



# Anubis - Analysis Report






















## Analysis Report for 09df4497f782fed550b8564dd1f32bcc

MD5: 09df4497f782fed550b8564dd1f32bcc

### Summary:

Description	Risk
<b>Write to foreign memory areas:</b> This executable tampers with the execution of another process.	● high
<b>Performs File Modification and Destruction:</b> The executable modifies and destructs files which are not temporary.	● low
<b>Packed Binary:</b> This executable is protected with a packer in order to prevent it from being reverse engineered.	● medium
<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.	● low
<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>Spawns Processes:</b> The executable produces processes during the execution.	● low
<b>Execution did not terminate correctly:</b> The executable crashed.	● medium
<b>Modify system files:</b> This executable modifies files in the windows system directories.	● medium
<b>Performs Registry Activities:</b> The executable creates and/or modifies registry entries.	● low

## Dependency overview:

-  **09df4497f7.exe** C:\09df4497f7.exe  
Analysis reason: Primary Analysis Subject
-  **csrss.exe** \??C:\WINDOWS\system32\csrss.exe  
Analysis reason: 09df4497f7.exe injected a remote thread into this process
-  **winlogon.exe** \??C:\WINDOWS\system32\winlogon.exe  
Analysis reason: csrss.exe injected a remote thread into this process
-  **Explorer.EXE** C:\WINDOWS\Explorer.EXE  
Analysis reason: csrss.exe injected a remote thread into this process
-  **services.exe** C:\WINDOWS\system32\services.exe  
Analysis reason: A service was started.
-  **lsass.exe** C:\WINDOWS\system32\lsass.exe  
Analysis reason: csrss.exe injected a remote thread into this process
-  **kxuckd.exe** C:\Program Files\Common Files\kxuckd.exe  
Analysis reason: csrss.exe injected a remote thread into this process
-  **svchost.exe** C:\WINDOWS\system32\svchost.exe  
Analysis reason: csrss.exe injected a remote thread into this process
-  **svchost.exe** C:\WINDOWS\system32\svchost.exe  
Analysis reason: csrss.exe injected a remote thread into this process
-  **svchost.exe** C:\WINDOWS\System32\svchost.exe  
Analysis reason: csrss.exe injected a remote thread into this process
-  **svchost.exe** C:\WINDOWS\system32\svchost.exe  
Analysis reason: csrss.exe injected a remote thread into this process
-  **svchost.exe** C:\WINDOWS\system32\svchost.exe  
Analysis reason: csrss.exe injected a remote thread into this process
-  **spoolsv.exe** C:\WINDOWS\system32\spoolsv.exe  
Analysis reason: csrss.exe injected a remote thread into this process
-  **drlwszvxbeo.exe** C:\Program Files\Common Files\drlwszvxbeo.exe  
Analysis reason: csrss.exe injected a remote thread into this process
-  **mscorsvw.exe** C:\WINDOWS\Microsoft.NET\Framework\v4.0.30319\mscorsvw.exe  
Analysis reason: csrss.exe injected a remote thread into this process
-  **wscntfy.exe** C:\WINDOWS\system32\wscntfy.exe  
Analysis reason: csrss.exe injected a remote thread into this process
-  **wuauclt.exe** C:\WINDOWS\system32\wuauclt.exe  
Analysis reason: csrss.exe injected a remote thread into this process
-  **explorer.exe** explorer.exe  
Analysis reason: Started by 09df4497f7.exe
-  **explorer.exe** explorer.exe  
Analysis reason: Started by 09df4497f7.exe

## **Table of Contents:**

1. General Information.....	4
2. 09df4497f7.exe.....	4
a) Registry Activities.....	4
b) File Activities.....	8
c) Process Activities.....	8
3. csrss.exe.....	9
a) Registry Activities.....	10
b) File Activities.....	11
c) Process Activities.....	11
d) Other Activities.....	12
4. winlogon.exe.....	12
a) Registry Activities.....	14
b) File Activities.....	14
5. Explorer.EXE.....	14
a) Registry Activities.....	16
b) File Activities.....	16
c) Other Activities.....	17
6. services.exe.....	17
a) Registry Activities.....	18
b) File Activities.....	18
7. explorer.exe.....	19
8. explorer.exe.....	19
9. lsass.exe.....	19
a) Registry Activities.....	20
b) File Activities.....	21
10. kxuckd.exe.....	21
a) Registry Activities.....	22
b) File Activities.....	22
11. svchost.exe.....	23
a) Registry Activities.....	24
b) File Activities.....	24
12. svchost.exe.....	24
a) Registry Activities.....	25
b) File Activities.....	26
13. svchost.exe.....	26
a) Registry Activities.....	29
b) File Activities.....	29
14. svchost.exe.....	29
a) Registry Activities.....	30
b) File Activities.....	30
15. svchost.exe.....	30
a) Registry Activities.....	31
b) File Activities.....	31
16. spoolsv.exe.....	31
a) Registry Activities.....	33
b) File Activities.....	33
17. dirlwsvxbeo.exe.....	33
a) Registry Activities.....	34
b) File Activities.....	34
18. mscorsvw.exe.....	34
a) Registry Activities.....	35
b) File Activities.....	35
19. wscntfy.exe.....	36
a) Registry Activities.....	36
b) File Activities.....	37
20. wuauclt.exe.....	37



## 1. General Information

### Information about Anubis' invocation

Time needed:	251 s
Report created:	07/22/12, 06:57:31 UTC
Termination reason:	Timeout
Program version:	1.76.3886

## 2. 09df4497f7.exe

### General information about this executable

Analysis Reason:	Primary Analysis Subject
Filename:	09df4497f7.exe
MD5:	09df4497f782fed550b8564dd1f32bcc
SHA-1:	5eedc6576c7c7ba6739722278509f6635ab2fe9e
File Size:	52736
Command Line:	"C:\09df4497f7.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\comctl32.dll	0x5D090000	0x0009A000
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\iphlpapi.dll	0x76D60000	0x00019000
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\ole32.dll	0x774E0000	0x0013D000
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\urlmon.dll	0x7E1E0000	0x000A2000

### 2.a) 09df4497f7.exe - Registry Activities

#### Registry Values Modified:

Key	Name	New Value
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon	System	kduha.exe



## Registry Values Modified:

Key	Name	New Value
HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths	Directory	C:\Documents and Settings\Administrator\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\Administrator\Local Settings\Temporary Internet Files\Content.IE5\Cache1
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\Administrator\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\Administrator\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\Administrator\Local Settings\Temporary Internet Files\Content.IE5\Cache4
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion	kduha.exe	0x657100003d0264111b0e6c796965243522b25dcc7c785b2ece5f49f8093ce
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	History	C:\Documents and Settings\Administrator\Local Settings\History

## Registry Values Read:

Key	Name	Value	Times
HKLM\SYSTEM\CurrentControlSet\Control\Session Manager	CriticalSectionTimeout	2592000	1
HKLM\SYSTEM\Setup	SystemSetupInProgress	0	1
HKLM\SYSTEM\WPA\MediaCenter	Installed	0	2
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\Policies\Microsoft\Windows\Safer\CodelIdentifiers	AuthenticodeEnabled	0	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodelIdentifiers	DefaultLevel	262144	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodelIdentifiers	PolicyScope	0	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodelIdentifiers	TransparentEnabled	1	2
HKLM\Software\Policies\Microsoft\Windows\Safer\CodelIdentifiers\0\Hashes\{349d35ab-37b5-462f-9b89-edd5fbde1328}	HashAlg	32771	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodelIdentifiers\0\Hashes\{349d35ab-37b5-462f-9b89-edd5fbde1328}	ItemData	0x5eab304f957a49896a006c1c31154015	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodelIdentifiers\0\Hashes\{349d35ab-37b5-462f-9b89-edd5fbde1328}	ItemSize	779	1
HKLM\Software\Policies\Microsoft\Windows\Safer\CodelIdentifiers\0\Hashes\{349d35ab-37b5-462f-9b89-edd5fbde1328}	SaferFlags	0	1



## Registry Values Read:

Key	Name	Value	Times
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
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\Terminal Server	TSUserEnabled	0	1
HKLM\System\Setup	SystemSetupInProgress	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Control Panel\International	iCountry	43	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\Control Panel\International\Geo	Nation	244	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Internet Explorer\TypedURLs	url1	http://www.java.com/de/download/installed.jsp	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Internet Explorer\TypedURLs	url2	http://www.google.at/	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Internet Explorer\TypedURLs	url3	http://www.microsoft.com/isapi/rediir.dll?prd=ie&pver=6&ar=msnhome	2



## Registry Values Read:

Key	Name	Value	Times
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	3
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	Cookies	%USERPROFILE%\Cookies	3
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	History	%USERPROFILE%\Local Settings\History	3
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache	Signature	Client UrlCache MMF Ver 5.2	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content	CacheLimit	163410	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content	CachePrefix		2
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content	PerUserItem	1	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content	CacheLimit	8192	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies	CachePrefix	Cookie:	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies	PerUserItem	1	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies	CacheLimit	8192	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012011021720110218	CacheOptions	11	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012011021720110218	CachePath	%USERPROFILE%\Local Settings\History\History.IE5\MSHist012011021720110218\	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012011021720110218	CachePrefix	:2011021720110218:	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012011021720110218	CacheRepair	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012011021820110219	CacheLimit	8192	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012011021820110219	CacheOptions	11	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012011021820110219	CachePath	%USERPROFILE%\Local Settings\History\History.IE5\MSHist012011021820110219\	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012011021820110219	CachePrefix	:2011021820110219:	2



## Registry Values Read:

Key	Name	Value	Times
Internet Settings\5.0\Cache\Extensible Cache\ MSHist012011021820110219			
HKU\S-1-5-21-842925246-1425521274-308236825-500\ Software\Microsoft\Windows\CurrentVersion\ Internet Settings\5.0\Cache\Extensible Cache\ MSHist012011021820110219	CacheRepair	0	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\ Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History	CacheLimit	8192	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\ Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History	CachePrefix	Visited:	2
HKU\S-1-5-21-842925246-1425521274-308236825-500\ Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History	PerUserItem	1	1

**2.b) 09df4497f7.exe - File Activities**

## Files Created:

C:\WINDOWS\system32\kduha.exe

## Files Modified:

C:\WINDOWS\system32\kduha.exe

Ip

\Device\Ip

\Device\Tcp

## 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
\Device\Tcp	0x00120003	6

## Memory Mapped Files:

File Name
C:\09df4497f7.exe
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
C:\WINDOWS\WindowsShell.Manifest
C:\WINDOWS\explorer.exe
C:\WINDOWS\system32\Apphelp.dll
C:\WINDOWS\system32\WININET.dll
C:\WINDOWS\system32\WS2HELP.dll
C:\WINDOWS\system32\WS2_32.dll
C:\WINDOWS\system32\comctl32.dll
C:\WINDOWS\system32\iphlpapi.dll
C:\WINDOWS\system32\kernel32.dll
C:\WINDOWS\system32\psapi.dll
C:\WINDOWS\system32\shell32.dll
C:\WINDOWS\system32\urlmon.dll
C:\Windows\AppPatch\sysmain.sdb

**2.c) 09df4497f7.exe - Process Activities**





## Processes Created:

Executable	Command Line
C:\WINDOWS\explorer.exe	
	C:\WINDOWS\explorer.exe
C:\WINDOWS\explorer.exe	
	C:\WINDOWS\explorer.exe

## Processes Killed:

C:\WINDOWS\explorer.exe

## Remote Threads Created:

## Affected Process

C:\WINDOWS\system32\csrss.exe  
 C:\WINDOWS\explorer.exe  
 C:\WINDOWS\explorer.exe

## Foreign Memory Regions Read:

Process: C:\WINDOWS\explorer.exe  
 Process: C:\WINDOWS\system32\csrss.exe  
 Process: C:\WINDOWS\system32\lsass.exe  
 Process: C:\WINDOWS\system32\services.exe  
 Process: C:\WINDOWS\system32\smss.exe  
 Process: C:\WINDOWS\system32\spoolsv.exe  
 Process: C:\WINDOWS\system32\svchost.exe  
 Process: C:\WINDOWS\system32\winlogon.exe

## Foreign Memory Regions Written:

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

### 3. csrss.exe

## General information about this executable

Analysis Reason:	09df4497f7.exe injected a remote thread into this process
Filename:	csrss.exe
Command Line:	C:\WINDOWS\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,3072,512 Windows=On SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=winsrv:ConServerDllInitialization,2 ProfileControl=Off MaxRequestThreads=16
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\CSRSRV.dll	0x75B40000	0x0000B000
C:\WINDOWS\system32\basesrv.dll	0x75B50000	0x00010000
C:\WINDOWS\system32\winsrv.dll	0x75B60000	0x0004B000
C:\WINDOWS\system32\GDI32.dll	0x77F10000	0x00049000
C:\WINDOWS\system32\KERNEL32.dll	0x7C800000	0x000F6000
C:\WINDOWS\system32\USER32.dll	0x7E410000	0x00091000
C:\WINDOWS\system32\sxs.dll	0x7E720000	0x000B0000
C:\WINDOWS\system32\ADVAPI32.dll	0x77DD0000	0x0009B000
C:\WINDOWS\system32\RPCRT4.dll	0x77E70000	0x00092000
C:\WINDOWS\system32\Secur32.dll	0x77FE0000	0x00011000



## Run-time DLLs

Module Name	Base Address	Size
C:\WINDOWS\system32\comctl32.dll	0x5D090000	0x0009A000
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\iphlpapi.dll	0x76D60000	0x00019000
C:\WINDOWS\system32\dnsapi.dll	0x76F20000	0x00027000
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\VERSION.dll	0x77C00000	0x00008000
C:\WINDOWS\system32\msvcrt.dll	0x77C10000	0x00058000
C:\WINDOWS\system32\SHLWAPI.dll	0x77F60000	0x00076000
C:\WINDOWS\system32\dhcpcsvc.dll	0x7D4B0000	0x00022000
C:\WINDOWS\system32\urlmon.dll	0x7E1E0000	0x000A2000

**3.a) csrss.exe - Registry Activities**

## Registry Keys Created Or Opened:

HKLM\SOFTWARE\CLASSES

## Registry Values Modified:

Key	Name	New Value
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters	DhcpNameServer	
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters	NameServer	
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{1AD45B38-4060-4F73-BB1E-A0439A2D97EB}	DhcpNameServer	85.255.114.43,85.255.112.229
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{1AD45B38-4060-4F73-BB1E-A0439A2D97EB}	NameServer	85.255.114.43,85.255.112.229

## Registry Values Read:

Key	Name	Value	Times
HKLM\SYSTEM\CurrentControlSet\Control\Session Manager	CriticalSectionTimeout	2592000	1
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Linkage	Bind	0x5c004400650076006900630065005c0077b00310030003100410044003500	4
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{1AD45B38-4060-4F73-BB1E-A0439A2D97EB}	AddressType	0	2
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{1AD45B38-4060-4F73-BB1E-A0439A2D97EB}	DhcpServer	255.255.255.255	8
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{1AD45B38-4060-4F73-BB1E-A0439A2D97EB}	EnableDHCP	0	4
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{1AD45B38-4060-4F73-BB1E-A0439A2D97EB}	NameServer	192.168.0.1	8
HKLM\SYSTEM\SETUP	SystemSetupInProgres	0	125
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\System\CurrentControlSet\Services\Tcpip\Parameters	UseDomainNameDevo	0	1
HKLM\System\Setup	SystemSetupInProgres	0	1



## Monitored Registry Keys:

Key Name	Watch subtree	Notify Filter	Count
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters	1	Key Change, Value Change	1

**3.b) csrss.exe - File Activities**

## Files Read:

C:\WINDOWS\WinSxS\Manifests\x86\_Microsoft.Windows.Common-Controls\_6595b64144ccf1df\_6.0.2600.5512\_x-ww\_35d4ce83.Manifest  
 C:\WINDOWS\WinSxS\Policies\x86\_Policy.6.0.Microsoft.Windows.Common-Controls\_6595b64144ccf1df\_x-ww\_5ddad775\6.0.2600.5512.Policy

## Files Modified:

Ip  
 NDIS  
 \Device\Ip  
 \Device\NetBT\_Tcpip\_{1AD45B38-4060-4F73-BB1E-A0439A2D97EB}  
 \Device\Tcp

## Device Control Communication:

File	Control Code	Times
\Device\Tcp	0x00120003	58
\Device\Ip	0x00120040	8
\Device\Ip	0x00120090	4
\Device\NetBT_Tcpip_{1AD45B38-4060-4F73-BB1E-A0439A2D97EB}	0x0021009A	4
NDIS	0x00170008	1

## Memory Mapped Files:

File Name
C:\WINDOWS\system32\WININET.dll
C:\WINDOWS\system32\WS2HELP.dll
C:\WINDOWS\system32\WS2_32.dll
C:\WINDOWS\system32\comctl32.dll
C:\WINDOWS\system32\dhcpcsvc.dll
C:\WINDOWS\system32\dnsapi.dll
C:\WINDOWS\system32\iphlpapi.dll
C:\WINDOWS\system32\psapi.dll
C:\WINDOWS\system32\urlmon.dll

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

## Remote Threads Created:

Affected Process
C:\WINDOWS\system32\winlogon.exe
C:\WINDOWS\explorer.exe
C:\WINDOWS\system32\winlogon.exe
C:\WINDOWS\system32\services.exe
C:\WINDOWS\system32\lsass.exe
C:\Program Files\Common Files\kxuckd.exe
C:\WINDOWS\system32\svchost.exe
C:\WINDOWS\system32\svchost.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
C:\Program Files\Common Files\drlwsvxbeo.exe
C:\WINDOWS\explorer.exe



## Remote Threads Created:

**Affected Process**

C:\WINDOWS\Microsoft.NET\Framework\v4.0.30319\mscorsvw.exe  
 C:\WINDOWS\system32\wscntfy.exe  
 C:\WINDOWS\system32\wuauclt.exe

## Foreign Memory Regions Read:

Process: C:\09df4497f7.exe  
 Process: C:\Program Files\Adobe\Reader 8.0\Reader\reader\_sl.exe  
 Process: C:\Program Files\Common Files\drwsvxvbeo.exe  
 Process: C:\Program Files\Common Files\kxuckd.exe  
 Process: C:\Program Files\Messenger\msmsgs.exe  
 Process: C:\WINDOWS\Microsoft.NET\Framework\v4.0.30319\mscorsvw.exe  
 Process: C:\WINDOWS\explorer.exe  
 Process: C:\WINDOWS\system32\alg.exe  
 Process: C:\WINDOWS\system32\csrss.exe  
 Process: C:\WINDOWS\system32\ctfmon.exe  
 Process: C:\WINDOWS\system32\lsass.exe  
 Process: C:\WINDOWS\system32\services.exe  
 Process: C:\WINDOWS\system32\smss.exe  
 Process: C:\WINDOWS\system32\spoolsv.exe  
 Process: C:\WINDOWS\system32\svchost.exe  
 Process: C:\WINDOWS\system32\winlogon.exe  
 Process: C:\WINDOWS\system32\wscntfy.exe  
 Process: C:\WINDOWS\system32\wuauclt.exe

## Foreign Memory Regions Written:

Process: C:\Program Files\Common Files\drwsvxvbeo.exe  
 Process: C:\Program Files\Common Files\kxuckd.exe  
 Process: C:\WINDOWS\Microsoft.NET\Framework\v4.0.30319\mscorsvw.exe  
 Process: C:\WINDOWS\explorer.exe  
 Process: C:\WINDOWS\system32\lsass.exe  
 Process: C:\WINDOWS\system32\services.exe  
 Process: C:\WINDOWS\system32\spoolsv.exe  
 Process: C:\WINDOWS\system32\svchost.exe  
 Process: C:\WINDOWS\system32\winlogon.exe  
 Process: C:\WINDOWS\system32\wscntfy.exe  
 Process: C:\WINDOWS\system32\wuauclt.exe

**3.d) csrss.exe - Other Activities**

## Mutexes Created:

ZonesCacheCounterMutex  
 ZonesCounterMutex  
 ZonesLockedCacheCounterMutex

## Windows SEH exceptions:

Description	Times
Exception 0xc0000005 (STATUS_ACCESS_VIOLATION) at 0x75b5a71a	3

**4. winlogon.exe**

## General information about this executable

Analysis Reason:	csrss.exe injected a remote thread into this process
Filename:	winlogon.exe



## General information about this executable

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\IMAGEHLP.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\Apphelp.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\csddl.dll	0x76600000	0x0001D000
C:\WINDOWS\System32\dimsntfy.dll	0x47020000	0x00008000
C:\WINDOWS\system32\WINotify.dll	0x75950000	0x0001A000
C:\WINDOWS\system32\MPR.dll	0x71B20000	0x00012000
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



## Load-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\iphlpapi.dll	0x76D60000	0x00019000
C:\WINDOWS\system32\ldap32.dll	0x76F60000	0x0002C000
C:\WINDOWS\system32\cscur.dll	0x77A20000	0x00054000
C:\WINDOWS\system32\xpss2res.dll	0x01760000	0x002C5000
C:\WINDOWS\system32\NTMARTA.DLL	0x77690000	0x00021000
C:\WINDOWS\system32\COMRes.dll	0x77050000	0x000C5000
C:\WINDOWS\system32\OLEAUT32.dll	0x77120000	0x0008B000
C:\WINDOWS\system32\CLBCATQ.DLL	0x76FD0000	0x0007F000

## Run-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\WININET.dll	0x771B0000	0x000AA000
C:\WINDOWS\system32\urlmon.dll	0x7E1E0000	0x000A2000

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

## Registry Values Read:

Key	Name	Value	Times
HKLM\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_BEHAVIORS	*	1	1
HKLM\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_DISABLE_MK_PROTOCOL	*	1	1

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

## Memory Mapped Files:

File Name
C:\WINDOWS\system32\WININET.dll
C:\WINDOWS\system32\urlmon.dll

### 5. Explorer.EXE

## General information about this executable

Analysis Reason:	csrss.exe injected a remote thread into 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



## Load-time Dlls

Module Name	Base Address	Size
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\AcGeneral.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\lcscui.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
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\leappcfg.dll	0x745B0000	0x00022000
C:\WINDOWS\system32\MSVCP60.dll	0x76080000	0x00065000



## Load-time Dlls

Module Name	Base Address	Size
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\advclnt.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\browsecl.dll	0x71600000	0x00012000
C:\WINDOWS\system32\shdoclc.dll	0x71800000	0x00088000

## Run-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\psapi.dll	0x76BF0000	0x0000B000

## 5.a) Explorer.EXE - Registry Activities

## Registry Values Read:

Key	Name	Value	Times
HKLM\SOFTWARE\CLASSES\CLSID\{2227A280-3AEA-1069-A2DE-08002B30309D}	LocalizedString	@%SystemRoot%\system32\SHELL32.dll,-9319	1
HKLM\SOFTWARE\CLASSES\CLSID\{2227A280-3AEA-1069-A2DE-08002B30309D}\SHELLFOLDER	Attributes	536870916	1
HKLM\SOFTWARE\CLASSES\CLSID\{7007ACC7-3202-11D1-AAD2-00805FC1270E}	LocalizedString	@C:\WINDOWS\system32\netshell.dll,-1200	1
HKLM\SOFTWARE\CLASSES\CLSID\{7007ACC7-3202-11D1-AAD2-00805FC1270E}\SHELLFOLDER	Attributes	0x00000020	1
HKLM\SOFTWARE\MICROSOFT\TRACING\NETSHELL	ConsoleTracingMask	4294901760	1
HKLM\SOFTWARE\MICROSOFT\TRACING\NETSHELL	EnableConsoleTracing	0	1
HKLM\SOFTWARE\MICROSOFT\TRACING\NETSHELL	EnableFileTracing	0	1
HKLM\SOFTWARE\MICROSOFT\TRACING\NETSHELL	FileDirectory	%windir%\tracing	2
HKLM\SOFTWARE\MICROSOFT\TRACING\NETSHELL	FileTracingMask	4294901760	1
HKLM\SOFTWARE\MICROSOFT\TRACING\NETSHELL	MaxFileSize	1048576	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\SOFTWARE\MICROSOFT\WINDOWS\SHELLNOROAM\MUICACHE\	@C:\WINDOWS\system32\SHELL32.dll	Printers and Faxes	1
HKU\S-1-5-21-842925246-1425521274-308236825-500\SOFTWARE\MICROSOFT\WINDOWS\SHELLNOROAM\MUICACHE\	@C:\WINDOWS\system32\netshell.dll,-	Network Connections	1

## Monitored Registry Keys:

Key Name	Watch subtree	Notify Filter	Count
HKLM\SOFTWARE\MICROSOFT\TRACING\NETSHELL	0	Attributes Change, Value Change, Security Descriptor Change	1

## 5.b) Explorer.EXE - File Activities





## Memory Mapped Files:

## File Name

C:\WINDOWS\system32\psapi.dll

**5.c) Explorer.EXE - Other Activities**

## Keyboard Keys Monitored:

Virtual Key Code	Times
VK_LBUTTON (1)	60

**6. services.exe**

## General information about this executable

Analysis Reason:	A service was started.
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\SCESESRV.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\iphlpapi.dll	0x76D60000	0x00019000
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



## Run-time DLLs

Module Name	Base Address	Size
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\urlmon.dll	0x7E1E0000	0x000A2000

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

## Registry Keys Created Or Opened:

HKLM\SOFTWARE\CLASSES

## Registry Values Read:

Key	Name	Value	Times
HKLM\SYSTEM\CONTROLSET001\ENUM\PCI\VEN_10EC&DEV_8029&SUBSYS_00000000&REV_00\3&13C0B0C5&0&18	Capabilities	0	1
HKLM\SYSTEM\CONTROLSET001\ENUM\PCI\VEN_10EC&DEV_8029&SUBSYS_00000000&REV_00\3&13C0B0C5&0&18	ConfigFlags	0	1
HKLM\SYSTEM\CONTROLSET001\SERVICES\Dnscache\Enum	0	Root\LEGACY_DNSCACHE\0000	1
HKLM\SYSTEM\CONTROLSET001\SERVICES\Dnscache\Enum	Count	1	2
HKLM\SYSTEM\CurrentControlSet\Control\Session Manager	CriticalSectionTimeout	2592000	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\System\CurrentControlSet\Services\SharedAccess	DependOnGroup	0x0000	1
HKLM\System\CurrentControlSet\Services\SharedAccess	DependOnService	0x4e00650074006d0061006e0000005700669006e004d0067006d0074000000	1
HKLM\System\CurrentControlSet\Services\SharedAccess	DisplayName	Windows Firewall/Internet Connection Sharing (ICS)	1
HKLM\System\CurrentControlSet\Services\SharedAccess	ErrorControl	1	1
HKLM\System\CurrentControlSet\Services\SharedAccess	ImagePath	%SystemRoot%\system32\svchost.exe -k netsvcs	1
HKLM\System\CurrentControlSet\Services\SharedAccess	ObjectName	LocalSystem	1
HKLM\System\CurrentControlSet\Services\SharedAccess	Start	2	1
HKLM\System\CurrentControlSet\Services\SharedAccess	Type	32	1

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

## Files Modified:

Ip  
 \Device\Ip  
 \Device\Tcp

## File System Control Communication:

File	Control Code	Times
C:\net\NtControlPipe4, Flags: Named pipe	0x0011C017	1

## Device Control Communication:

File	Control Code	Times
\Device\Tcp	0x00120003	6



## 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\WININET.dll  
 C:\WINDOWS\system32\iphlpapi.dll  
 C:\WINDOWS\system32\urlmon.dll

## 7. explorer.exe

## General information about this executable

Analysis Reason:	Started by 09df4497f7.exe
Filename:	explorer.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

## 8. explorer.exe

## General information about this executable

Analysis Reason:	Started by 09df4497f7.exe
Filename:	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

## 9. lsass.exe

## General information about this executable

Analysis Reason:	csrss.exe injected a remote thread into 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



## Load-time Dlls

Module Name	Base Address	Size
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\scecli.dll	0x74410000	0x0002F000
C:\WINDOWS\system32\SETUPAPI.dll	0x77920000	0x000F3000
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\pstorvc.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
C:\WINDOWS\system32\urlmon.dll	0x7E1E0000	0x000A2000

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



## Registry Keys Created Or Opened:

HKLM\SOFTWARE\CLASSES

## Registry Values Read:

Key	Name	Value	Times
HKLM\SECURITY\Policy\SecDesc		0x0100048098000000a8000000000000011400000002008400060000000100	3
HKLM\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_BEHAVIORS	*	1	1
HKLM\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_DISABLE_MK_PROTOCOL	*	1	1

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

## Files Created:

PIPE\lsass

## Files Read:

C:\lsass, Flags: Named pipe

PIPE\lsass

## Files Modified:

C:\lsass, Flags: Named pipe

PIPE\lsass

## File System Control Communication:

File	Control Code	Times
C:\lsass, Flags: Named pipe	0x00110008	2
C:\lsass, Flags: Named pipe	0x00110024	4
C:\lsass, Flags: Named pipe	0x0011001C	8
PIPE\lsass	0x00110008	1
C:\lsass, Flags: Named pipe	0x00110004	2
PIPE\lsass	0x00110024	2
PIPE\lsass	0x0011001C	4
PIPE\lsass	0x00110004	1

## Memory Mapped Files:

## File Name

C:\WINDOWS\system32\WININET.dll

C:\WINDOWS\system32\psapi.dll

C:\WINDOWS\system32\urlmon.dll

**10. kxuckd.exe**

## General information about this executable

Analysis Reason:	csrss.exe injected a remote thread into this process
Filename:	kxuckd.exe
MD5:	ed22e108cca63fab4ad592f04b117289
SHA-1:	a11b96e200594f19b8e67af04797b61267710fec
File Size:	327901
Command Line:	"C:\Program Files\Common Files\kxuckd.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\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\COMCTL32.dll	0x773D0000	0x00103000
C:\WINDOWS\system32\msvcrt.dll	0x77C10000	0x00058000
C:\WINDOWS\system32\GDI32.dll	0x77F10000	0x00049000
C:\WINDOWS\system32\USER32.dll	0x7E410000	0x00091000
C:\WINDOWS\system32\SHLWAPI.dll	0x77F60000	0x00076000
C:\WINDOWS\system32\comdlg32.dll	0x763B0000	0x00049000
C:\WINDOWS\system32\SHELL32.dll	0x7C9C0000	0x00817000
C:\WINDOWS\system32\MPR.dll	0x71B20000	0x00012000
C:\WINDOWS\system32\ole32.dll	0x774E0000	0x0013D000
C:\WINDOWS\system32\OLEAUT32.dll	0x77120000	0x0008B000
C:\WINDOWS\system32\VERSION.dll	0x77C00000	0x00008000
C:\WINDOWS\system32\WINMM.dll	0x76B40000	0x0002D000
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\uxtheme.dll	0x5AD70000	0x00038000
C:\WINDOWS\system32\SETUPAPI.dll	0x77920000	0x000F3000
C:\WINDOWS\system32\MSCTF.dll	0x74720000	0x0004C000

## Run-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\psapi.dll	0x76BF0000	0x0000B000
C:\WINDOWS\system32\iphlpapi.dll	0x76D60000	0x00019000
C:\WINDOWS\system32\WININET.dll	0x771B0000	0x000AA000
C:\WINDOWS\system32\CRYPT32.dll	0x77A80000	0x00095000
C:\WINDOWS\system32\MSASN1.dll	0x77B20000	0x00012000
C:\WINDOWS\system32\urlmon.dll	0x7E1E0000	0x000A2000

## SigBuster Output

UPX All\_Versions SN:1634

**10.a) kxuckd.exe - Registry Activities**

## Registry Values Read:

Key	Name	Value	Times
HKLM\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_BEHAVIORS	*	1	1
HKLM\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_DISABLE_MK_PROTOCOL	*	1	1

**10.b) kxuckd.exe - File Activities**

## Files Modified:

Ip
\Device\Ip
\Device\Tcp



## Device Control Communication:

File	Control Code	Times
\\Device\\Tcp	0x00120003	6

## Memory Mapped Files:

File Name
C:\WINDOWS\system32\WININET.dll
C:\WINDOWS\system32\iphlpapi.dll
C:\WINDOWS\system32\psapi.dll
C:\WINDOWS\system32\urlmon.dll

## 11. svchost.exe

## General information about this executable

Analysis Reason:	csrss.exe injected a remote thread into this process
Filename:	svchost.exe
MD5:	27c6d03bcdb8cf8b96b716f3d8be3e18
SHA-1:	49083ae3725a0488e0a8fbbe1335c745f70c4667
File Size:	14336
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
c:\windows\system32\WS2HELP.dll	0x71AA0000	0x00008000
C:\WINDOWS\system32\XPS2RES.dll	0x005F0000	0x002C5000
C:\WINDOWS\system32\CLBCATQ.DLL	0x76FD0000	0x0007F000
C:\WINDOWS\system32\COMRes.dll	0x77050000	0x000C5000
c:\windows\system32\termsrv.dll	0x760F0000	0x00053000



Load-time Dlls		
Module Name	Base Address	Size
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\IMAGEHELP.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\Apphelp.dll	0x77B40000	0x00022000

Run-time Dlls		
Module Name	Base Address	Size
C:\WINDOWS\system32\psapi.dll	0x76BF0000	0x0000B000
C:\WINDOWS\system32\iphlpapi.dll	0x76D60000	0x00019000
C:\WINDOWS\system32\WININET.dll	0x771B0000	0x000AA000
C:\WINDOWS\system32\urlmon.dll	0x7E1E0000	0x000A2000

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

Registry Values Read:			
Key	Name	Value	Times
HKLM\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_BEHAVIORS	*	1	1
HKLM\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_DISABLE_MK_PROTOCOL	*	1	1

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

Files Modified:
Ip
\Device\Ip
\Device\Tcp

Device Control Communication:		
File	Control Code	Times
\Device\Tcp	0x00120003	6

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

## 12. svchost.exe

General information about this executable	
Analysis Reason:	csrss.exe injected a remote thread into this process





## General information about this executable

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\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
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
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\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
C:\WINDOWS\system32\urlmon.dll	0x7E1E0000	0x000A2000

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



## Registry Values Read:

Key	Name	Value	Times
HKLM\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_BEHAVIORS	*	1	1
HKLM\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_DISABLE_MK_PROTOCOL	*	1	1

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

## Memory Mapped Files:

File Name
C:\WINDOWS\system32\WININET.dll
C:\WINDOWS\system32\psapi.dll
C:\WINDOWS\system32\urlmon.dll

**13. svchost.exe**

## General information about this executable

Analysis Reason:	csrss.exe injected a remote thread into 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



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\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\ESSENT.dll	0x606B0000	0x0010D000
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\mswsock.dll	0x71A50000	0x0003F000
C:\WINDOWS\System32\hnetcfg.dll	0x662B0000	0x00058000
C:\WINDOWS\System32\wshtcpip.dll	0x71A90000	0x00008000
c:\windows\system32\cryptsvc.dll	0x76CE0000	0x00012000
c:\windows\system32\certcli.dll	0x77B90000	0x00032000
c:\windows\system32\dmserver.dll	0x74F90000	0x00009000
c:\windows\system32\ersvc.dll	0x74F80000	0x00009000
c:\windows\system32\es.dll	0x77710000	0x00042000
c:\windows\pchealth\helpctr\binaries\pchsvc.dll	0x74F40000	0x0000C000
c:\windows\system32\srvc.dll	0x75090000	0x0001A000
c:\windows\system32\netman.dll	0x77D00000	0x00033000
c:\windows\system32\netshell.dll	0x76400000	0x001A5000
c:\windows\system32\credui.dll	0x76C00000	0x0002E000



## Load-time Dlls

Module Name	Base Address	Size
c:\windows\system32\dot3dlg.dll	0x736D0000	0x00006000
c:\windows\system32\OneX.DLL	0x5DCA0000	0x00028000
c:\windows\system32\leappcfg.dll	0x745B0000	0x00022000
c:\windows\system32\leappprxy.dll	0x5DCD0000	0x0000E000
c:\windows\system32\WZCSAPI.DLL	0x73030000	0x00010000
c:\windows\system32\srsvc.dll	0x751A0000	0x0002E000
c:\windows\system32\POWRPROF.dll	0x74AD0000	0x00008000
c:\windows\system32\sens.dll	0x722D0000	0x0000D000
c:\windows\system32\seclogon.dll	0x73D20000	0x00008000
c:\windows\system32\trkwks.dll	0x75070000	0x00019000
c:\windows\system32\w32time.dll	0x767C0000	0x0002C000
c:\windows\system32\wbem\wmisvc.dll	0x59490000	0x00028000
C:\WINDOWS\system32\VSSAPI.DLL	0x753E0000	0x0006D000
c:\windows\system32\wuauserv.dll	0x50000000	0x00005000
C:\WINDOWS\system32\wuaueng.dll	0x50040000	0x001D9000
C:\WINDOWS\System32\WINSPOOL.DRV	0x73000000	0x00026000
C:\WINDOWS\System32\Cabinet.dll	0x75150000	0x00013000
C:\WINDOWS\System32\mspata.dll	0x600A0000	0x0000B000
c:\windows\system32\wscsvcs.dll	0x4C0A0000	0x00017000
c:\windows\system32\msi.dll	0x7D1E0000	0x002BC000
C:\WINDOWS\system32\wbem\wbemcomn.dll	0x75290000	0x00037000
C:\WINDOWS\System32\winrnr.dll	0x76FB0000	0x00008000
C:\WINDOWS\System32\rasadhlp.dll	0x76FC0000	0x00006000
C:\WINDOWS\System32\sfcs.dll	0x76BB0000	0x00005000
C:\WINDOWS\System32\sfcs_os.dll	0x76C60000	0x0002A000
c:\windows\system32\browser.dll	0x76DA0000	0x00016000
C:\WINDOWS\system32\Aphhelp.dll	0x77B40000	0x00022000
C:\WINDOWS\System32\SXS.DLL	0x7E720000	0x000B0000
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\ipnathlp.dll	0x66460000	0x00055000
c:\windows\system32\AUTHZ.dll	0x776C0000	0x00012000
C:\WINDOWS\system32\upnp.dll	0x76DE0000	0x00024000
C:\WINDOWS\system32\SSDPAPI.dll	0x74F00000	0x0000C000
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\wbem\wbemsvc.dll	0x74ED0000	0x0000E000
C:\WINDOWS\system32\wbem\wmiutils.dll	0x75020000	0x0001B000
C:\WINDOWS\system32\wbem\repdrvfs.dll	0x75200000	0x0002F000
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\wups2.dll	0x50F00000	0x0000D000
C:\WINDOWS\system32\wbem\ncprov.dll	0x5F740000	0x0000E000
C:\WINDOWS\System32\RASDLG.dll	0x768D0000	0x000A4000
C:\WINDOWS\System32\dssenh.dll	0x68100000	0x00026000
C:\WINDOWS\system32\wuapi.dll	0x506A0000	0x0008E000
C:\WINDOWS\system32\netcfgx.dll	0x755F0000	0x0009A000



## Run-time DLLs

Module Name	Base Address	Size
C:\WINDOWS\system32\urlmon.dll	0x7E1E0000	0x000A2000

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

## Registry Values Read:

Key	Name	Value	Times
HKLM\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_BEHAVIORS	*	1	1
HKLM\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_DISABLE_MK_PROTOCOL	*	1	1

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

## Memory Mapped Files:

File Name
C:\WINDOWS\system32\urlmon.dll

**14. svchost.exe**

## General information about this executable

Analysis Reason:	csrss.exe injected a remote thread into 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\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\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



## Load-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\mswsock.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
C:\WINDOWS\system32\urlmon.dll	0x7E1E0000	0x000A2000

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

## Registry Values Read:

Key	Name	Value	Times
HKLM\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_BEHAVIORS	*	1	1
HKLM\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_DISABLE_MK_PROTOCOL	*	1	1

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

## Memory Mapped Files:

File Name
C:\WINDOWS\system32\WININET.dll
C:\WINDOWS\system32\psapi.dll
C:\WINDOWS\system32\urlmon.dll

**15. svchost.exe**

## General information about this executable

Analysis Reason:	csrss.exe injected a remote thread into this process
Filename:	svchost.exe
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\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
C:\WINDOWS\system32\OLEAUT32.dll	0x77120000	0x0008B000
C:\WINDOWS\system32\MSACM32.dll	0x77BE0000	0x00015000
C:\WINDOWS\system32\VERSION.dll	0x77C00000	0x00008000



## Load-time Dlls

Module Name	Base Address	Size
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
C:\WINDOWS\system32\COMRes.dll	0x77050000	0x000C5000
C:\WINDOWS\system32\mswsock.dll	0x71A50000	0x0003F000
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\urlmon.dll	0x7E1E0000	0x000A2000

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

## Registry Values Read:

Key	Name	Value	Times
HKLM\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_BEHAVIORS	*	1	1
HKLM\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_DISABLE_MK_PROTOCOL	*	1	1

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

## Memory Mapped Files:

File Name
C:\WINDOWS\system32\psapi.dll
C:\WINDOWS\system32\urlmon.dll

**16. spoolsv.exe**

## General information about this executable

Analysis Reason:	csrss.exe injected a remote thread into this process
Filename:	spoolsv.exe
MD5:	d8e14a61acc1d4a6cd0d38aebac7fa3b
SHA-1:	0e5d1a09a103eae3bd693c7a1c7531fde2e2402b



## General information about this executable

File Size:	57856
Command Line:	C:\WINDOWS\system32\spoolsv.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\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\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
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\IMAGEHELP.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\spool\PRTPROCS\W32X86\filterpipelineprintproc.dll	0x00900000	0x0000A000
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\inetpp.dll	0x74300000	0x00015000
C:\WINDOWS\system32\xpsp2res.dll	0x01010000	0x002C5000





## Run-time DLLs

Module Name	Base Address	Size
C:\WINDOWS\system32\psapi.dll	0x76BF0000	0x0000B000
C:\WINDOWS\system32\iphlpapi.dll	0x76D60000	0x00019000
C:\WINDOWS\system32\WININET.dll	0x771B0000	0x000AA000
C:\WINDOWS\system32\urlmon.dll	0x7E1E0000	0x000A2000

**16.a) spoolsv.exe - Registry Activities**

## Registry Values Read:

Key	Name	Value	Times
HKLM\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_BEHAVIORS	*	1	1
HKLM\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_DISABLE_MK_PROTOCOL	*	1	1

**16.b) spoolsv.exe - File Activities**

## Files Modified:

Ip
\Device\Ip
\Device\Tcp

## Device Control Communication:

File	Control Code	Times
\Device\Tcp	0x00120003	6

## Memory Mapped Files:

File Name
C:\WINDOWS\system32\WININET.dll
C:\WINDOWS\system32\iphlpapi.dll
C:\WINDOWS\system32\psapi.dll
C:\WINDOWS\system32\urlmon.dll

**17. drlwszvxbeo.exe**

## General information about this executable

Analysis Reason:	csrss.exe injected a remote thread into this process
Filename:	drlwszvxbeo.exe
MD5:	ec95a4d3adc866c53bfafc3ba177d905
SHA-1:	78d7358cebb7681ba22b1ec453eb98308eadd619
File Size:	1256684
Command Line:	"C:\Program Files\Common Files\drlwszvxbeo.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\PSAPI.DLL	0x76BF0000	0x0000B000



## 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\iphlpapi.dll	0x76D60000	0x00019000
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\ole32.dll	0x774E0000	0x0013D000
C:\WINDOWS\system32\CRYPT32.dll	0x77A80000	0x00095000
C:\WINDOWS\system32\MSASN1.dll	0x77B20000	0x00012000
C:\WINDOWS\system32\VERSION.dll	0x77C00000	0x00008000
C:\WINDOWS\system32\GDI32.dll	0x77F10000	0x00049000
C:\WINDOWS\system32\SHLWAPI.dll	0x77F60000	0x00076000
C:\WINDOWS\system32\urlmon.dll	0x7E1E0000	0x000A2000
C:\WINDOWS\system32\USER32.dll	0x7E410000	0x00091000

## Program output

<b>Stdout:</b>	..
----------------	----

**17.a) drlwszvxbeo.exe - Registry Activities**

## Registry Values Read:

Key	Name	Value	Times
HKLM\SYSTEM\CurrentControlSet\Control\Session Manager	CriticalSectionTimeout	2592000	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

**17.b) drlwszvxbeo.exe - File Activities**

## Files Modified:

Ip
\Device\Ip
\Device\Tcp

## Device Control Communication:

File	Control Code	Times
\Device\KsecDD	0x00390008	1
\Device\Tcp	0x00120003	6

## 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\WININET.dll
C:\WINDOWS\system32\WS2HELP.dll
C:\WINDOWS\system32\WS2_32.dll
C:\WINDOWS\system32\iphlpapi.dll
C:\WINDOWS\system32\urlmon.dll

**18. mscorsvw.exe**



## General information about this executable

Analysis Reason:	csrss.exe injected a remote thread into this process
Filename:	mscorsvw.exe
MD5:	c5a75eb48e2344abdc162bda79e16841
SHA-1:	ed4851c89bc80c7a38960bc14686513ac1b3fb47
File Size:	130384
Command Line:	C:\WINDOWS\Microsoft.NET\Framework\v4.0.30319\mscorsvw.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\MSVCR100_CLR0400.dll	0x79060000	0x000BE000
C:\WINDOWS\system32\ADVAPI32.dll	0x77DD0000	0x0009B000
C:\WINDOWS\system32\RPCRT4.dll	0x77E70000	0x00092000
C:\WINDOWS\system32\Secur32.dll	0x77FE0000	0x00011000
C:\WINDOWS\system32\USER32.dll	0x7E410000	0x00091000
C:\WINDOWS\system32\GDI32.dll	0x77F10000	0x00049000
C:\WINDOWS\system32\mscoree.dll	0x79000000	0x0004A000
C:\WINDOWS\system32\ole32.dll	0x774E0000	0x0013D000
C:\WINDOWS\system32\msvcrt.dll	0x77C10000	0x00058000
C:\WINDOWS\system32\OLEAUT32.dll	0x77120000	0x0008B000
C:\WINDOWS\Microsoft.NET\Framework\v4.0.30319\mscorsvc.dll	0x608D0000	0x00054000
C:\WINDOWS\Microsoft.NET\Framework\v4.0.30319\fusion.dll	0x604A0000	0x0000C000
C:\WINDOWS\Microsoft.NET\Framework\v4.0.30319\mscoreei.dll	0x603B0000	0x00066000
C:\WINDOWS\system32\SHLWAPI.dll	0x77F60000	0x00076000
C:\WINDOWS\system32\msidle.dll	0x74F50000	0x00005000
C:\WINDOWS\system32\Wtsapi32.dll	0x76F50000	0x00008000
C:\WINDOWS\system32\WINSTA.dll	0x76360000	0x00010000
C:\WINDOWS\system32\NETAPI32.dll	0x5B860000	0x00055000
C:\WINDOWS\system32\powrprof.dll	0x74AD0000	0x00008000

## Run-time DLLs

Module Name	Base Address	Size
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll	0x773D0000	0x00103000
C:\WINDOWS\system32\VERSION.dll	0x77C00000	0x00008000
C:\WINDOWS\system32\urlmon.dll	0x7E1E0000	0x000A2000

**18.a) mscorsvw.exe - Registry Activities**

## Registry Keys Created Or Opened:

HKLM\SOFTWARE\CLASSES

## Registry Values Read:

Key	Name	Value	Times
HKLM\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_BEHAVIORS	*	1	1
HKLM\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_DISABLE_MK_PROTOCOL	*	1	1

**18.b) mscorsvw.exe - File Activities**

## Files Modified:

lp



## Files Modified:

\Device\lp  
 \Device\Tcp

## Device Control Communication:

File	Control Code	Times
\Device\Tcp	0x00120003	6

## 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\WS2HELP.dll
C:\WINDOWS\system32\WS2_32.dll
C:\WINDOWS\system32\iphlpapi.dll
C:\WINDOWS\system32\urlmon.dll

## 19. wscntfy.exe

## General information about this executable

Analysis Reason:	csrss.exe injected a remote thread into this process
Filename:	wscntfy.exe
MD5:	f92e1076c42fcd6db3d72d8cfe9816d5
SHA-1:	549f0a01848375d03159fc74171ed97790fa9650
File Size:	13824
Command Line:	C:\WINDOWS\system32\wscntfy.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\msvcrt.dll	0x77C10000	0x00058000
C:\WINDOWS\system32\USER32.dll	0x7E410000	0x00091000
C:\WINDOWS\system32\GDI32.dll	0x77F10000	0x00049000
C:\WINDOWS\system32\SHELL32.dll	0x7C9C0000	0x00817000
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\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll	0x773D0000	0x00103000
C:\WINDOWS\system32\xpsp2res.dll	0x007C0000	0x002C5000
C:\WINDOWS\system32\MSCTF.dll	0x74720000	0x0004C000
C:\WINDOWS\system32\Apphelp.dll	0x77B40000	0x00022000
C:\WINDOWS\system32\VERSION.dll	0x77C00000	0x00008000

## Run-time DLLs

Module Name	Base Address	Size
C:\WINDOWS\system32\ole32.dll	0x774E0000	0x0013D000
C:\WINDOWS\system32\urlmon.dll	0x7E1E0000	0x000A2000

### 19.a) wscntfy.exe - Registry Activities



## Registry Values Read:

Key	Name	Value	Times
HKLM\SYSTEM\CurrentControlSet\Control\Session Manager	CriticalSectionTimeout	2592000	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

**19.b) wscntfy.exe - File Activities**

## Memory Mapped Files:

File Name
C:\WINDOWS\system32\WS2HELP.dll
C:\WINDOWS\system32\WS2_32.dll
C:\WINDOWS\system32\iphlpapi.dll
C:\WINDOWS\system32\urlmon.dll

**20. wuauclt.exe**

## General information about this executable

Analysis Reason:	csrss.exe injected a remote thread into this process
Filename:	wuauclt.exe
MD5:	62bb79160f86cd962f312c68c6239bfd
SHA-1:	c2de8148e1a8e8f097e3a40232ddb04efd0a7cc6
File Size:	53472
Command Line:	"C:\WINDOWS\system32\wuauclt.exe" /RunStoreAsComServer Local [2a8]SUSDSf0c7666bfc54a04ca39ec51a6dc8d2fd
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\msvcrt.dll	0x77C10000	0x00058000
C:\WINDOWS\system32\ole32.dll	0x774E0000	0x0013D000
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\OLEAUT32.dll	0x77120000	0x0008B000
C:\WINDOWS\system32\SHLWAPI.dll	0x77F60000	0x00076000
C:\WINDOWS\system32\ShimEng.dll	0x5CB70000	0x00026000
C:\WINDOWS\AppPatch\AcGeneral.DLL	0x6F880000	0x001CA000
C:\WINDOWS\system32\WINMM.dll	0x76B40000	0x0002D000
C:\WINDOWS\system32\MSACM32.dll	0x77BE0000	0x00015000
C:\WINDOWS\system32\VERSION.dll	0x77C00000	0x00008000
C:\WINDOWS\system32\SHELL32.dll	0x7C9C0000	0x00817000
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\wuaueng.dll	0x50040000	0x001D9000
C:\WINDOWS\system32\WS2_32.dll	0x71AB0000	0x00017000
C:\WINDOWS\system32\WS2HELP.dll	0x71AA0000	0x00008000
C:\WINDOWS\system32\ESENT.dll	0x606B0000	0x0010D000



## Load-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\WTSAPI32.dll	0x76F50000	0x00008000
C:\WINDOWS\system32\WINSTA.dll	0x76360000	0x00010000
C:\WINDOWS\system32\NETAPI32.dll	0x5B860000	0x00055000
C:\WINDOWS\system32\WINSPOOL.DRV	0x73000000	0x00026000
C:\WINDOWS\system32\IPHLPAPI.DLL	0x76D60000	0x00019000
C:\WINDOWS\system32\WINHTTP.dll	0x4D4F0000	0x00059000
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\Cabinet.dll	0x75150000	0x00013000
C:\WINDOWS\system32\mspatcha.dll	0x600A0000	0x0000B000
C:\WINDOWS\system32\Xpsp2res.dll	0x00B30000	0x002C5000
C:\WINDOWS\system32\CLBCATQ.DLL	0x76FD0000	0x0007F000
C:\WINDOWS\system32\COMRes.dll	0x77050000	0x000C5000
C:\WINDOWS\system32\wups2.dll	0x50F00000	0x0000D000