# Anubis - Analysis Report

## Analysis Report for 59611375

MD5: 8a2ce75583848c2bb16cb12047671278

### Summary:

| Description | Risk |
|---|---|
| **Write to foreign memory areas**: This executable tampers with the execution of another process. | high |
| **Performs File Modification and Destruction**: The executable modifies and destructs files which are not temporary. | low |
| **Autostart capabilities**: This executable registers processes to be executed at system start. This could result in unwanted actions to be performed automatically. | medium |
| **Spawns Processes**: The executable produces processes during the execution. | low |
| **Execution did not terminate correctly**: The executable crashed. | medium |
| **Performs Registry Activities**: The executable creates and/or modifies registry entries. | low |

## Dependency overview:

**59611375.exe** C:\59611375.exe

Analysis reason: Primary Analysis Subject

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

Analysis reason: Started by 59611375.exe

## Table of Contents:

1. General Information..... 4
2. 59611375.exe..... 4
   a) Registry Activities..... 4
   b) File Activities..... 5
   c) Process Activities..... 6
3. svchost.exe..... 6
   a) Registry Activities..... 7
   b) File Activities..... 12
   c) Network Activities..... 13

# 1. General Information

| Information about Anubis' invocation | |
|---|---|
| Time needed: | 251 s |
| Report created: | 02/08/12, 00:28:33 UTC |
| Termination reason: | Timeout |
| Program version: | 1.75.3394 |

# 2. 59611375.exe

| General information about this executable | |
|---|---|
| Analysis Reason: | Primary Analysis Subject |
| Filename: | 59611375.exe |
| MD5: | 8a2ce75583848c2bb16cb12047671278 |
| SHA-1: | 53a2590cf00544092bba241ad08ce52d323a4d5e |
| File Size: | 108032 |
| Command Line: | "C:\59611375.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\msvcrt.dll | 0x77C10000 | 0x00058000 |
| C:\WINDOWS\system32\USER32.dll | 0x7E410000 | 0x00091000 |
| C:\WINDOWS\system32\GDI32.dll | 0x77F10000 | 0x00049000 |

Run-time Dlls

| Module Name | Base Address | Size |
|---|---|---|
| C:\WINDOWS\system32\svchost.exe | 0x01000000 | 0x00006000 |
| C:\WINDOWS\system32\Apphelp.dll | 0x77B40000 | 0x00022000 |
| C:\WINDOWS\system32\VERSION.dll | 0x77C00000 | 0x00008000 |
| C:\WINDOWS\system32\ADVAPI32.DLL | 0x77DD0000 | 0x0009B000 |
| C:\WINDOWS\system32\RPCRT4.dll | 0x77E70000 | 0x00092000 |
| C:\WINDOWS\system32\Secur32.dll | 0x77FE0000 | 0x00011000 |

## 2.a) 59611375.exe - Registry Activities

Registry Values Read:

| Key | Name | Value | Times |
|---|---|---|---|
| HKLM\SYSTEM\WPA\MediaCenter | Installed | 0 | 1 |
| HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers | AuthenticodeEnabled | 0 | 1 |
| HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers | DefaultLevel | 262144 | 1 |
| HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers | PolicyScope | 0 | 1 |
| HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers | TransparentEnabled | 1 | 2 |
| HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{349d35ab-37b5-462f-9b89-edd5fbde1328} | HashAlg | 32771 | 1 |
| HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{349d35ab-37b5-462f-9b89-edd5fbde1328} | ItemData | 0x5eab304f957a49896a006c1c31154015 | 1 |
| HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{349d35ab-37b5-462f-9b89-edd5fbde1328} | ItemSize | 779 | 1 |

Registry Values Read:

| Key | Name | Value | Times |
|---|---|---|---|
| HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{349d35ab-37b5-462f-9b89-edd5fbde1328} | SaferFlags | 0 | 1 |
| HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{7fb9cd2e-3076-4df9-a57b-b813f72dbb91} | HashAlg | 32771 | 1 |
| HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{7fb9cd2e-3076-4df9-a57b-b813f72dbb91} | ItemData | 0x67b0d48b343a3fd3bce9dc646704f394 | 1 |
| HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{7fb9cd2e-3076-4df9-a57b-b813f72dbb91} | ItemSize | 517 | 1 |
| HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{7fb9cd2e-3076-4df9-a57b-b813f72dbb91} | SaferFlags | 0 | 1 |
| HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f} | HashAlg | 32771 | 1 |
| HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f} | ItemData | 0x327802dcfef8c893dc8ab006dd847d1d | 1 |
| HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f} | ItemSize | 918 | 1 |
| HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f} | SaferFlags | 0 | 1 |
| 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 |
| 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 |

## 2.b) 59611375.exe - File Activities

File System Control Communication:

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

Memory Mapped Files:

| File Name |
|---|
| C:\WINDOWS\system32\Apphelp.dll |
| C:\WINDOWS\system32\svchost.exe |
| C:\Windows\AppPatch\sysmain.sdb |

## 2.c) 59611375.exe - Process Activities

Processes Created:

| Executable | Command Line |
|---|---|
| C:\WINDOWS\system32\svchost.exe | |
| | svchost.exe |

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

# 3. svchost.exe

General information about this executable

| | |
|---|---|
| Analysis Reason: | Started by 59611375.exe |
| Filename: | svchost.exe |
| Command Line: | svchost.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\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 |

Load-time Dlls

| Module Name | Base Address | Size |
|---|---|---|
| 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 |

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\WS2HELP.dll | 0x71AA0000 | 0x00008000 |
| C:\WINDOWS\system32\ws2_32.dll | 0x71AB0000 | 0x00017000 |
| C:\WINDOWS\system32\MSCTF.dll | 0x74720000 | 0x0004C000 |
| C:\WINDOWS\system32\DNSAPI.dll | 0x76F20000 | 0x00027000 |
| C:\WINDOWS\system32\WLDAP32.dll | 0x76F60000 | 0x0002C000 |
| C:\WINDOWS\System32\winrnr.dll | 0x76FB0000 | 0x00008000 |
| C:\WINDOWS\system32\rasadhlp.dll | 0x76FC0000 | 0x00006000 |

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

Registry Values Modified:

| Key | Name | New Value |
|---|---|---|
| HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon | Taskman | C:\Documents and Settings\Administrator\mscdcx.exe |

Registry Values Read:

| Key | Name | Value | Times |
|---|---|---|---|
| HKLM\SOFTWARE\Microsoft\CTF\SystemShared\ | CUAS | 0 | 1 |
| HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon | Taskman | C:\Documents and Settings\Administrator\mscdcx.exe | 70 |
| HKLM\SYSTEM\CurrentControlSet\Control\Session Manager | CriticalSectionTimeout | 2592000 | 1 |
| HKLM\SYSTEM\CurrentControlSet\Services\Winsock\Parameters | Transports | 0x540063007000690070000000 4e00650077400420049004f00530000000000 | 2 |
| HKLM\SYSTEM\Setup | SystemSetupInProgres | 0 | 1 |
| HKLM\SYSTEM\WPA\MediaCenter | Installed | 0 | 1 |
| HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.iac2 | aFormatTagCache | 0x01000000100000000204000014000000 | 1 |
| HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.iac2 | cFilterTags | 0 | 1 |
| HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.iac2 | cFormatTags | 2 | 1 |
| HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.iac2 | fdwSupport | 1 | 1 |
| HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.imaadpcm | aFormatTagCache | 0x01000000100000001100000014000000 | 1 |
| HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.imaadpcm | cFilterTags | 0 | 1 |
| HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.imaadpcm | cFormatTags | 2 | 1 |
| HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.imaadpcm | fdwSupport | 1 | 1 |
| HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.l3acm | aFormatTagCache | 0x01000000100000000550000001e000000 | 1 |
| HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.l3acm | cFilterTags | 0 | 1 |
| HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.l3acm | cFormatTags | 2 | 1 |

Registry Values Read:

| Key | Name | Value | Times |
|---|---|---|---|
| HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.l3acm | fdwSupport | 1 | 1 |
| HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msadpcm | aFormatTagCache | 0x01000000100000000200000032000000 | 1 |
| HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msadpcm | cFilterTags | 0 | 1 |
| HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msadpcm | cFormatTags | 2 | 1 |
| HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msadpcm | fdwSupport | 1 | 1 |
| HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msaudio1 | aFormatTagCache | 0x01000000120000006001000016000000661010000 1c000000 | 1 |
| HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msaudio1 | cFilterTags | 0 | 1 |
| HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msaudio1 | cFormatTags | 3 | 1 |
| HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msaudio1 | fdwSupport | 1 | 1 |
| HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msg711 | aFormatTagCache | 0x01000000100000000600000012000000070000001200000 0 | 1 |
| HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msg711 | cFilterTags | 0 | 1 |
| HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msg711 | cFormatTags | 3 | 1 |
| HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msg711 | fdwSupport | 1 | 1 |
| HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msg723 | aFormatTagCache | 0x01000000100000004200000001c000000 | 1 |
| HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msg723 | cFilterTags | 0 | 1 |
| HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msg723 | cFormatTags | 2 | 1 |
| HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msg723 | fdwSupport | 1 | 1 |
| HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msgsm610 | aFormatTagCache | 0x01000000100000003100000014000000 | 1 |
| HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msgsm610 | cFilterTags | 0 | 1 |
| HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msgsm610 | cFormatTags | 2 | 1 |
| HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.msgsm610 | fdwSupport | 1 | 1 |
| HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.sl_anet | aFormatTagCache | 0x01000000100000003001000016000000 | 1 |
| HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.sl_anet | cFilterTags | 0 | 1 |
| HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.sl_anet | cFormatTags | 2 | 1 |
| HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.sl_anet | fdwSupport | 1 | 1 |
| HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.trspch | aFormatTagCache | 0x01000000100000002200000032000000 | 1 |
| HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.trspch | cFilterTags | 0 | 1 |
| HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.trspch | cFormatTags | 2 | 1 |
| HKLM\Software\Microsoft\AudioCompressionManager\DriverCache\msacm.trspch | fdwSupport | 1 | 1 |
| HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32 | midimapper | | 2 |
| HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32 | msacm.iac2 | C:\WINDOWS\system32\iac25_32.ax | 2 |
| HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32 | msacm.imaadpcm | | 3 |

Registry Values Read:

| Key | Name | Value | Times |
|---|---|---|---|
| HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32 | msacm.l3acm | C:\WINDOWS\system32\l3codeca.acm | 2 |
| HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32 | msacm.msadpcm | | 3 |
| HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32 | msacm.msaudio1 | | 3 |
| HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32 | msacm.msg711 | | 3 |
| HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32 | msacm.msg723 | | 3 |
| HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32 | msacm.msgsm610 | msgsm32.acm | 3 |
| HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32 | msacm.sl_anet | sl_anet.acm | 2 |
| HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32 | msacm.trspch | tssoft32.acm | 3 |
| HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32 | vidc.I420 | | 2 |
| HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32 | vidc.M261 | | 2 |
| HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32 | vidc.M263 | | 2 |
| HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32 | vidc.cvid | | 2 |
| HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32 | vidc.iv31 | | 2 |
| HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32 | vidc.iv32 | | 2 |
| HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32 | vidc.iv41 | | 2 |
| HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32 | vidc.iv50 | | 1 |
| HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32 | vidc.iyuv | | 2 |
| HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32 | vidc.mrle | | 2 |
| HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32 | vidc.msvc | | 2 |
| HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32 | vidc.uyvy | | 2 |
| HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32 | vidc.yuy2 | | 2 |
| HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32 | vidc.yvu9 | | 2 |
| HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32 | vidc.yvyu | | 2 |
| HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32 | wavemapper | | 2 |
| HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers | TransparentEnabled | 1 | 1 |
| HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName | ComputerName | PC | 1 |
| HKLM\System\CurrentControlSet\Control\MediaProperties\PrivateProperties\Joystick\Winmm | wheel | 1 | 1 |
| HKLM\System\CurrentControlSet\Control\ProductOptions | ProductType | WinNT | 1 |
| HKLM\System\CurrentControlSet\Services\LDAP | LdapClientIntegrity | 1 | 1 |
| HKLM\System\CurrentControlSet\Services\Tcpip\Parameters | Domain | | 6 |
| HKLM\System\CurrentControlSet\Services\Tcpip\Parameters | Hostname | pc | 6 |
| HKLM\System\CurrentControlSet\Services\Tcpip\Parameters | UseDomainNameDevo | 0 | 1 |

Registry Values Read:

| Key | Name | Value | Times |
|---|---|---|---|
| HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Winsock | HelperDllName | %SystemRoot%\System32\wshtcpip.dll | 1 |
| HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Winsock | Mapping | 0x0b000000030000000200000001000000006000000020000000100000000000 | 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 | UseDelayedAcceptanc | 0 | 1 |
| HKLM\System\CurrentControlSet\Services\WinSock2\Parameters | WinSock_Registry_Ver | 2.0 | 4 |
| HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5 | Num_Catalog_Entries | 3 | 1 |
| HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5 | Serial_Access_Num | 4 | 2 |
| HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001 | DisplayString | Tcpip | 4 |
| HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001 | Enabled | 1 | 1 |
| HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001 | LibraryPath | %SystemRoot%\System32\mswsock.dll | 2 |
| HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001 | ProviderId | 0x409d05229e7ecf11ae5a00aa00a7112b | 1 |
| HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001 | StoresServiceClassInfo | 0 | 1 |
| HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001 | SupportedNameSpace | 12 | 1 |
| HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001 | Version | 0 | 1 |
| HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002 | DisplayString | NTDS | 4 |
| HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002 | Enabled | 1 | 1 |
| HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002 | LibraryPath | %SystemRoot%\System32\winrnr.dll | 2 |
| HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002 | ProviderId | 0xee37263b80e5cf11a55500c04fd8d4ac | 1 |
| HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002 | StoresServiceClassInfo | 0 | 1 |
| HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002 | SupportedNameSpace | 32 | 1 |
| HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002 | Version | 0 | 1 |
| HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003 | DisplayString | Network Location Awareness (NLA) Namespace | 4 |
| HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003 | Enabled | 1 | 1 |

Registry Values Read:

| Key | Name | Value | Times |
|---|---|---|---|
| HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003 | LibraryPath | %SystemRoot%\System32\mswsock.dll | 2 |
| HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003 | ProviderId | 0x3a244266a83ba64abaa52e0bd71fdd83 | 1 |
| HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003 | StoresServiceClassInfo | 0 | 1 |
| HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003 | SupportedNameSpace | 15 | 1 |
| HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003 | Version | 0 | 1 |
| HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9 | Next_Catalog_Entry_ID | 1020 | 1 |
| HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9 | Num_Catalog_Entries | 13 | 1 |
| HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9 | Serial_Access_Num | 6 | 2 |
| HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000001 | PackedCatalogItem | %SystemRoot%\system32\mswsock. | 1 |
| HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000002 | PackedCatalogItem | %SystemRoot%\system32\mswsock. | 1 |
| HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000003 | PackedCatalogItem | %SystemRoot%\system32\mswsock. | 1 |
| HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000004 | PackedCatalogItem | %SystemRoot%\system32\rsvpsp.d | 1 |
| HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000005 | PackedCatalogItem | %SystemRoot%\system32\rsvpsp.d | 1 |
| HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000006 | PackedCatalogItem | %SystemRoot%\system32\mswsock. | 1 |
| HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000007 | PackedCatalogItem | %SystemRoot%\system32\mswsock. | 1 |
| HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000008 | PackedCatalogItem | %SystemRoot%\system32\mswsock. | 1 |
| HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000009 | PackedCatalogItem | %SystemRoot%\system32\mswsock. | 1 |
| HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000010 | PackedCatalogItem | %SystemRoot%\system32\mswsock. | 1 |
| HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000011 | PackedCatalogItem | %SystemRoot%\system32\mswsock. | 1 |
| HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000012 | PackedCatalogItem | %SystemRoot%\system32\mswsock. | 1 |
| HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000013 | PackedCatalogItem | %SystemRoot%\system32\mswsock. | 1 |
| HKLM\System\Setup | SystemSetupInProgres | 0 | 1 |
| HKU\S-1-5-21-842925246-1425521274-308236825-500\Keyboard Layout\Toggle | Language Hotkey | 1 | 2 |
| HKU\S-1-5-21-842925246-1425521274-308236825-500\Keyboard Layout\Toggle | Layout Hotkey | 2 | 2 |

Registry Values Read:

| Key | Name | Value | Times |
|---|---|---|---|
| HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Multimedia\Audio | SystemFormats | CD Quality,Radio Quality,Telephone Quality | 1 |
| HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders | Local Settings | %USERPROFILE%\Local Settings | 1 |
| HKU\S-1-5-21-842925246-1425521274-308236825-500\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders | Personal | %USERPROFILE%\My Documents | 1 |

Monitored Registry Keys:

| Key Name | Watch subtree | Notify Filter | Count |
|---|---|---|---|
| HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5 | 0 | Key Change | 1 |
| HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9 | 0 | Key Change | 1 |

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

Files Created:

| |
|---|
| C:\Documents and Settings\Administrator\mscdcx.exe |
| \Device\NamedPipe\Win32Pipes.000004b4.00000001 |

Files Read:

| |
|---|
| PIPE\lsarpc |

Files Modified:

| |
|---|
| C:\Documents and Settings\Administrator\mscdcx.exe |
| PIPE\lsarpc |
| \Device\Afd\Endpoint |
| \Device\RasAcd |

File System Control Communication:

| File | Control Code | Times |
|---|---|---|
| C:\Program Files\Common Files\ | 0x00090028 | 1 |
| PIPE\lsarpc | 0x0011C017 | 3 |

Device Control Communication:

| File | Control Code | Times |
|---|---|---|
| \Device\KsecDD | 0x00390008 | 8 |
| \Device\Afd\Endpoint | AFD_GET_INFO (0x0001207B) | 2 |
| \Device\Afd\Endpoint | AFD_SET_CONTEXT (0x00012047) | 5 |
| \Device\Afd\Endpoint | AFD_SET_INFO (0x0001203B) | 3 |
| \Device\RasAcd | 0x00F14014 | 1 |
| \Device\Afd\Endpoint | AFD_GET_TDI_HAND (0x00012037) | 4 |
| \Device\Afd\Endpoint | AFD_BIND (0x00012003) | 2 |
| \Device\Afd\Endpoint | AFD_GET_SOCK_NAI (0x0001202F) | 2 |

Memory Mapped Files:

| File Name |
|---|
| C:\59611375.exe |

Memory Mapped Files:

| File Name |
|---|
| C:\WINDOWS\AppPatch\AcGenral.DLL |
| C:\WINDOWS\System32\winrnr.dll |
| C:\WINDOWS\System32\wshtcpip.dll |
| C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll |
| C:\WINDOWS\WindowsShell.Manifest |
| C:\WINDOWS\system32\DNSAPI.dll |
| C:\WINDOWS\system32\MSACM32.dll |
| C:\WINDOWS\system32\MSCTF.dll |
| C:\WINDOWS\system32\SHELL32.dll |
| C:\WINDOWS\system32\ShimEng.dll |
| C:\WINDOWS\system32\UxTheme.dll |
| C:\WINDOWS\system32\WINMM.dll |
| C:\WINDOWS\system32\WS2HELP.dll |
| C:\WINDOWS\system32\comctl32.dll |
| C:\WINDOWS\system32\hnetcfg.dll |
| C:\WINDOWS\system32\imm32.dll |
| C:\WINDOWS\system32\mswsock.dll |
| C:\WINDOWS\system32\rasadhlp.dll |
| C:\WINDOWS\system32\ws2_32.dll |
| C:\Windows\AppPatch\sysmain.sdb |

## 3.c) svchost.exe - Network Activity

DNS Queries:

| Name | Query Type | Query Result | Successful | Protocol |
|---|---|---|---|---|
| slade.safehousenumber.cor | DNS_TYPE_A | | NO | udp |
| murik.portal-protection.net.ru | DNS_TYPE_A | | NO | udp |