# Malware Analysis Appliance by Blue Coat Systems, Inc.

## Task Details

| | |
|---|---|
| Task ID: | 552 |
| Risk Level: | 7 |
| Date Processed: | 2016-04-28 13:01:58 (UTC) |
| Processing Time: | 2.88 seconds |
| Virtual Environment: | IntelliVM |
| Execution Arguments: | "c:\windows\temp\9b4316a022e8ffa53c35fafab8f7753b.exe" |
| Sample ID: | 138 |
| Type: | basic |
| Owner: | admin |
| Label: | 9b4316a022e8ffa53c35fafab8f7753b |
| Date Added: | 2016-04-28 12:45:04 (UTC) |
| File Type: | PE32:win32:gui |
| File Size: | 305192 bytes |
| MD5: | 9b4316a022e8ffa53c35fafab8f7753b |
| SHA256: | ff81ac1ada501179e980e72ae0459d6be9d6987581d867e79039f84ad8ebda54 |
| Description: | None |

## Pattern Matching Results

| | |
|---|---|
| 3 | Long sleep detected |
| 5 | PE: Contains compressed section |
| 5 | Packer: UPX |
| 4 | Checks whether debugger is present |
| 2 | PE: Nonstandard section |
| 7 | Signed by adware producer [Adware, PUA] |
| 7 | Creates known events: Amonetize 2 |

## Static Events

| | |
|---|---|
| Anomaly: | PE: Contains a virtual section |
| Anomaly: | PE: Contains one or more non-standard sections |
| Packer: | UPX |

## Process/Thread Events

| | |
|---|---|
| Creates process: | C:\windows\temp\9b4316a022e8ffa53c35fafab8f7753b.exe ["C:\windows\temp\9b4316a022e8ffa53c35fafab8f7753b.exe" ] |
| Terminates process: | C:\Windows\Temp\9b4316a022e8ffa53c35fafab8f7753b.exe |

## Named Object Events

| | |
|---|---|
| Creates mutex: | \Sessions\1\BaseNamedObjects\DBWinMutex |
| Creates mutex: | \BaseNamedObjects\AmInst__Runing_1 |
| Creates event: | \Sessions\1\BaseNamedObjects\AmiUpdInstallProgress |
| Creates event: | \Security\LSA_AUTHENTICATION_INITIALIZED |
| Creates event: | \KernelObjects\MaximumCommitCondition |

## File System Events

| | |
|---|---|
| Opens: | C:\Windows\Prefetch\9B4316A022E8FFA53C35FAFAB8F77-1D483179.pf |
| Opens: | C:\Windows\System32 |
| Opens: | C:\Windows\System32\sechost.dll |
| Opens: | C:\windows\temp\VERSION.dll |
| Opens: | C:\Windows\System32\version.dll |
| Opens: | C:\windows\temp\WINHTTP.dll |
| Opens: | C:\Windows\System32\winhttp.dll |
| Opens: | C:\windows\temp\webio.dll |
| Opens: | C:\Windows\System32\webio.dll |
| Opens: | C:\Windows\System32\imm32.dll |
| Opens: | C:\Users\Admin\AppData\Local\Temp |
| Opens: | C:\windows\temp\SspiCli.dll |
| Opens: | C:\Windows\System32\sspicli.dll |
| Opens: | C:\Windows\System32\rpcss.dll |
| Opens: | C:\windows\temp\CRYPTBASE.dll |
| Opens: | C:\Windows\System32\cryptbase.dll |
| Opens: | C:\Windows\System32\uxtheme.dll |
| Opens: | C:\windows\temp\Iphlpapi.dll |
| Opens: | C:\Windows\System32\IPHLPAPI.DLL |
| Opens: | C:\windows\temp\WINNSI.DLL |
| Opens: | C:\Windows\System32\winnsi.dll |
| Opens: | C:\windows\temp\dhcpcsvc6.DLL |
| Opens: | C:\Windows\System32\dhcpcsvc6.dll |
| Opens: | C:\windows\temp\dhcpcsvc.DLL |
| Opens: | C:\Windows\System32\dhcpcsvc.dll |
| Opens: | C:\Program Files\Microsoft Silverlight\sllauncher.exe |
| Opens: | C:\Program Files\Microsoft Silverlight\sllauncher.exe.DLL |
| Opens: | C:\Windows\Temp\9b4316a022e8ffa53c35fafab8f7753b.exe |
| Opens: | C:\windows\temp\CRYPTSP.dll |

```
  Opens:                  C:\Windows\System32\cryptsp.dll
  Opens:                  C:\Windows\System32\rsaenh.dll
  Opens:                  C:\Windows\Globalization\Sorting\SortDefault.nls
  Opens:                  C:\windows\temp\RpcRtRemote.dll
  Opens:                  C:\Windows\System32\RpcRtRemote.dll
  Opens:                  C:\Windows\System32\en-US\KernelBase.dll.mui
  Opens:                  C:\windows\temp\credssp.dll
  Opens:                  C:\Windows\System32\credssp.dll
```

# Windows Registry Events

```
  Opens key:              HKLM\system\currentcontrolset\control\session manager
  Opens key:              HKLM\system\currentcontrolset\control\safeboot\option
  Opens key:              HKLM\system\currentcontrolset\control\srp\gp\dll
  Opens key:              HKLM\software\policies\microsoft\windows\safer\codeidentifiers
  Opens key:              HKCU\software\policies\microsoft\windows\safer\codeidentifiers
  Opens key:              HKCU\
  Opens key:              HKCU\control panel\desktop\muicached\machinelanguageconfiguration
  Opens key:              HKLM\software\policies\microsoft\mui\settings
  Opens key:              HKCU\software\policies\microsoft\control panel\desktop
  Opens key:              HKCU\control panel\desktop\languageconfiguration
  Opens key:              HKCU\control panel\desktop
  Opens key:              HKCU\control panel\desktop\muicached
  Opens key:              HKLM\software\microsoft\windows\currentversion\sidebyside
  Opens key:              HKLM\system\currentcontrolset\control\nls\sorting\versions
  Opens key:              HKLM\
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\diagnostics
  Opens key:              HKLM\system\currentcontrolset\control\error message instrument\
  Opens key:              HKLM\system\currentcontrolset\control\error message instrument
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\gre_initialize
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\compatibility32
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\ime compatibility
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\windows
  Opens key:              HKLM\software\microsoft\ole
  Opens key:              HKLM\software\microsoft\ole\tracing
  Opens key:              HKLM\software\microsoft\oleaut
  Opens key:              HKLM\software\microsoft\rpc
  Opens key:              HKLM\system\currentcontrolset\control\computername\activecomputername
  Opens key:              HKLM\system\setup
  Opens key:              HKLM\software\policies\microsoft\windows nt\rpc
  Opens key:              HKLM\software\policies\microsoft\sqmclient\windows
  Opens key:              HKLM\software\microsoft\sqmclient\windows
  Opens key:              HKLM\software\microsoft\net framework setup\ndp\v1.1.4322
  Opens key:              HKLM\software\microsoft\net framework setup\ndp\v3.5
  Opens key:              HKLM\software\microsoft\net framework setup\ndp\v4\full
  Opens key:              HKLM\software\microsoft\net framework setup\ndp\v4\client
  Opens key:              HKLM\system\currentcontrolset\control\computername
  Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}
  Opens key:              HKCU\software\classes\
  Opens key:              HKLM\software\microsoft\com3
  Opens key:              HKCU\software\classes\clsid\{67bd9eeb-aa06-4329-a940-d250019300c9}
  Opens key:              HKCR\clsid\{67bd9eeb-aa06-4329-a940-d250019300c9}
  Opens key:              HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces
  Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}
  Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}
  Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}
  Opens key:              HKLM\system\currentcontrolset\services\tcpip\linkage
  Opens key:              HKLM\system\currentcontrolset\control\nls\customlocale
  Opens key:              HKLM\system\currentcontrolset\control\nls\extendedlocale
  Opens key:              HKLM\system\currentcontrolset\control\network\{4d36e972-e325-11ce-bfc1-
08002be10318}\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection
  Opens key:              HKLM\software\microsoft\cryptography
  Opens key:              HKLM\software\microsoft\windows nt\currentversion
  Opens key:              HKCU\software\clients\startmenuinternet
  Opens key:              HKLM\software\clients\startmenuinternet
  Opens key:              HKCU\software\classes\appid\9b4316a022e8ffa53c35fafab8f7753b.exe
  Opens key:              HKCR\appid\9b4316a022e8ffa53c35fafab8f7753b.exe
  Opens key:              HKLM\software\microsoft\ole\appcompat
  Opens key:              HKLM\system\currentcontrolset\control\lsa
  Opens key:              HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider
  Opens key:              HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy
  Opens key:
HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration
  Opens key:              HKLM\software\policies\microsoft\cryptography
  Opens key:                HKLM\software\microsoft\cryptography\offload
  Opens key:                HKCU\software\classes\interface\{00000134-0000-0000-c000-000000000046}
  Opens key:                HKCR\interface\{00000134-0000-0000-c000-000000000046}
  Opens key:                HKCU\software\classes\interface\{00000134-0000-0000-c000-
000000000046}\proxystubclsid32
  Opens key:                HKCR\interface\{00000134-0000-0000-c000-000000000046}\proxystubclsid32
  Opens key:                HKLM\software\microsoft\rpc\extensions
  Opens key:                HKLM\system\currentcontrolset\services\bfe
  Opens key:                HKLM\software\microsoft\sqmclient\windows\disabledprocesses\
  Opens key:                HKLM\software\microsoft\sqmclient\windows\disabledsessions\
  Opens key:                HKLM\software\microsoft\windows\currentversion\internet
settings\winhttp\tracing
  Opens key:                HKLM\software\microsoft\windows\currentversion\internet settings
  Opens key:                HKLM\software\microsoft\windows\currentversion\internet settings\winhttp
  Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{8ff7f47b-d658-4061-baea-
1709a0196aed}
  Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{7b9cb019-1924-49a5-867c-
a68f334c8d34}
  Opens key:                HKLM\software\policies\microsoft\windows\currentversion\internet
settings
  Opens key:                HKU\
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\connections
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet settings\wpad
  Opens key:                HKLM\system\currentcontrolset\services\winsock2\parameters
  Opens key:                HKCU\control panel\international
  Opens key:                HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\23648168
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000019
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000012
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000013
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000014
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000015
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000016
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000017
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000018
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\0000000c
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002
```

```
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006
  Opens key:                 HKLM\system\currentcontrolset\control\cmf\config
  Opens key:                 HKLM\system\currentcontrolset\control\lsaextensionconfig\sspicli
  Opens key:                 HKLM\system\currentcontrolset\control\securityproviders
  Opens key:                 HKLM\system\currentcontrolset\control\lsa\sspicache
  Opens key:                 HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll
  Opens key:                 HKLM\system\currentcontrolset\control\securityproviders\saslprofiles
  Opens key:                 HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}
  Opens key:                 HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\b6-0e-33-cb-db-77
  Opens key:                 HKCU\software\classes\interface\{9edc0c90-2b5b-4512-953e-35767bad5c67}
  Opens key:                 HKCR\interface\{9edc0c90-2b5b-4512-953e-35767bad5c67}
  Queries value:             HKLM\system\currentcontrolset\control\session
manager[cwdillegalindllsearch]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
  Queries value:             HKCU\control panel\desktop[preferreduilanguages]
  Queries value:             HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
  Queries value:
HKLM\software\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
  Queries value:             HKLM\system\currentcontrolset\control\nls\sorting\versions[]
  Queries value:             HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
  Queries value:             HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
  Queries value:             HKLM\software\microsoft\windows
nt\currentversion\compatibility32[9b4316a022e8ffa53c35fafab8f7753b]
  Queries value:             HKLM\software\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
  Queries value:             HKLM\software\microsoft\ole[pageallocatorusesystemheap]
  Queries value:             HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
  Queries value:             HKLM\software\microsoft\rpc[maxrpcsize]
  Queries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
  Queries value:             HKLM\system\setup[oobeinprogress]
  Queries value:             HKLM\system\setup[systemsetupinprogress]
  Queries value:             HKLM\software\microsoft\sqmclient\windows[ceipenable]
  Queries value:             HKLM\software\microsoft\net framework setup\ndp\v3.5[install]
  Queries value:             HKLM\software\microsoft\net framework setup\ndp\v3.5[version]
  Queries value:             HKLM\software\microsoft\net framework setup\ndp\v3.5[sp]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[searchlist]
  Queries value:             HKLM\software\microsoft\com3[com+enabled]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[enabledhcp]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[registrationenabled]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[registeradaptername]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[domain]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[dhcpdomain]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[dhcpv6domain]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[nameserver]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[dhcpnameserver]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[enabledhcp]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[registrationenabled]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[registeradaptername]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[domain]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[dhcpdomain]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[nameserver]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[dhcpnameserver]
  Queries value:          HKLM\system\currentcontrolset\services\tcpip\linkage[bind]
  Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
  Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
  Queries value:          HKLM\system\currentcontrolset\control\network\{4d36e972-e325-11ce-bfc1-
08002be10318}\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection[pnpinstanceid]
  Queries value:          HKLM\software\microsoft\cryptography[machineguid]
  Queries value:          HKLM\software\microsoft\windows nt\currentversion[digitalproductid]
  Queries value:          HKLM\software\microsoft\windows nt\currentversion[digitalproductid4]
  Queries value:          HKLM\software\clients\startmenuinternet[]
  Queries value:          HKLM\software\microsoft\ole\appcompat[raisedefaultauthnlevel]
  Queries value:          HKLM\software\microsoft\ole[defaultaccesspermission]
  Queries value:          HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]
  Queries value:          HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider[type]
  Queries value:          HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider[image path]
  Queries value:          HKLM\system\currentcontrolset\control\session
manager[safeprocesssearchmode]
  Queries value:          HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
  Queries value:          HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
  Queries value:          HKLM\software\policies\microsoft\cryptography[privkeycachemaxitems]
  Queries value:
HKLM\software\policies\microsoft\cryptography[privkeycachepurgeintervalseconds]
  Queries value:          HKLM\software\policies\microsoft\cryptography[privatekeylifetimeseconds]
  Queries value:          HKCR\interface\{00000134-0000-0000-c000-000000000046}\proxystubclsid32[]
  Queries value:          HKLM\software\microsoft\rpc\extensions[ndroleextdll]
  Queries value:          HKLM\software\microsoft\rpc\extensions[remoterpcdll]
  Queries value:          HKLM\software\microsoft\sqmclient\windows\disabledprocesses[4c9167ef]
  Queries value:
HKLM\software\microsoft\sqmclient\windows\disabledsessions[machinethrottling]
  Queries value:
HKLM\software\microsoft\sqmclient\windows\disabledsessions[globalsession]
  Queries value:          HKLM\software\microsoft\ole[maxsxshashcount]
  Queries value:          HKLM\software\microsoft\windows\currentversion\internet
settings\winhttp\tracing[enabled]
  Queries value:          HKLM\software\microsoft\windows\currentversion\internet
settings[sharecredswithwinhttp]
  Queries value:          HKLM\software\microsoft\windows\currentversion\internet
settings\winhttp[disablebranchcache]
  Queries value:          HKLM\software\policies\microsoft\windows\currentversion\internet
settings[proxysettingsperuser]
  Queries value:          HKCU\software\microsoft\windows\currentversion\internet
settings\connections[defaultconnectionsettings]
  Queries value:          HKCU\software\microsoft\windows\currentversion\internet
settings\wpad[wpadoverride]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
  Queries value:          HKCU\control panel\international[localename]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[namespace_callout]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007[packedcatalogitem]
```

```
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000012[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000013[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000014[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000015[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000016[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000017[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000018[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[librarypath]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[displaystring]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerid]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[addressfamily]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[supportednamespace]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[enabled]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[storesserviceclassinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[librarypath]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[displaystring]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerid]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[addressfamily]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[supportednamespace]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[enabled]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[storesserviceclassinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[librarypath]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[displaystring]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerid]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[addressfamily]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[supportednamespace]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[enabled]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[storesserviceclassinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[librarypath]
  Queries value:
```

```
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[displaystring]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[providerid]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[addressfamily]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[supportednamespace]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[enabled]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[version]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[storesserviceclassinfo]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[providerinfo]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[librarypath]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[displaystring]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[providerid]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[addressfamily]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[supportednamespace]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[enabled]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[version]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[storesserviceclassinfo]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[providerinfo]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[librarypath]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[displaystring]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[providerid]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[addressfamily]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[supportednamespace]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[enabled]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[version]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[storesserviceclassinfo]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[providerinfo]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32spincount]
   Queries value:            HKLM\system\currentcontrolset\control\cmf\config[system]
   Queries value:
HKLM\system\currentcontrolset\control\lsaextensionconfig\sspicli[checksignaturedll]
   Queries value:
HKLM\system\currentcontrolset\control\lsaextensionconfig\sspicli[checksignatureroutine]
   Queries value:
HKLM\system\currentcontrolset\control\securityproviders[securityproviders]
   Queries value:            HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[name]
   Queries value:            HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[comment]
   Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[capabilities]
   Queries value:            HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[rpcid]
   Queries value:            HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[version]
   Queries value:            HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[type]
   Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[tokensize]
   Queries value:            HKLM\software\microsoft\ole[maximumallowedallocationsize]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[nameserver]
```