll	0x77C70000	0x00024000
C:\WINDOWS\system32\iphlpapi.dll	0x76D60000	0x00019000
C:\WINDOWS\system32\netlogon.dll	0x744B0000	0x00065000
C:\WINDOWS\system32\w32time.dll	0x767C0000	0x0002C000
C:\WINDOWS\system32\MSVCP60.dll	0x76080000	0x00065000
C:\WINDOWS\system32\schannel.dll	0x767F0000	0x00027000
C:\WINDOWS\system32\CRYPT32.dll	0x77A80000	0x00095000
C:\WINDOWS\system32\wdigest.dll	0x74380000	0x0000F000
C:\WINDOWS\system32\rsaenh.dll	0x68000000	0x00036000
C:\WINDOWS\system32\setupapi.dll	0x77920000	0x000F3000



## Load-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\scecli.dll	0x74410000	0x0002F000
C:\WINDOWS\system32\ipsecsvc.dll	0x743E0000	0x0002F000
C:\WINDOWS\system32\AUTHZ.dll	0x776C0000	0x00012000
C:\WINDOWS\system32\oakley.DLL	0x75D90000	0x000D0000
C:\WINDOWS\system32\WINIPSEC.DLL	0x74370000	0x0000B000
C:\WINDOWS\system32\mswsock.dll	0x71A50000	0x0003F000
C:\WINDOWS\system32\hnetcfg.dll	0x662B0000	0x00058000
C:\WINDOWS\System32\wshtcpip.dll	0x71A90000	0x00008000
C:\WINDOWS\system32\dssenh.dll	0x68100000	0x00026000
C:\WINDOWS\system32\pstersvc.dll	0x743A0000	0x0000B000
C:\WINDOWS\system32\psbase.dll	0x743C0000	0x0001B000

## Run-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\PSAPI.DLL	0x76BF0000	0x0000B000
C:\WINDOWS\system32\WININET.dll	0x771B0000	0x000AA000

**7.a) Isass.exe - Registry Activities**

## Registry Keys Created:

HKU\S-1-5-18\SOFTWARE\Microsoft\Protected Storage System Provider
HKU\S-1-5-18\SOFTWARE\Microsoft\Protected Storage System Provider\S-1-5-18
HKU\S-1-5-18\SOFTWARE\Microsoft\Protected Storage System Provider\S-1-5-18\Data 2
HKU\S-1-5-18\SOFTWARE\Microsoft\Protected Storage System Provider\S-1-5-18\Data 2\Windows
HKU\S-1-5-20\SOFTWARE\Microsoft\Protected Storage System Provider
HKU\S-1-5-20\SOFTWARE\Microsoft\Protected Storage System Provider\S-1-5-20
HKU\S-1-5-20\SOFTWARE\Microsoft\Protected Storage System Provider\S-1-5-20\Data 2
HKU\S-1-5-20\SOFTWARE\Microsoft\Protected Storage System Provider\S-1-5-20\Data 2\Windows

## Registry Values Modified:

Key	Name	New Value
HKU\S-1-5-18\SOFTWARE\Microsoft\Protected Storage System Provider\S-1-5-18	Migrate	2
HKU\S-1-5-18\SOFTWARE\Microsoft\Protected Storage System Provider\S-1-5-18\Data 2\Windows	Value	0x010000001c00000003000000ec10f305eef5fa8ea05a9d9baaf6eeaa6a1a53
HKU\S-1-5-20\SOFTWARE\Microsoft\Protected Storage System Provider\S-1-5-20	Migrate	2
HKU\S-1-5-20\SOFTWARE\Microsoft\Protected Storage System Provider\S-1-5-20\Data 2\Windows	Value	0x010000001c00000003000000ce4717d177817d025f6abea31f47ac1d6fc8f

## Registry Values Read:

Key	Name	Value	Times
HKLM\SECURITY\Policy\SecDesc		0x0100048098000000a8000000000000011400000002008400060000000100	20
HKLM\software\microsoft\windows nt\currentversion\network	UID	pc5_7875768F3D3DB1CC	1

**7.b) Isass.exe - File Activities**

## Files Created:

PIPE\lsass
------------

## Files Read:

C:\lsass, Flags: Named pipe
PIPE\lsarpc



## Files Read:

PIPE\lsass

## Files Modified:

C:\lsass, Flags: Named pipe

PIPE\lsarpc

PIPE\lsass

## File System Control Communication:

File	Control Code	Times
PIPE\lsass	0x00110008	6
C:\lsass, Flags: Named pipe	0x00110024	11
PIPE\lsarpc	0x0011C017	7
C:\lsass, Flags: Named pipe	0x0011001C	43
PIPE\lsass	0x00110024	15
PIPE\lsass	0x0011001C	45

## Memory Mapped Files:

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

## 8. svchost.exe

## General information about this executable

Analysis Reason:	svchost.exe wrote to the virtual memory of this process
Filename:	svchost.exe
Command Line:	C:\WINDOWS\system32\svchost -k rpcss
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\ShimEng.dll	0x5CB70000	0x00026000
C:\WINDOWS\AppPatch\AcGeneral.DLL	0x6F880000	0x001CA000
C:\WINDOWS\system32\USER32.dll	0x7E410000	0x00091000
C:\WINDOWS\system32\GDI32.dll	0x77F10000	0x00049000
C:\WINDOWS\system32\WINMM.dll	0x76B40000	0x0002D000
C:\WINDOWS\system32\ole32.dll	0x774E0000	0x0013D000
C:\WINDOWS\system32\msvcrt.dll	0x77C10000	0x00058000
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
c:\windows\system32\rpcss.dll	0x76A80000	0x00064000



## Load-time Dlls

Module Name	Base Address	Size
c:\windows\system32\WS2_32.dll	0x71AB0000	0x00017000
c:\windows\system32\WS2HELP.dll	0x71AA0000	0x00008000
C:\WINDOWS\system32\xpsp2res.dll	0x005F0000	0x002C5000
C:\WINDOWS\system32\rsaenh.dll	0x68000000	0x00036000
C:\WINDOWS\system32\mswsock.dll	0x71A50000	0x0003F000
C:\WINDOWS\system32\hnetcfg.dll	0x662B0000	0x00058000
C:\WINDOWS\System32\wshtcpip.dll	0x71A90000	0x00008000
C:\WINDOWS\system32\DNSAPI.dll	0x76F20000	0x00027000
C:\WINDOWS\system32\iphlpapi.dll	0x76D60000	0x00019000
C:\WINDOWS\System32\winnr.dll	0x76FB0000	0x00008000
C:\WINDOWS\system32\WLDAP32.dll	0x76F60000	0x0002C000
C:\WINDOWS\system32\rasadhlp.dll	0x76FC0000	0x00006000
C:\WINDOWS\system32\CLBCATQ.DLL	0x76FD0000	0x0007F000
C:\WINDOWS\system32\COMRes.dll	0x77050000	0x000C5000

## Run-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\pstorec.dll	0x5E0C0000	0x0000D000
C:\WINDOWS\system32\ATL.DLL	0x76B20000	0x00011000
C:\WINDOWS\system32\PSAPI.DLL	0x76BF0000	0x0000B000
C:\WINDOWS\system32\WININET.dll	0x771B0000	0x000AA000
C:\WINDOWS\system32\CRYPT32.dll	0x77A80000	0x00095000
C:\WINDOWS\system32\MSASN1.dll	0x77B20000	0x00012000

**8.a) svchost.exe - Registry Activities**

## Registry Values Modified:

Key	Name	New Value
HKU\S-1-5-20\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	AppData	C:\Documents and Settings\NetworkService\Application Data
HKU\S-1-5-20\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	Cache	C:\Documents and Settings\NetworkService\Local Settings\Temporary Internet Files
HKU\S-1-5-20\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	Cookies	C:\Documents and Settings\NetworkService\Cookies
HKU\S-1-5-20\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	History	C:\Documents and Settings\NetworkService\Local Settings\History
HKU\S-1-5-20\software\microsoft\windows nt\currentversion\network	UID	pc5_7875768F3D3DB1CC

## Registry Values Read:

Key	Name	Value	Times
HKLM\SOFTWARE\CLASSES\AppID\{1BE1F766-5536-11D1-B726-00C04FB926AF}	LaunchPermission	0x01000480700000008000000000000001 1400000002005c00040000000000	5
HKLM\SOFTWARE\CLASSES\AppID\{1BE1F766-5536-11D1-B726-00C04FB926AF}	LocalService	EventSystem	5
HKLM\SOFTWARE\CLASSES\AppID\{8BC3F05E-D86B-11D0-A075-00C04FB68820}		Windows Management and Instrumentation	5
HKLM\SOFTWARE\CLASSES\AppID\{8BC3F05E-D86B-11D0-A075-00C04FB68820}	LaunchPermission	0x0100048094000000a400000000000001 1400000002008000010000000000	5
HKLM\SOFTWARE\CLASSES\AppID\{8BC3F05E-D86B-11D0-A075-00C04FB68820}	LocalService	winmgmt	5
HKLM\SOFTWARE\CLASSES\AppID\{1BE1F766-5536-11D1-B726-00C04FB926AF}	LocalService	EventSystem	2
HKLM\SOFTWARE\CLASSES\AppID\{8BC3F05E-D86B-11D0-A075-00C04FB68820}	LocalService	winmgmt	2
HKLM\SOFTWARE\CLASSES\CLSID\{1BE1F766-5536-11D1-B726-00C04FB926AF}	AppID	{1BE1F766-5536-11D1-B726-00C04FB926AF}	2
HKLM\SOFTWARE\CLASSES\CLSID\{8BC3F05E-D86B-11D0-A075-00C04FB68820}	AppID	{8BC3F05E-D86B-11D0-A075-00C04FB68820}	2



## Registry Values Read:

Key	Name	Value	Times
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion	DigitalProductId	0xa40000000300000037363438372d36343302d313435373233362d32333833	1
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion	InstallDate	1212451221	1
HKLM\Software\Microsoft\COM3	REGDBVersion	0x0700000000000000	8
HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName	ComputerName	PC	1
HKLM\System\Setup	SystemSetupInProgress	0	1
HKU\S-1-5-20\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	AppData	%USERPROFILE%\Application Data	1
HKU\S-1-5-20\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	Cache	%USERPROFILE%\Local Settings\Temporary Internet Files	3
HKU\S-1-5-20\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	Cookies	%USERPROFILE%\Cookies	3
HKU\S-1-5-20\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	History	%USERPROFILE%\Local Settings\History	3
HKU\S-1-5-20\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache	Signature	Client UrlCache MMF Ver 5.2	2
HKU\S-1-5-20\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content	CacheLimit	163410	1
HKU\S-1-5-20\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content	CachePrefix		2
HKU\S-1-5-20\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content	PerUserItem	1	1
HKU\S-1-5-20\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies	CacheLimit	8192	1
HKU\S-1-5-20\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies	CachePrefix	Cookie:	2
HKU\S-1-5-20\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies	PerUserItem	1	1
HKU\S-1-5-20\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History	CacheLimit	8192	1
HKU\S-1-5-20\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History	CachePrefix	Visited:	2
HKU\S-1-5-20\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History	PerUserItem	1	1

## 8.b) svchost.exe - File Activities

## Files Read:

PIPE\sarpc  
pipe\_AVIRA\_2108

## Files Modified:

PIPE\sarpc  
pipe\_AVIRA\_2108

## File System Control Communication:

File	Control Code	Times
PIPE\sarpc	0x0011C017	7

## Memory Mapped Files:

File Name
C:\WINDOWS\system32\ATL.DLL
C:\WINDOWS\system32\PSAPI.DLL
C:\WINDOWS\system32\WININET.dll
C:\WINDOWS\system32\pstorec.dll
C:\Documents and Settings\NetworkService\Local Settings\Temporary Internet Files\Content.IE5\index.dat



## 9. svchost.exe

### General information about this executable

Analysis Reason:	svchost.exe wrote to the virtual memory of this process
Filename:	svchost.exe
Command Line:	C:\WINDOWS\System32\svchost.exe -k netsvcs
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\ShimEng.dll	0x5CB70000	0x00026000
C:\WINDOWS\AppPatch\AcGeneral.DLL	0x6F880000	0x001CA000
C:\WINDOWS\system32\USER32.dll	0x7E410000	0x00091000
C:\WINDOWS\system32\GDI32.dll	0x77F10000	0x00049000
C:\WINDOWS\System32\WINMM.dll	0x76B40000	0x0002D000
C:\WINDOWS\system32\ole32.dll	0x774E0000	0x0013D000
C:\WINDOWS\system32\msvcrt.dll	0x77C10000	0x00058000
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
C:\WINDOWS\System32\NTMARTA.DLL	0x77690000	0x00021000
C:\WINDOWS\System32\SAMLIB.dll	0x71BF0000	0x00013000
C:\WINDOWS\system32\WLDAP32.dll	0x76F60000	0x0002C000
C:\WINDOWS\System32\xpsp2res.dll	0x005B0000	0x002C5000
c:\windows\system32\shsvcs.dll	0x776E0000	0x00023000
C:\WINDOWS\System32\WINSTA.dll	0x76360000	0x00010000
C:\WINDOWS\system32\NETAPI32.dll	0x5B860000	0x00055000
C:\WINDOWS\System32\rsaenh.dll	0x68000000	0x00036000
c:\windows\system32\dhcpcsvc.dll	0x7D4B0000	0x00022000
c:\windows\system32\DNSAPI.dll	0x76F20000	0x00027000
c:\windows\system32\WS2_32.dll	0x71AB0000	0x00017000
c:\windows\system32\WS2HELP.dll	0x71AA0000	0x00008000
c:\windows\system32\iphlpapi.dll	0x76D60000	0x00019000
c:\windows\system32\wzcsvc.dll	0x7DB10000	0x0008C000
c:\windows\system32\rtutils.dll	0x76E80000	0x0000E000
c:\windows\system32\WMI.dll	0x76D30000	0x00004000
C:\WINDOWS\system32\CRYPT32.dll	0x77A80000	0x00095000
C:\WINDOWS\system32\MSASN1.dll	0x77B20000	0x00012000
c:\windows\system32\EapolQec.dll	0x72810000	0x0000B000
c:\windows\system32\ATL.DLL	0x76B20000	0x00011000
c:\windows\system32\QUtil.dll	0x726C0000	0x00016000
c:\windows\system32\MSVCP60.dll	0x76080000	0x00065000
c:\windows\system32\dot3api.dll	0x478C0000	0x0000A000
c:\windows\system32\WTSAPI32.dll	0x76F50000	0x00008000
c:\windows\system32\ESENT.dll	0x606B0000	0x0010D000



## Load-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\System32\CLBCATQ.DLL	0x76FD0000	0x0007F000
C:\WINDOWS\System32\COMRes.dll	0x77050000	0x000C5000
C:\WINDOWS\System32\rastls.dll	0x76B70000	0x00027000
C:\WINDOWS\system32\CRYPTUI.dll	0x754D0000	0x00080000
C:\WINDOWS\system32\WININET.dll	0x771B0000	0x000AA000
C:\WINDOWS\system32\WINTRUST.dll	0x76C30000	0x0002E000
C:\WINDOWS\system32\IMAGEHLP.dll	0x76C90000	0x00028000
C:\WINDOWS\System32\MPRAPI.dll	0x76D40000	0x00018000
C:\WINDOWS\System32\ACTIVEDS.dll	0x77CC0000	0x00032000
C:\WINDOWS\System32\adsldpc.dll	0x76E10000	0x00025000
C:\WINDOWS\System32\SETUPAPI.dll	0x77920000	0x000F3000
C:\WINDOWS\System32\RASAPI32.dll	0x76EE0000	0x0003C000
C:\WINDOWS\System32\rasman.dll	0x76E90000	0x00012000
C:\WINDOWS\System32\TAPI32.dll	0x76EB0000	0x0002F000
C:\WINDOWS\System32\SCHANNEL.dll	0x767F0000	0x00027000
C:\WINDOWS\System32\WinSCard.dll	0x723D0000	0x0001C000
C:\WINDOWS\System32\PSAPI.DLL	0x76BF0000	0x0000B000
C:\WINDOWS\System32\raschap.dll	0x76BD0000	0x00016000
C:\WINDOWS\system32\msv1_0.dll	0x77C70000	0x00024000
c:\windows\system32\schedsvc.dll	0x77300000	0x00033000
c:\windows\system32\NTDSAPI.dll	0x767A0000	0x00013000
C:\WINDOWS\System32\MSIDLE.DLL	0x74F50000	0x00005000
c:\windows\system32\audiosrv.dll	0x708B0000	0x0000D000
c:\windows\system32\wkssvc.dll	0x76E40000	0x00023000
c:\windows\system32\qmgr.dll	0x5B9F0000	0x0006B000
C:\WINDOWS\system32\MPR.dll	0x71B20000	0x00012000
c:\windows\system32\SHFOLDER.dll	0x76780000	0x00009000
c:\windows\system32\WINHTTP.dll	0x4D4F0000	0x00059000
c:\windows\system32\wuauerv.dll	0x50000000	0x00005000
c:\windows\system32\wbem\wmisvc.dll	0x59490000	0x00028000
C:\WINDOWS\system32\VSSAPI.DLL	0x753E0000	0x0006D000
c:\windows\system32\w32time.dll	0x767C0000	0x0002C000
c:\windows\system32\trkwns.dll	0x75070000	0x00019000
c:\windows\system32\srsvc.dll	0x751A0000	0x0002E000
c:\windows\system32\POWERPROF.dll	0x74AD0000	0x00008000
c:\windows\system32\seclogon.dll	0x73D20000	0x00008000
c:\windows\system32\netman.dll	0x77D00000	0x00033000
c:\windows\system32\netshell.dll	0x76400000	0x001A5000
c:\windows\system32\credui.dll	0x76C00000	0x0002E000
c:\windows\system32\dot3dlg.dll	0x736D0000	0x00006000
c:\windows\system32\OneX.DLL	0x5DCA0000	0x00028000
c:\windows\system32\eappcfg.dll	0x745B0000	0x00022000
c:\windows\system32\eappprxy.dll	0x5DCD0000	0x0000E000
c:\windows\system32\WZCSAPI.DLL	0x73030000	0x00010000
C:\WINDOWS\system32\wuaueng.dll	0x50040000	0x001AB000
C:\WINDOWS\System32\WINSPOOL.DRV	0x73000000	0x00026000
C:\WINDOWS\System32\Cabinet.dll	0x75150000	0x00013000
C:\WINDOWS\System32\mspatcha.dll	0x600A0000	0x0000B000
c:\windows\system32\srsvcs.dll	0x75090000	0x0001A000
c:\windows\pchealth\helpctr\binaries\pchsvc.dll	0x74F40000	0x0000C000
c:\windows\system32\es.dll	0x77710000	0x00042000
c:\windows\system32\ersvc.dll	0x74F80000	0x00009000
c:\windows\system32\dmserver.dll	0x74F90000	0x00009000
c:\windows\system32\cryptsvc.dll	0x76CE0000	0x00012000
c:\windows\system32\certcli.dll	0x77B90000	0x00032000
C:\WINDOWS\system32\mswsock.dll	0x71A50000	0x0003F000



## Load-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\System32\hnetcfg.dll	0x662B0000	0x00058000
C:\WINDOWS\System32\wshtcpip.dll	0x71A90000	0x00008000
c:\windows\system32\wscsvc.dll	0x4C0A0000	0x00017000
c:\windows\system32\msi.dll	0x7D1E0000	0x002BC000
c:\windows\system32\sens.dll	0x722D0000	0x0000D000
C:\WINDOWS\System32\winrnr.dll	0x76FB0000	0x00008000
C:\WINDOWS\System32\sfc.dll	0x76BB0000	0x00005000
C:\WINDOWS\System32\sfc_os.dll	0x76C60000	0x0002A000
c:\windows\system32\browser.dll	0x76DA0000	0x00016000
C:\WINDOWS\system32\wbem\wbemcomn.dll	0x75290000	0x00037000
C:\WINDOWS\System32\Wbem\wbemcore.dll	0x762C0000	0x00085000
C:\WINDOWS\System32\Wbem\lesscli.dll	0x75310000	0x0003F000
C:\WINDOWS\System32\Wbem\FastProx.dll	0x75690000	0x00076000
C:\WINDOWS\System32\SXS.DLL	0x7E720000	0x000B0000
C:\WINDOWS\system32\wbem\wmiutils.dll	0x75020000	0x0001B000
C:\WINDOWS\system32\wbem\repdrvfs.dll	0x75200000	0x0002F000
C:\WINDOWS\system32\comsvcs.dll	0x76620000	0x0013C000
C:\WINDOWS\system32\colbact.DLL	0x75130000	0x00014000
C:\WINDOWS\system32\MTXCLU.DLL	0x750F0000	0x00013000
C:\WINDOWS\system32\WSOCK32.dll	0x71AD0000	0x00009000
C:\WINDOWS\System32\CLUSAPI.DLL	0x76D10000	0x00012000
C:\WINDOWS\System32\RESUTILS.DLL	0x750B0000	0x00012000
C:\WINDOWS\system32\wbem\wmiprvsd.dll	0x597F0000	0x0006D000
C:\WINDOWS\system32\NCOBJAPI.DLL	0x5F770000	0x0000C000
C:\WINDOWS\system32\wbem\wbemess.dll	0x75390000	0x00046000
c:\windows\system32\ipnathlp.dll	0x66460000	0x00055000
c:\windows\system32\AUTHZ.dll	0x776C0000	0x00012000
C:\WINDOWS\system32\wbem\ncprov.dll	0x5F740000	0x0000E000
C:\WINDOWS\System32\rasadhlp.dll	0x76FC0000	0x00006000
C:\WINDOWS\system32\Apphelp.dll	0x77B40000	0x00022000
C:\WINDOWS\system32\upnp.dll	0x76DE0000	0x00024000
C:\WINDOWS\system32\SSDPAPI.dll	0x74F00000	0x0000C000
C:\WINDOWS\System32\RASDLG.dll	0x768D0000	0x000A4000
C:\WINDOWS\system32\wups2.dll	0x50E60000	0x0000C000
C:\WINDOWS\system32\msxml3.dll	0x74980000	0x00113000
C:\WINDOWS\System32\dssenh.dll	0x68100000	0x00026000

## Run-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\wbem\wbemsvc.dll	0x74ED0000	0x0000E000
C:\WINDOWS\system32\wbem\wbemprox.dll	0x74EF0000	0x00008000

## 9.a) svchost.exe - Registry Activities

## Registry Values Modified:

Key	Name	New Value
HKLM\SOFTWARE\MICROSOFTWINDOWS\CURRENTVERSION\WINDOWSUPDATE\REPORTING\EVENTCACHE\3DA21691-E39D-4DA6-8A4B-B43877BCB1B7	FlushCacheFiles	0x43003a005c00570049004e0044004f00570053005c0053006f0066007400

## Registry Values Read:

Key	Name	Value	Times
HKLM\HARDWARE\DESCRIPTION\System	Identifier	AT/AT COMPATIBLE	1
HKLM\SOFTWARE\CLASSES\Interface\{D597BAB1-5B9F-11D1-8DD2-00AA004ABD5E}\TypeLib		{D597DEED-5B9F-11D1-8DD2-00AA004ABD5 1	



## Registry Values Read:

Key	Name	Value	Times
HKLM\SOFTWARE\CLASSES\Interface\{D597BAB1-5B9F-11D1-8DD2-00AA004ABD5E}\TypeLib	Version	2.0	1
HKLM\SOFTWARE\CLASSES\TypeLib\{00020430-0000-0000-C000-000000000046}\2.0\win32		C:\WINDOWS\system32\stdole2.tlb	1
HKLM\SOFTWARE\CLASSES\TypeLib\{D597DEED-5B9F-11D1-8DD2-00AA004ABD5E}\2.0\win32		C:\WINDOWS\system32\SENS.DLL	1
HKLM\SOFTWARE\CLASSES\AppID\{1BE1F766-5536-11D1-B726-00C04FB926AF}	LocalService	EventSystem	2
HKLM\SOFTWARE\CLASSES\AppID\{8BC3F05E-D86B-11D0-A075-00C04FB68820}	LocalService	winmgmt	1
HKLM\SOFTWARE\CLASSES\AppID\{D5978620-5B9F-11D1-8DD2-00AA004ABD5E}	DllSurrogate		4
HKLM\SOFTWARE\CLASSES\CLSID\{1BE1F766-5536-11D1-B726-00C04FB926AF}	AppID	{1BE1F766-5536-11D1-B726-00C04FB926AF}	2
HKLM\SOFTWARE\CLASSES\CLSID\{4590F811-1D3A-11D0-891F-00AA004B2E24}\InprocServer32		C:\WINDOWS\system32\wbem\wbemprox.dll	2
HKLM\SOFTWARE\CLASSES\CLSID\{4590F811-1D3A-11D0-891F-00AA004B2E24}\InprocServer32	ThreadingModel	Both	1
HKLM\SOFTWARE\CLASSES\CLSID\{4FA18276-912A-11D1-AD9B-00C04FD8FDFE}\InprocServer32		C:\WINDOWS\system32\wbem\wbemcore.dll	1
HKLM\SOFTWARE\CLASSES\CLSID\{64B8F404-A4AE-11D1-B7B6-00C04FB926AF}\InprocServer32		C:\WINDOWS\system32\es.dll	1
HKLM\SOFTWARE\CLASSES\CLSID\{7C857801-7381-11CF-884D-00AA004B2E24}\InprocServer32		C:\WINDOWS\system32\wbem\wbemsvc.dll	1
HKLM\SOFTWARE\CLASSES\CLSID\{7C857801-7381-11CF-884D-00AA004B2E24}\InprocServer32	ThreadingModel	Both	1
HKLM\SOFTWARE\CLASSES\CLSID\{8BC3F05E-D86B-11D0-A075-00C04FB68820}	AppID	{8BC3F05E-D86B-11D0-A075-00C04FB68820}	1
HKLM\SOFTWARE\CLASSES\CLSID\{CF4CC405-E2C5-4DDD-B3CE-5E7582D8C9FA}\InprocServer32		C:\WINDOWS\system32\wbem\wmiutils.dll	1
HKLM\SOFTWARE\CLASSES\CLSID\{D5978620-5B9F-11D1-8DD2-00AA004ABD5E}	AppID	{D5978620-5B9F-11D1-8DD2-00AA004ABD5E}	2
HKLM\SOFTWARE\CLASSES\CLSID\{D5978620-5B9F-11D1-8DD2-00AA004ABD5E}\InprocServer32		C:\WINDOWS\System32\ES.DLL	2
HKLM\SOFTWARE\CLASSES\CLSID\{D5978620-5B9F-11D1-8DD2-00AA004ABD5E}\InprocServer32	ThreadingModel	Both	1
HKLM\SOFTWARE\MICROSOFT\EVENTSYSTEM\{26C409CC-AE86-11D1-B616-00805FC79216}\EVENTCLASSES\{D5978620-5B9F-11D1-8DD2-00AA004ABD5E}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}	AllowInprocActivation	4294967295	1
HKLM\SOFTWARE\MICROSOFT\EVENTSYSTEM\{26C409CC-AE86-11D1-B616-00805FC79216}\EVENTCLASSES\{D5978620-5B9F-11D1-8DD2-00AA004ABD5E}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}	EventClassApplication	{00000000-0000-0000-0000-000000000000}	1
HKLM\SOFTWARE\MICROSOFT\EVENTSYSTEM\{26C409CC-AE86-11D1-B616-00805FC79216}\EVENTCLASSES\{D5978620-5B9F-11D1-8DD2-00AA004ABD5E}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}	EventClassID	{D5978620-5B9F-11D1-8DD2-00AA004ABD5E}	1
HKLM\SOFTWARE\MICROSOFT\EVENTSYSTEM\{26C409CC-AE86-11D1-B616-00805FC79216}\EVENTCLASSES\{D5978620-5B9F-11D1-8DD2-00AA004ABD5E}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}	EventClassName	SENS Network Events	1



## Registry Values Read:

Key	Name	Value	Times
{00000000-0000-0000-0000-000000000000}- {00000000-0000-0000-0000-000000000000}			
HKLM\SOFTWARE\MICROSOFT\EVENTSYSTEM\{26C409CC-AE86-11D1-B616-00805FC79216}\EVENTCLASSES\{D5978620-5B9F-11D1-8DD2-00AA004ABD5E}- {00000000-0000-0000-0000-000000000000}- {00000000-0000-0000-0000-000000000000}	EventClassPartitionID	{00000000-0000-0000-0000-000000000000}	1
HKLM\SOFTWARE\MICROSOFT\EVENTSYSTEM\{26C409CC-AE86-11D1-B616-00805FC79216}\EVENTCLASSES\{D5978620-5B9F-11D1-8DD2-00AA004ABD5E}- {00000000-0000-0000-0000-000000000000}- {00000000-0000-0000-0000-000000000000}	FireInParallel	0	1
HKLM\SOFTWARE\MICROSOFT\EVENTSYSTEM\{26C409CC-AE86-11D1-B616-00805FC79216}\EVENTCLASSES\{D5978620-5B9F-11D1-8DD2-00AA004ABD5E}- {00000000-0000-0000-0000-000000000000}- {00000000-0000-0000-0000-000000000000}	FiringInterfaceIID	{D597BAB1-5B9F-11D1-8DD2-00AA004ABD5E}	1
HKLM\SOFTWARE\MICROSOFT\EVENTSYSTEM\{26C409CC-AE86-11D1-B616-00805FC79216}\EVENTCLASSES\{D5978620-5B9F-11D1-8DD2-00AA004ABD5E}- {00000000-0000-0000-0000-000000000000}- {00000000-0000-0000-0000-000000000000}	OwnerSID	S-1-5-18	1
HKLM\SOFTWARE\MICROSOFT\EVENTSYSTEM\{26C409CC-AE86-11D1-B616-00805FC79216}\SUBSCRIPTIONS\{0971EAC5-2E46-44BB-83DA-3450FB37DD1D}- {00000000-0000-0000-0000-000000000000}- {00000000-0000-0000-0000-000000000000}	Active	1	1
HKLM\SOFTWARE\MICROSOFT\EVENTSYSTEM\{26C409CC-AE86-11D1-B616-00805FC79216}\SUBSCRIPTIONS\{0971EAC5-2E46-44BB-83DA-3450FB37DD1D}- {00000000-0000-0000-0000-000000000000}- {00000000-0000-0000-0000-000000000000}	EventClassID	{D5978620-5B9F-11D1-8DD2-00AA004ABD5E}	3
HKLM\SOFTWARE\MICROSOFT\EVENTSYSTEM\{26C409CC-AE86-11D1-B616-00805FC79216}\SUBSCRIPTIONS\{0971EAC5-2E46-44BB-83DA-3450FB37DD1D}- {00000000-0000-0000-0000-000000000000}- {00000000-0000-0000-0000-000000000000}	EventClassPartitionID	{00000000-0000-0000-0000-000000000000}	1
HKLM\SOFTWARE\MICROSOFT\EVENTSYSTEM\{26C409CC-AE86-11D1-B616-00805FC79216}\SUBSCRIPTIONS\{0971EAC5-2E46-44BB-83DA-3450FB37DD1D}- {00000000-0000-0000-0000-000000000000}- {00000000-0000-0000-0000-000000000000}	InterfaceID	{D597BAB1-5B9F-11D1-8DD2-00AA004ABD5E}	1
HKLM\SOFTWARE\MICROSOFT\EVENTSYSTEM\{26C409CC-AE86-11D1-B616-00805FC79216}\SUBSCRIPTIONS\{1D0F2203-E6A9-4C21-B011-703EA64EA176}- {00000000-0000-0000-0000-000000000000}- {00000000-0000-0000-0000-000000000000}	Active	1	1
HKLM\SOFTWARE\MICROSOFT\EVENTSYSTEM\{26C409CC-AE86-11D1-B616-00805FC79216}\SUBSCRIPTIONS\{1D0F2203-E6A9-4C21-B011-703EA64EA176}- {00000000-0000-0000-0000-000000000000}- {00000000-0000-0000-0000-000000000000}	EventClassID	{FAF53CC4-BD73-4E36-83F1-2B23F46E513E}	12
HKLM\SOFTWARE\MICROSOFT\EVENTSYSTEM\{26C409CC-AE86-11D1-B616-00805FC79216}\SUBSCRIPTIONS\{37BB25C3-D617-4538-A034-08B5B02A3A55}- {00000000-0000-0000-0000-000000000000}- {00000000-0000-0000-0000-000000000000}	Active	1	1
HKLM\SOFTWARE\MICROSOFT\EVENTSYSTEM\{26C409CC-AE86-11D1-	EventClassID	{FAF53CC4-BD73-4E36-83F1-2B23F46E513E}	12



## Registry Values Read:

Key	Name	Value	Times
B616-00805FC79216)\SUBSCRIPTIONS\ {37BB25C3-D617-4538-A034-08B5B02A3A55}- {00000000-0000-0000-0000-000000000000}- {00000000-0000-0000-0000-000000000000}			
HKLM\SOFTWARE\MICROSOFT\ EVENTSYSTEM{26C409CC-AE86-11D1- B616-00805FC79216)\SUBSCRIPTIONS\ {569E7DC3-147B-4F2B-99C7-6730A24F7C67}- {00000000-0000-0000-0000-000000000000}- {00000000-0000-0000-0000-000000000000}	Active	1	1
HKLM\SOFTWARE\MICROSOFT\ EVENTSYSTEM{26C409CC-AE86-11D1- B616-00805FC79216)\SUBSCRIPTIONS\ {569E7DC3-147B-4F2B-99C7-6730A24F7C67}- {00000000-0000-0000-0000-000000000000}- {00000000-0000-0000-0000-000000000000}	EventClassID	{FAF53CC4- BD73-4E36-83F1-2B23F46E513E}	12
HKLM\SOFTWARE\MICROSOFT\ EVENTSYSTEM{26C409CC-AE86-11D1- B616-00805FC79216)\SUBSCRIPTIONS\ {7092EABE-3BD2-4008-8046-85F42A551BB4}- {00000000-0000-0000-0000-000000000000}- {00000000-0000-0000-0000-000000000000}	Active	1	1
HKLM\SOFTWARE\MICROSOFT\ EVENTSYSTEM{26C409CC-AE86-11D1- B616-00805FC79216)\SUBSCRIPTIONS\ {7092EABE-3BD2-4008-8046-85F42A551BB4}- {00000000-0000-0000-0000-000000000000}- {00000000-0000-0000-0000-000000000000}	EventClassID	{FAF53CC4- BD73-4E36-83F1-2B23F46E513E}	2
HKLM\SOFTWARE\MICROSOFT\ EVENTSYSTEM{26C409CC-AE86-11D1- B616-00805FC79216)\SUBSCRIPTIONS\ {D789AB02-5B9F-11D1-8DD2-00AA004ABD5E}- {00000000-0000-0000-0000-000000000000}- {00000000-0000-0000-0000-000000000000}	Active	1	1
HKLM\SOFTWARE\MICROSOFT\ EVENTSYSTEM{26C409CC-AE86-11D1- B616-00805FC79216)\SUBSCRIPTIONS\ {D789AB02-5B9F-11D1-8DD2-00AA004ABD5E}- {00000000-0000-0000-0000-000000000000}- {00000000-0000-0000-0000-000000000000}	EventClassID	{D0565000-9DF4-11D1- A281-00C04FCA0AA7}	8
HKLM\SOFTWARE\MICROSOFT\ EVENTSYSTEM{26C409CC-AE86-11D1- B616-00805FC79216)\SUBSCRIPTIONS\ {D789AB02-5B9F-11D1-8DD2-00AA004ABD5E}- {00000000-0000-0000-0000-000000000000}- {00000000-0000-0000-0000-000000000000}	PublisherID	{5FEE1BD6-5B9B-11D1-8DD2-00AA004ABD5	4
HKLM\SOFTWARE\MICROSOFT\ EVENTSYSTEM{26C409CC-AE86-11D1- B616-00805FC79216)\SUBSCRIPTIONS\ {D789AB02-5B9F-11D1-8DD2-00AA004ABD5E}- {00000000-0000-0000-0000-000000000000}- {00000000-0000-0000-0000-000000000000}	SubscriberCLSID	{D3938AB0-5B9D-11D1-8DD2-00AA004ABD5	1
HKLM\SYSTEM\CONTROLSET001\SERVICES\TCPIP\ LINKAGE	Bind	0x5c004400650076006900630065005c007 7b00310041004400340035004200	2
HKLM\Software\Microsoft\COM3	REGDBVersion	0x0700000000000000	22
HKLM\Software\Microsoft\WBEM\CIMOM	Log File Max Size	65536	1
HKLM\Software\Microsoft\WBEM\CIMOM	Logging	1	1
HKLM\System\CurrentControlSet\Control\ComputerName \ActiveComputerName	ComputerName	PC	1
HKLM\System\CurrentControlSet\Services\Tcpip\ Parameters	Domain		4
HKLM\System\CurrentControlSet\Services\Tcpip\ Parameters	Hostname	pc	4
HKLM\software\microsoft\windows nt\currentversion\ network	UID	pc5_7875768F3D3DB1CC	1



## Monitored Registry Keys:

Key Name	Watch subtree	Notify Filter	Count
HKU	1	Key Change, Value Change	3

**9.b) svchost.exe - File Activities**

## Files Read:

C:\WINDOWS\SoftwareDistribution\EventCache\{005CDD85-B361-444A-AF89-B49D160705B2}.bin  
 C:\WINDOWS\system32\SENS.DLL  
 C:\WINDOWS\system32\stdole2.tlb  
 C:\WINDOWS\system32\wbem\Repository\FS\INDEX.BTR  
 PIPE\lsarpc

## Files Modified:

PIPE\lsarpc

## File System Control Communication:

File	Control Code	Times
PIPE\lsarpc	0x0011C017	7

## Device Control Communication:

File	Control Code	Times
unnamed file	0x00120003	8
unnamed file	0x00120040	1

## Memory Mapped Files:

File Name
C:\WINDOWS\system32\SENS.DLL
C:\WINDOWS\system32\stdole2.tlb
C:\WINDOWS\system32\wbem\wbemprox.dll
C:\WINDOWS\system32\wbem\wbemsvc.dll

**10. svchost.exe**

## General information about this executable

Analysis Reason:	svchost.exe wrote to the virtual memory of this process
Filename:	svchost.exe
Command Line:	C:\WINDOWS\system32\svchost.exe -k NetworkService
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\ShimEng.dll	0x5CB70000	0x00026000
C:\WINDOWS\AppPatch\AcGenral.DLL	0x6F880000	0x001CA000
C:\WINDOWS\system32\USER32.dll	0x7E410000	0x00091000
C:\WINDOWS\system32\GDI32.dll	0x77F10000	0x00049000
C:\WINDOWS\system32\WINMM.dll	0x76B40000	0x0002D000
C:\WINDOWS\system32\ole32.dll	0x774E0000	0x0013D000
C:\WINDOWS\system32\msvcrt.dll	0x77C10000	0x00058000



Load-time Dlls		
Module Name	Base Address	Size
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
c:\windows\system32\dnsrslvr.dll	0x76770000	0x0000D000
c:\windows\system32\DNSAPI.dll	0x76F20000	0x00027000
c:\windows\system32\WS2_32.dll	0x71AB0000	0x00017000
c:\windows\system32\WS2HELP.dll	0x71AA0000	0x00008000
c:\windows\system32\iphlpapi.dll	0x76D60000	0x00019000
C:\WINDOWS\system32\rsaenh.dll	0x68000000	0x00036000
C:\WINDOWS\system32\mwssock.dll	0x71A50000	0x0003F000
C:\WINDOWS\system32\hnetcfg.dll	0x662B0000	0x00058000
C:\WINDOWS\System32\wshtcpip.dll	0x71A90000	0x00008000

Run-time Dlls		
Module Name	Base Address	Size
C:\WINDOWS\system32\PSAPI.DLL	0x76BF0000	0x0000B000
C:\WINDOWS\system32\WININET.dll	0x771B0000	0x000AA000
C:\WINDOWS\system32\CRYPT32.dll	0x77A80000	0x00095000
C:\WINDOWS\system32\MSASN1.dll	0x77B20000	0x00012000

### 10.a) svchost.exe - Registry Activities

Registry Values Modified:		
Key	Name	New Value
HKU\S-1-5-20\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	AppData	C:\Documents and Settings\NetworkService\Application Data

Registry Values Read:			
Key	Name	Value	Times
HKU\S-1-5-20\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	AppData	%USERPROFILE%\Application Data	1

### 10.b) svchost.exe - File Activities

Files Read:
PIPE\lsarpc

Files Modified:
PIPE\lsarpc

File System Control Communication:		
File	Control Code	Times
PIPE\lsarpc	0x0011C017	7

Memory Mapped Files:
File Name
C:\WINDOWS\system32\PSAPI.DLL



## Memory Mapped Files:

## File Name

C:\WINDOWS\system32\WININET.dll

## 11. svchost.exe

## General information about this executable

Analysis Reason:	svchost.exe wrote to the virtual memory of this process
Filename:	svchost.exe
MD5:	27c6d03bcdb8cf8b96b716f3d8be3e18
SHA-1:	49083ae3725a0488e0a8fbbe1335c745f70c4667
File Size:	14336
Command Line:	C:\WINDOWS\system32\svchost.exe -k LocalService
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\ShimEng.dll	0x5CB70000	0x00026000
C:\WINDOWS\AppPatch\AcGeneral.DLL	0x6F880000	0x001CA000
C:\WINDOWS\system32\USER32.dll	0x7E410000	0x00091000
C:\WINDOWS\system32\GDI32.dll	0x77F10000	0x00049000
C:\WINDOWS\system32\WINMM.dll	0x76B40000	0x0002D000
C:\WINDOWS\system32\ole32.dll	0x774E0000	0x0013D000
C:\WINDOWS\system32\msvcrt.dll	0x77C10000	0x00058000
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
C:\WINDOWS\system32\NTMARTA.DLL	0x77690000	0x00021000
C:\WINDOWS\system32\SAMLIB.dll	0x71BF0000	0x00013000
C:\WINDOWS\system32\WLDAP32.dll	0x76F60000	0x0002C000
C:\WINDOWS\system32\xpsp2res.dll	0x005B0000	0x002C5000
c:\windows\system32\lmhsvc.dll	0x74C40000	0x00006000
c:\windows\system32\iphlpapi.dll	0x76D60000	0x00019000
c:\windows\system32\WS2_32.dll	0x71AB0000	0x00017000
c:\windows\system32\WS2HELP.dll	0x71AA0000	0x00008000
c:\windows\system32\webclnt.dll	0x5A6E0000	0x00015000
C:\WINDOWS\system32\WININET.dll	0x771B0000	0x000AA000
C:\WINDOWS\system32\CRYPT32.dll	0x77A80000	0x00095000
C:\WINDOWS\system32\MSASN1.dll	0x77B20000	0x00012000
C:\WINDOWS\system32\wsock32.dll	0x71AD0000	0x00009000
c:\windows\system32\regsvc.dll	0x76AF0000	0x00012000
c:\windows\system32\ssdpsrv.dll	0x765E0000	0x00014000
C:\WINDOWS\system32\hnetcfg.dll	0x662B0000	0x00058000
C:\WINDOWS\system32\CLBCATQ.DLL	0x76FD0000	0x0007F000



## Load-time DLLs

Module Name	Base Address	Size
C:\WINDOWS\system32\COMRes.dll	0x77050000	0x000C5000
C:\WINDOWS\system32\mswsock.dll	0x71A50000	0x0003F000
C:\WINDOWS\System32\wshtcpip.dll	0x71A90000	0x00008000
c:\windows\system32\alrsvc.dll	0x70F80000	0x00008000
C:\WINDOWS\system32\NETAPI32.dll	0x5B860000	0x00055000

## Run-time DLLs

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

**11.a) svchost.exe - Registry Activities**

## Registry Values Modified:

Key	Name	New Value
HKU\S-1-5-19\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	AppData	C:\Documents and Settings\LocalService\Application Data
HKU\S-1-5-19\software\microsoft\windows nt\currentversion\network	UID	pc5_7875768F3D3DB1CC

## Registry Values Read:

Key	Name	Value	Times
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion	DigitalProductId	0xa4000000300000037363438372d36343302d313435373233362d32333833	1
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion	InstallDate	1212451221	1
HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName	ComputerName	PC	1
HKU\S-1-5-19\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	AppData	%USERPROFILE%\Application Data	1

**11.b) svchost.exe - File Activities**

## Files Read:

PIPE\lsarpc

## Files Modified:

PIPE\lsarpc

## File System Control Communication:

File	Control Code	Times
PIPE\lsarpc	0x0011C017	7

## Memory Mapped Files:

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

**12. spoolsv.exe**

## General information about this executable

Analysis Reason:	svchost.exe wrote to the virtual memory of this process
Filename:	spoolsv.exe
MD5:	d8e14a61acc1d4a6cd0d38aebac7fa3b
SHA-1:	0e5d1a09a103eae3bd693c7a1c7531fde2e2402b
File Size:	57856
Command Line:	C:\WINDOWS\system32\spoolsv.exe



## General information about this executable

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\GDI32.dll	0x77F10000	0x00049000
C:\WINDOWS\system32\USER32.dll	0x7E410000	0x00091000
C:\WINDOWS\system32\msvcrt.dll	0x77C10000	0x00058000
C:\WINDOWS\system32\ShimEng.dll	0x5CB70000	0x00026000
C:\WINDOWS\AppPatch\AcGeneral.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
C:\WINDOWS\system32\SPOOLSS.DLL	0x742E0000	0x00015000
C:\WINDOWS\system32\WS2_32.dll	0x71AB0000	0x00017000
C:\WINDOWS\system32\WS2HELP.dll	0x71AA0000	0x00008000
C:\WINDOWS\system32\DNSAPI.dll	0x76F20000	0x00027000
C:\WINDOWS\system32\rasadhlp.dll	0x76FC0000	0x00006000
C:\WINDOWS\system32\localspl.dll	0x75BB0000	0x00056000
C:\WINDOWS\system32\sfc_os.dll	0x76C60000	0x0002A000
C:\WINDOWS\system32\WINTRUST.dll	0x76C30000	0x0002E000
C:\WINDOWS\system32\CRYPT32.dll	0x77A80000	0x00095000
C:\WINDOWS\system32\MSASN1.dll	0x77B20000	0x00012000
C:\WINDOWS\system32\IMAGEHLP.dll	0x76C90000	0x00028000
C:\WINDOWS\system32\winspool.drv	0x73000000	0x00026000
C:\WINDOWS\system32\netapi32.dll	0x5B860000	0x00055000
C:\WINDOWS\system32\cnbjmon.dll	0x742A0000	0x0000E000
C:\WINDOWS\system32\pjimon.dll	0x74280000	0x00007000
C:\WINDOWS\system32\tcpmon.dll	0x72400000	0x0000E000
C:\WINDOWS\system32\usbmon.dll	0x723F0000	0x00007000
C:\WINDOWS\System32\mswsock.dll	0x71A50000	0x0003F000
C:\WINDOWS\System32\winnr.dll	0x76FB0000	0x00008000
C:\WINDOWS\system32\WLDAP32.dll	0x76F60000	0x0002C000
C:\WINDOWS\system32\win32spl.dll	0x75C10000	0x00024000
C:\WINDOWS\system32\NETRAP.dll	0x71C80000	0x00007000
C:\WINDOWS\system32\NTDSAPI.dll	0x767A0000	0x00013000
C:\WINDOWS\system32\CLBCATQ.DLL	0x76FD0000	0x0007F000
C:\WINDOWS\system32\COMRes.dll	0x77050000	0x000C5000
C:\WINDOWS\system32\xpsp2res.dll	0x01010000	0x002C5000
C:\WINDOWS\system32\inetpp.dll	0x74300000	0x00015000



Run-time DLLs

Module Name	Base Address	Size
C:\WINDOWS\system32\PSAPI.DLL	0x76BF0000	0x0000B000
C:\WINDOWS\system32\WININET.dll	0x771B0000	0x000AA000

**12.a) spoolsv.exe - File Activities**

Files Read:

PIPE\lsarpc

Files Modified:

PIPE\lsarpc

File System Control Communication:

File	Control Code	Times
PIPE\lsarpc	0x0011C017	7

Memory Mapped Files:

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