Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 3330, Task ID: 830

Task ID: Risk Level: 10

Date Processed: 2016-05-18 10:43:47 (UTC)

Processing Time: 62.59 seconds IntelliVM Virtual Environment:

Execution Arguments: "c:\windows\temp\1b213953a4baf79fadfe9968cf3a1446.exe"

Sample ID: Type: admin Owner:

1b213953a4baf79fadfe9968cf3a1446 Label:

Date Added: 2016-05-18 10:30:51 (UTC)

File Type: PE32:win32:gui File Size: 565248 bytes

1b213953a4baf79fadfe9968cf3a1446 MD5:

3de393336565e1e6d500ce152e99281a2e3d785c3c41dc1a2f0c7b242c134e57 SHA256:

Description: None

Pattern Matching Results

10 Resolves malicious domain: Fosniw trojan

4 Checks whether debugger is present

1 HTTP connection - response code 404 (file not found)

Process/Thread Events

C:\windows\temp\1b213953a4baf79fadfe9968cf3a1446.exe Creates process:

["C:\windows\temp\1b213953a4baf79fadfe9968cf3a1446.exe"]

Named Object Events

Creates mutex \Sessions\1\BaseNamedObjects\DBWinMutex Creates event: \BaseNamedObjects\SvcctrlStartEvent_A3752DX

Creates event: \BaseNamedObjects\BFE_Notify_Event_{9c43605b-4953-4a5c-af27-

2e2acaa3de19}

File System Events

Opens: C:\Windows\Prefetch\1B213953A4BAF79FADFE9968CF3A1-C996567E.pf

Opens: C:\Windows

Opens: C:\Windows\System32\wow64.dll C:\Windows\System32\wow64win.dll Opens: Opens: C:\Windows\System32\wow64cpu.dll Opens: C:\Windows\system32\wow64log.dll

Opens: C:\Windows\SysWOW64

Opens: C:\Windows\SysWOW64\sechost.dll Opens: C:\windows\temp\NETAPI32.dll C:\Windows\SysWOW64\netapi32.dll Opens: Opens: C:\windows\temp\netutils.dll Opens: C:\Windows\SysWOW64\netutils.dll Opens: C:\windows\temp\srvcli.dll Opens: C:\Windows\SysWOW64\srvcli.dll Opens: C:\windows\temp\wkscli.dll C:\Windows\SysWOW64\wkscli.dll Opens: Opens: C:\Windows\SysWOW64\imm32.dll Opens: C:\Windows\SysWOW64\rpcss.dll

C:\Windows\SysWOW64\uxtheme.dll Opens: Opens: C:\Windows\Globalization\Sorting\SortDefault.nls

Opens: C:\windows\temp\netbios.dll C:\Windows\SysWOW64\netbios.dll Opens: Opens: C:\Windows\SysWOW64\mswsock.dll Opens: C:\Windows\SysWOW64\WSHTCPIP.DLL C:\Windows\SysWOW64\nlaapi.dll Opens: Opens: C:\Windows\SysWOW64\NapiNSP.dll C:\Windows\SysWOW64\pnrpnsp.dll Opens: Opens: C:\windows\temp\DNSAPI.dll Opens: C:\Windows\SysWOW64\dnsapi.dll C:\Windows\SysWOW64\winrnr.dll Opens:

Opens: C:\windows\temp\IPHLPAPI.DLL Opens: C:\Windows\SysWOW64\IPHLPAPI.DLL Opens: C:\windows\temp\WINNSI.DLL Opens: C:\Windows\SysWOW64\winnsi.dll Opens: C:\windows\temp\dhcpcsvc6.DLL Opens: C:\Windows\SysWOW64\dhcpcsvc6.dll Opens: C:\windows\temp\dhcpcsvc.DLL C:\Windows\SysWOW64\dhcpcsvc.dll Opens: C:\Windows\System32\drivers\etc\hosts Opens: Opens: C:\Windows\SysWOW64\FWPUCLNT.DLL Opens: C:\windows\temp\rasadhlp.dll

Opens: C:\Windows\SysWOW64\rasadhlp.dll Reads from: C:\Windows\System32\drivers\etc\hosts

Network Events

DNS query: appx. koreasys1.com DNS query: appx. koreasys2.com DNS query: appx. koreasys3.com DNS query: appx. koreasys3.com DNS query: appx. koreasys4.com DNS query: appx. koreasys5.com DNS query: appx. koreasys5.com DNS query: appx. koreasys6.com DNS query: appx. koreasys8.com DNS query: appx. koreasys9.com DNS query: appx. koreasys9.com DNS query: appx. koreasys10.com DNS query: appx. koreasys11.com DNS query: appx. koreasys11.com DNS query: appx. koreasys13.com DNS query: appx. koreasys14.com DNS query: appx. koreasys17.com DNS query: appx. koreasys17.com DNS query: appx. koreasys17.com DNS query: appx. koreasys17.com DNS query: appx. koreasys18.com DNS query: appx. koreasys18.com DNS query: appx. koreasys19.com DNS query: appx. koreasys19.com DNS query: appx. koreasys20.com DNS query: appx. koreasys21.com DNS query: appx. koreasys22.com DNS query: appx. koreasys21.com DNS query: appx. koreasys21.com DNS query: appx. koreasys22.com DNS query: appx. koreasys21.com DNS query: appx. koreasys21.com DNS query: appx. koreasys22.com DNS query: appx. koreasys21.com DNS query: appx. koreasys21.com DNS query: appx. koreasys22.com DNS query: appx. koreasys23.com DNS query: appx. koreasys23.com DNS query: appx. koreasys23.com DNS query: appx. koreasys31.com DNS query: appx. koreasys31.com DNS query: appx. koreasys31.com DNS query: appx. koreasys31.com DNS query: appx. koreasys33.com
DNS query: appx.koreasys3.com DNS query: appx.koreasys5.com DNS query: appx.koreasys5.com DNS query: appx.koreasys6.com DNS query: appx.koreasys7.com DNS query: appx.koreasys7.com DNS query: appx.koreasys9.com DNS query: appx.koreasys9.com DNS query: appx.koreasys10.com DNS query: appx.koreasys11.com DNS query: appx.koreasys12.com DNS query: appx.koreasys13.com DNS query: appx.koreasys13.com DNS query: appx.koreasys14.com DNS query: appx.koreasys16.com DNS query: appx.koreasys17.com DNS query: appx.koreasys18.com DNS query: appx.koreasys19.com DNS query: appx.koreasys19.com DNS query: appx.koreasys20.com DNS query: appx.koreasys20.com DNS query: appx.koreasys21.com DNS query: appx.koreasys21.com DNS query: appx.koreasys22.com DNS query: appx.koreasys23.com DNS query: appx.koreasys23.com DNS query: appx.koreasys24.com DNS query: appx.koreasys25.com DNS query: appx.koreasys26.com DNS query: appx.koreasys26.com DNS query: appx.koreasys27.com DNS query: appx.koreasys28.com DNS query: appx.koreasys26.com DNS query: appx.koreasys27.com DNS query: appx.koreasys27.com DNS query: appx.koreasys28.com DNS query: appx.koreasys20.com DNS query: appx.koreasys20.com DNS query: appx.koreasys23.com DNS query: appx.koreasys23.com DNS query: appx.koreasys33.com
DNS query: appx.koreasys5.com DNS query: appx.koreasys5.com DNS query: appx.koreasys5.com DNS query: appx.koreasys7.com DNS query: appx.koreasys8.com DNS query: appx.koreasys9.com DNS query: appx.koreasys10.com DNS query: appx.koreasys11.com DNS query: appx.koreasys11.com DNS query: appx.koreasys13.com DNS query: appx.koreasys13.com DNS query: appx.koreasys13.com DNS query: appx.koreasys15.com DNS query: appx.koreasys16.com DNS query: appx.koreasys16.com DNS query: appx.koreasys18.com DNS query: appx.koreasys18.com DNS query: appx.koreasys19.com DNS query: appx.koreasys20.com DNS query: appx.koreasys20.com DNS query: appx.koreasys21.com DNS query: appx.koreasys21.com DNS query: appx.koreasys21.com DNS query: appx.koreasys23.com DNS query: appx.koreasys23.com DNS query: appx.koreasys24.com DNS query: appx.koreasys25.com DNS query: appx.koreasys25.com DNS query: appx.koreasys26.com DNS query: appx.koreasys27.com DNS query: appx.koreasys27.com DNS query: appx.koreasys28.com DNS query: appx.koreasys23.com DNS query: appx.koreasys23.com DNS query: appx.koreasys33.com
DNS query: appx.koreasys5.com DNS query: appx.koreasys6.com DNS query: appx.koreasys7.com DNS query: appx.koreasys8.com DNS query: appx.koreasys9.com DNS query: appx.koreasys9.com DNS query: appx.koreasys10.com DNS query: appx.koreasys11.com DNS query: appx.koreasys12.com DNS query: appx.koreasys13.com DNS query: appx.koreasys13.com DNS query: appx.koreasys15.com DNS query: appx.koreasys15.com DNS query: appx.koreasys17.com DNS query: appx.koreasys17.com DNS query: appx.koreasys17.com DNS query: appx.koreasys19.com DNS query: appx.koreasys21.com DNS query: appx.koreasys23.com DNS query: appx.koreasys23.com DNS query: appx.koreasys24.com DNS query: appx.koreasys24.com DNS query: appx.koreasys25.com DNS query: appx.koreasys26.com DNS query: appx.koreasys27.com DNS query: appx.koreasys28.com DNS query: appx.koreasys28.com DNS query: appx.koreasys28.com DNS query: appx.koreasys28.com DNS query: appx.koreasys23.com DNS query: appx.koreasys23.com DNS query: appx.koreasys23.com DNS query: appx.koreasys31.com DNS query: appx.koreasys31.com DNS query: appx.koreasys31.com DNS query: appx.koreasys33.com
DNS query: appx.koreasys6.com DNS query: appx.koreasys7.com DNS query: appx.koreasys9.com DNS query: appx.koreasys9.com DNS query: appx.koreasys10.com DNS query: appx.koreasys11.com DNS query: appx.koreasys12.com DNS query: appx.koreasys13.com DNS query: appx.koreasys13.com DNS query: appx.koreasys14.com DNS query: appx.koreasys15.com DNS query: appx.koreasys16.com DNS query: appx.koreasys17.com DNS query: appx.koreasys17.com DNS query: appx.koreasys19.com DNS query: appx.koreasys20.com DNS query: appx.koreasys21.com DNS query: appx.koreasys22.com DNS query: appx.koreasys22.com DNS query: appx.koreasys23.com DNS query: appx.koreasys23.com DNS query: appx.koreasys24.com DNS query: appx.koreasys25.com DNS query: appx.koreasys25.com DNS query: appx.koreasys25.com DNS query: appx.koreasys26.com DNS query: appx.koreasys27.com DNS query: appx.koreasys23.com DNS query: appx.koreasys23.com DNS query: appx.koreasys31.com DNS query: appx.koreasys31.com DNS query: appx.koreasys33.com
DNS query: appx.koreasys6.com DNS query: appx.koreasys7.com DNS query: appx.koreasys9.com DNS query: appx.koreasys9.com DNS query: appx.koreasys10.com DNS query: appx.koreasys11.com DNS query: appx.koreasys12.com DNS query: appx.koreasys13.com DNS query: appx.koreasys13.com DNS query: appx.koreasys14.com DNS query: appx.koreasys15.com DNS query: appx.koreasys16.com DNS query: appx.koreasys17.com DNS query: appx.koreasys17.com DNS query: appx.koreasys19.com DNS query: appx.koreasys20.com DNS query: appx.koreasys21.com DNS query: appx.koreasys22.com DNS query: appx.koreasys22.com DNS query: appx.koreasys23.com DNS query: appx.koreasys23.com DNS query: appx.koreasys24.com DNS query: appx.koreasys25.com DNS query: appx.koreasys25.com DNS query: appx.koreasys25.com DNS query: appx.koreasys26.com DNS query: appx.koreasys27.com DNS query: appx.koreasys23.com DNS query: appx.koreasys23.com DNS query: appx.koreasys31.com DNS query: appx.koreasys31.com DNS query: appx.koreasys33.com
DNS query: appx.koreasys7.com DNS query: appx.koreasys8.com DNS query: appx.koreasys8.com DNS query: appx.koreasys10.com DNS query: appx.koreasys11.com DNS query: appx.koreasys12.com DNS query: appx.koreasys13.com DNS query: appx.koreasys13.com DNS query: appx.koreasys14.com DNS query: appx.koreasys15.com DNS query: appx.koreasys15.com DNS query: appx.koreasys15.com DNS query: appx.koreasys17.com DNS query: appx.koreasys17.com DNS query: appx.koreasys19.com DNS query: appx.koreasys19.com DNS query: appx.koreasys20.com DNS query: appx.koreasys21.com DNS query: appx.koreasys22.com DNS query: appx.koreasys22.com DNS query: appx.koreasys22.com DNS query: appx.koreasys23.com DNS query: appx.koreasys25.com DNS query: appx.koreasys25.com DNS query: appx.koreasys27.com DNS query: appx.koreasys29.com DNS query: appx.koreasys29.com DNS query: appx.koreasys21.com DNS query: appx.koreasys23.com DNS query: appx.koreasys31.com DNS query: appx.koreasys31.com DNS query: appx.koreasys31.com DNS query: appx.koreasys31.com DNS query: appx.koreasys33.com
DNS query: appx.koreasys8.com DNS query: appx.koreasys9.com DNS query: appx.koreasys11.com DNS query: appx.koreasys11.com DNS query: appx.koreasys13.com DNS query: appx.koreasys13.com DNS query: appx.koreasys13.com DNS query: appx.koreasys14.com DNS query: appx.koreasys15.com DNS query: appx.koreasys16.com DNS query: appx.koreasys17.com DNS query: appx.koreasys18.com DNS query: appx.koreasys19.com DNS query: appx.koreasys20.com DNS query: appx.koreasys21.com DNS query: appx.koreasys21.com DNS query: appx.koreasys22.com DNS query: appx.koreasys23.com DNS query: appx.koreasys24.com DNS query: appx.koreasys24.com DNS query: appx.koreasys24.com DNS query: appx.koreasys25.com DNS query: appx.koreasys27.com DNS query: appx.koreasys26.com DNS query: appx.koreasys27.com DNS query: appx.koreasys28.com DNS query: appx.koreasys29.com DNS query: appx.koreasys30.com DNS query: appx.koreasys31.com DNS query: appx.koreasys33.com
DNS query: appx.koreasys10.com DNS query: appx.koreasys11.com DNS query: appx.koreasys11.com DNS query: appx.koreasys13.com DNS query: appx.koreasys13.com DNS query: appx.koreasys14.com DNS query: appx.koreasys15.com DNS query: appx.koreasys15.com DNS query: appx.koreasys16.com DNS query: appx.koreasys16.com DNS query: appx.koreasys19.com DNS query: appx.koreasys19.com DNS query: appx.koreasys20.com DNS query: appx.koreasys21.com DNS query: appx.koreasys22.com DNS query: appx.koreasys22.com DNS query: appx.koreasys23.com DNS query: appx.koreasys24.com DNS query: appx.koreasys25.com DNS query: appx.koreasys26.com DNS query: appx.koreasys27.com DNS query: appx.koreasys26.com DNS query: appx.koreasys27.com DNS query: appx.koreasys28.com DNS query: appx.koreasys29.com DNS query: appx.koreasys29.com DNS query: appx.koreasys31.com DNS query: appx.koreasys31.com DNS query: appx.koreasys31.com DNS query: appx.koreasys33.com
DNS query: appx.koreasys10.com DNS query: appx.koreasys11.com DNS query: appx.koreasys12.com DNS query: appx.koreasys13.com DNS query: appx.koreasys14.com DNS query: appx.koreasys15.com DNS query: appx.koreasys16.com DNS query: appx.koreasys17.com DNS query: appx.koreasys17.com DNS query: appx.koreasys19.com DNS query: appx.koreasys20.com DNS query: appx.koreasys21.com DNS query: appx.koreasys21.com DNS query: appx.koreasys22.com DNS query: appx.koreasys22.com DNS query: appx.koreasys23.com DNS query: appx.koreasys24.com DNS query: appx.koreasys26.com DNS query: appx.koreasys26.com DNS query: appx.koreasys27.com DNS query: appx.koreasys27.com DNS query: appx.koreasys28.com DNS query: appx.koreasys29.com DNS query: appx.koreasys29.com DNS query: appx.koreasys29.com DNS query: appx.koreasys30.com DNS query: appx.koreasys31.com DNS query: appx.koreasys31.com DNS query: appx.koreasys33.com
DNS query: appx.koreasys11.com DNS query: appx.koreasys12.com DNS query: appx.koreasys13.com DNS query: appx.koreasys14.com DNS query: appx.koreasys15.com DNS query: appx.koreasys15.com DNS query: appx.koreasys16.com DNS query: appx.koreasys17.com DNS query: appx.koreasys19.com DNS query: appx.koreasys19.com DNS query: appx.koreasys20.com DNS query: appx.koreasys21.com DNS query: appx.koreasys22.com DNS query: appx.koreasys22.com DNS query: appx.koreasys23.com DNS query: appx.koreasys24.com DNS query: appx.koreasys25.com DNS query: appx.koreasys25.com DNS query: appx.koreasys26.com DNS query: appx.koreasys27.com DNS query: appx.koreasys28.com DNS query: appx.koreasys28.com DNS query: appx.koreasys29.com DNS query: appx.koreasys29.com DNS query: appx.koreasys30.com DNS query: appx.koreasys31.com DNS query: appx.koreasys331.com
DNS query: appx.koreasys12.com DNS query: appx.koreasys13.com DNS query: appx.koreasys14.com DNS query: appx.koreasys15.com DNS query: appx.koreasys16.com DNS query: appx.koreasys17.com DNS query: appx.koreasys17.com DNS query: appx.koreasys19.com DNS query: appx.koreasys19.com DNS query: appx.koreasys20.com DNS query: appx.koreasys21.com DNS query: appx.koreasys22.com DNS query: appx.koreasys23.com DNS query: appx.koreasys23.com DNS query: appx.koreasys24.com DNS query: appx.koreasys25.com DNS query: appx.koreasys25.com DNS query: appx.koreasys26.com DNS query: appx.koreasys27.com DNS query: appx.koreasys27.com DNS query: appx.koreasys28.com DNS query: appx.koreasys29.com DNS query: appx.koreasys31.com DNS query: appx.koreasys31.com DNS query: appx.koreasys33.com
DNS query: appx.koreasys13.com DNS query: appx.koreasys15.com DNS query: appx.koreasys16.com DNS query: appx.koreasys17.com DNS query: appx.koreasys17.com DNS query: appx.koreasys18.com DNS query: appx.koreasys19.com DNS query: appx.koreasys20.com DNS query: appx.koreasys21.com DNS query: appx.koreasys21.com DNS query: appx.koreasys22.com DNS query: appx.koreasys23.com DNS query: appx.koreasys24.com DNS query: appx.koreasys24.com DNS query: appx.koreasys25.com DNS query: appx.koreasys26.com DNS query: appx.koreasys27.com DNS query: appx.koreasys27.com DNS query: appx.koreasys28.com DNS query: appx.koreasys28.com DNS query: appx.koreasys29.com DNS query: appx.koreasys30.com DNS query: appx.koreasys31.com DNS query: appx.koreasys31.com DNS query: appx.koreasys33.com
DNS query: appx.koreasys14.com DNS query: appx.koreasys15.com DNS query: appx.koreasys16.com DNS query: appx.koreasys17.com DNS query: appx.koreasys18.com DNS query: appx.koreasys19.com DNS query: appx.koreasys20.com DNS query: appx.koreasys20.com DNS query: appx.koreasys21.com DNS query: appx.koreasys21.com DNS query: appx.koreasys22.com DNS query: appx.koreasys23.com DNS query: appx.koreasys24.com DNS query: appx.koreasys25.com DNS query: appx.koreasys25.com DNS query: appx.koreasys26.com DNS query: appx.koreasys27.com DNS query: appx.koreasys28.com DNS query: appx.koreasys28.com DNS query: appx.koreasys29.com DNS query: appx.koreasys21.com DNS query: appx.koreasys30.com DNS query: appx.koreasys31.com DNS query: appx.koreasys31.com DNS query: appx.koreasys32.com DNS query: appx.koreasys33.com
DNS query: appx.koreasys15.com DNS query: appx.koreasys16.com DNS query: appx.koreasys17.com DNS query: appx.koreasys18.com DNS query: appx.koreasys19.com DNS query: appx.koreasys20.com DNS query: appx.koreasys21.com DNS query: appx.koreasys22.com DNS query: appx.koreasys23.com DNS query: appx.koreasys23.com DNS query: appx.koreasys24.com DNS query: appx.koreasys25.com DNS query: appx.koreasys25.com DNS query: appx.koreasys26.com DNS query: appx.koreasys27.com DNS query: appx.koreasys28.com DNS query: appx.koreasys29.com DNS query: appx.koreasys29.com DNS query: appx.koreasys29.com DNS query: appx.koreasys30.com DNS query: appx.koreasys31.com DNS query: appx.koreasys31.com DNS query: appx.koreasys33.com
DNS query: appx.koreasys16.com DNS query: appx.koreasys17.com DNS query: appx.koreasys18.com DNS query: appx.koreasys19.com DNS query: appx.koreasys20.com DNS query: appx.koreasys21.com DNS query: appx.koreasys21.com DNS query: appx.koreasys23.com DNS query: appx.koreasys24.com DNS query: appx.koreasys24.com DNS query: appx.koreasys25.com DNS query: appx.koreasys26.com DNS query: appx.koreasys27.com DNS query: appx.koreasys27.com DNS query: appx.koreasys28.com DNS query: appx.koreasys29.com DNS query: appx.koreasys29.com DNS query: appx.koreasys30.com DNS query: appx.koreasys31.com DNS query: appx.koreasys31.com DNS query: appx.koreasys31.com DNS query: appx.koreasys32.com DNS query: appx.koreasys33.com DNS query: appx.koreasys33.com DNS query: appx.koreasys33.com DNS query: appx.koreasys33.com DNS query: appx.koreasys34.com
DNS query: appx.koreasys17.com DNS query: appx.koreasys19.com DNS query: appx.koreasys20.com DNS query: appx.koreasys21.com DNS query: appx.koreasys21.com DNS query: appx.koreasys22.com DNS query: appx.koreasys23.com DNS query: appx.koreasys24.com DNS query: appx.koreasys25.com DNS query: appx.koreasys25.com DNS query: appx.koreasys26.com DNS query: appx.koreasys27.com DNS query: appx.koreasys28.com DNS query: appx.koreasys28.com DNS query: appx.koreasys29.com DNS query: appx.koreasys30.com DNS query: appx.koreasys31.com DNS query: appx.koreasys31.com DNS query: appx.koreasys32.com DNS query: appx.koreasys33.com DNS query: appx.koreasys34.com
DNS query: appx.koreasys18.com DNS query: appx.koreasys20.com DNS query: appx.koreasys21.com DNS query: appx.koreasys21.com DNS query: appx.koreasys22.com DNS query: appx.koreasys23.com DNS query: appx.koreasys24.com DNS query: appx.koreasys25.com DNS query: appx.koreasys25.com DNS query: appx.koreasys26.com DNS query: appx.koreasys27.com DNS query: appx.koreasys27.com DNS query: appx.koreasys28.com DNS query: appx.koreasys29.com DNS query: appx.koreasys29.com DNS query: appx.koreasys30.com DNS query: appx.koreasys31.com DNS query: appx.koreasys31.com DNS query: appx.koreasys32.com DNS query: appx.koreasys33.com DNS query: appx.koreasys33.com DNS query: appx.koreasys33.com DNS query: appx.koreasys33.com DNS query: appx.koreasys34.com
DNS query: appx.koreasys19.com DNS query: appx.koreasys21.com DNS query: appx.koreasys21.com DNS query: appx.koreasys22.com DNS query: appx.koreasys23.com DNS query: appx.koreasys24.com DNS query: appx.koreasys25.com DNS query: appx.koreasys26.com DNS query: appx.koreasys26.com DNS query: appx.koreasys27.com DNS query: appx.koreasys27.com DNS query: appx.koreasys28.com DNS query: appx.koreasys29.com DNS query: appx.koreasys30.com DNS query: appx.koreasys31.com DNS query: appx.koreasys31.com DNS query: appx.koreasys32.com DNS query: appx.koreasys33.com DNS query: appx.koreasys34.com
DNS query: appx.koreasys20.com DNS query: appx.koreasys21.com DNS query: appx.koreasys22.com DNS query: appx.koreasys23.com DNS query: appx.koreasys24.com DNS query: appx.koreasys25.com DNS query: appx.koreasys26.com DNS query: appx.koreasys27.com DNS query: appx.koreasys27.com DNS query: appx.koreasys28.com DNS query: appx.koreasys29.com DNS query: appx.koreasys29.com DNS query: appx.koreasys30.com DNS query: appx.koreasys31.com DNS query: appx.koreasys31.com DNS query: appx.koreasys32.com DNS query: appx.koreasys33.com DNS query: appx.koreasys34.com
DNS query: appx.koreasys21.com DNS query: appx.koreasys23.com DNS query: appx.koreasys23.com DNS query: appx.koreasys24.com DNS query: appx.koreasys25.com DNS query: appx.koreasys26.com DNS query: appx.koreasys27.com DNS query: appx.koreasys27.com DNS query: appx.koreasys28.com DNS query: appx.koreasys29.com DNS query: appx.koreasys29.com DNS query: appx.koreasys30.com DNS query: appx.koreasys31.com DNS query: appx.koreasys32.com DNS query: appx.koreasys32.com DNS query: appx.koreasys33.com DNS query: appx.koreasys33.com DNS query: appx.koreasys33.com DNS query: appx.koreasys34.com
DNS query: appx.koreasys22.com DNS query: appx.koreasys24.com DNS query: appx.koreasys24.com DNS query: appx.koreasys25.com DNS query: appx.koreasys26.com DNS query: appx.koreasys27.com DNS query: appx.koreasys27.com DNS query: appx.koreasys28.com DNS query: appx.koreasys29.com DNS query: appx.koreasys29.com DNS query: appx.koreasys30.com DNS query: appx.koreasys31.com DNS query: appx.koreasys32.com DNS query: appx.koreasys32.com DNS query: appx.koreasys33.com DNS query: appx.koreasys33.com DNS query: appx.koreasys33.com DNS query: appx.koreasys34.com
DNS query: appx.koreasys23.com DNS query: appx.koreasys24.com DNS query: appx.koreasys25.com DNS query: appx.koreasys26.com DNS query: appx.koreasys27.com DNS query: appx.koreasys28.com DNS query: appx.koreasys28.com DNS query: appx.koreasys29.com DNS query: appx.koreasys30.com DNS query: appx.koreasys31.com DNS query: appx.koreasys31.com DNS query: appx.koreasys32.com DNS query: appx.koreasys33.com DNS query: appx.koreasys33.com DNS query: appx.koreasys33.com DNS query: appx.koreasys34.com
DNS query: appx.koreasys24.com DNS query: appx.koreasys25.com DNS query: appx.koreasys26.com DNS query: appx.koreasys27.com DNS query: appx.koreasys28.com DNS query: appx.koreasys28.com DNS query: appx.koreasys29.com DNS query: appx.koreasys30.com DNS query: appx.koreasys31.com DNS query: appx.koreasys31.com DNS query: appx.koreasys32.com DNS query: appx.koreasys33.com DNS query: appx.koreasys33.com DNS query: appx.koreasys34.com
DNS query: appx.koreasys25.com DNS query: appx.koreasys26.com DNS query: appx.koreasys27.com DNS query: appx.koreasys28.com DNS query: appx.koreasys29.com DNS query: appx.koreasys29.com DNS query: appx.koreasys30.com DNS query: appx.koreasys31.com DNS query: appx.koreasys31.com DNS query: appx.koreasys32.com DNS query: appx.koreasys33.com DNS query: appx.koreasys33.com DNS query: appx.koreasys34.com
DNS query: appx.koreasys26.com DNS query: appx.koreasys27.com DNS query: appx.koreasys28.com DNS query: appx.koreasys29.com DNS query: appx.koreasys30.com DNS query: appx.koreasys31.com DNS query: appx.koreasys31.com DNS query: appx.koreasys32.com DNS query: appx.koreasys33.com DNS query: appx.koreasys33.com DNS query: appx.koreasys33.com DNS query: appx.koreasys34.com
DNS query: appx.koreasys27.com DNS query: appx.koreasys28.com DNS query: appx.koreasys29.com DNS query: appx.koreasys30.com DNS query: appx.koreasys31.com DNS query: appx.koreasys31.com DNS query: appx.koreasys32.com DNS query: appx.koreasys33.com DNS query: appx.koreasys33.com DNS query: appx.koreasys34.com
DNS query: appx.koreasys28.com DNS query: appx.koreasys29.com DNS query: appx.koreasys30.com DNS query: appx.koreasys31.com DNS query: appx.koreasys32.com DNS query: appx.koreasys32.com DNS query: appx.koreasys33.com DNS query: appx.koreasys33.com DNS query: appx.koreasys34.com
DNS query: appx.koreasys29.com DNS query: appx.koreasys30.com DNS query: appx.koreasys31.com DNS query: appx.koreasys32.com DNS query: appx.koreasys33.com DNS query: appx.koreasys33.com DNS query: appx.koreasys34.com
DNS query: appx.koreasys30.com DNS query: appx.koreasys31.com DNS query: appx.koreasys32.com DNS query: appx.koreasys33.com DNS query: appx.koreasys33.com DNS query: appx.koreasys34.com
DNS query: appx.koreasys31.com DNS query: appx.koreasys32.com DNS query: appx.koreasys33.com DNS query: appx.koreasys34.com
DNS query: appx.koreasys32.com DNS query: appx.koreasys33.com DNS query: appx.koreasys34.com
DNS query: appx.koreasys33.com DNS query: appx.koreasys34.com
DNS query: appx.koreasys34.com
DNS query: appx.koreasys35.com
DNS query: appx.koreasys36.com
DNS query: appx.koreasys37.com
DNS query: appx.koreasys38.com
DNS query: appx.koreasys39.com
DNS query: appx.koreasys40.com
DNS query: appx.koreasys41.com
DNS query: appx.koreasys42.com
DNS query: appx.koreasys43.com
DNS response: appx.koreasys1.com \Rightarrow 208.100.26.234
DNS response: $appx.koreasys3.com \Rightarrow 200.700.200.204$ DNS response: $appx.koreasys3.com \Rightarrow 109.74.196.143$
DNS response: appx.koreasys4.com \Rightarrow 192.155.89.148
Connects to: 208.100.26.234:80
Connects to: 200.100.26.234.80
Connects to: 0.0.0.0.80 Connects to: 109.74.196.143:80
Sends data to: 0.0.0.0:0 Receives data from: 8.8.8.8:53
Receives data from: appx.koreasys1.com:80 (208.100.26.234)

Windows Pogistry Events

Windows Registry Events		
Creates key:	HKLM\system\currentcontrolset\services\tcpip\parameters	
Opens key:	<pre>HKLM\software\microsoft\windows nt\currentversion\image file execution</pre>	
options		
Opens key:	HKLM\system\currentcontrolset\control\session manager	
Opens key:	HKLM\software\microsoft\wow64	
Opens key:	HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file	
execution options		
Opens key:	HKLM\system\currentcontrolset\control\safeboot\option	
Opens key:	<pre>HKLM\system\currentcontrolset\control\srp\gp\dll</pre>	
Opens key:		
HKLM\software\wow6	5432node\policies\microsoft\windows\safer\codeidentifiers	
Opens key:	<pre>HKLM\software\policies\microsoft\windows\safer\codeidentifiers</pre>	
Opens key:	<pre>HKCU\software\policies\microsoft\windows\safer\codeidentifiers</pre>	
Opens key:	<pre>HKLM\system\currentcontrolset\control\nls\customlocale</pre>	
Opens key:	<pre>HKLM\system\currentcontrolset\control\nls\language</pre>	
Opens key:	<pre>HKLM\system\currentcontrolset\control\mui\uilanguages</pre>	
Opens key:	<pre>HKLM\system\currentcontrolset\control\mui\uilanguages\en-us</pre>	
Opens key:	HKLM\system\currentcontrolset\control\mui\uilanguages\pendingdelete	

Opens key:

Opens key: HKLM\software\wow6432node\policies\microsoft\mui\settings

Opens key: ${\tt HKLM \backslash software \backslash policies \backslash \dot{m} icrosoft \backslash mui \backslash settings}$

Opens key:

Opens key: $\label{thm:local_machine} \begin{tabular}{ll} HKCU\control panel\desktop\muicached\machinelanguageconfiguration \\ \end{tabular}$

HKLM\system\currentcontrolset\control\mui\settings\languageconfiguration Opens key: Opens key: HKCU\software\policies\microsoft\control panel\desktop Opens kev: HKCU\control panel\desktop\languageconfiguration HKCU\control panel\desktop Opens key: Opens key: HKCU\control panel\desktop\muicached Opens key: $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ side by side$ HKLM\system\currentcontrolset\control\nls\sorting\versions Opens key: Opens key: HKLM\ Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\diagnostics HKLM\software\wow6432node\microsoft\windows Opens kev: nt\currentversion\gre_initialize Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\compatibility32 Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\ime compatibility HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows Opens kev: Opens key: HKLM\software\wow6432node\microsoft\ole Opens key: HKLM\software\wow6432node\microsoft\ole\tracing Opens key: HKLM\software\microsoft\ole\tracing Opens key: HKLM\system\currentcontrolset\services\lanmanworkstation\parameters Opens key: HKLM\software\policies\microsoft\sqmclient\windows Opens kev: HKLM\software\microsoft\samclient\windows Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters Opens key: Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\043dd211 Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9 Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000005 HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries Opens kev: Opens kev: Opens kev: Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006 Opens key: Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008 Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000000 Opens key: Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5 Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000028 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries Opens key: Opens key: Opens key: Opens key: Opens key:

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006

HKCU\software\545c7be91acf Opens kev:

Opens key: HKLM\system\currentcontrolset\services\winsock\parameters Opens key: HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock Opens kev: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock Opens key: HKLM\system\currentcontrolset\services\winsock\setup migration\providers

Opens key: HKLM\system\currentcontrolset\services\winsock\setup

migration\providers\tcpip

HKLM\software\wow6432node\microsoft\rpc Opens key:

Opens key: ${\tt HKLM \ } system \verb|\ current control \ \\ computer name \verb|\ active computer name \ \\$

Opens key: HKLM\svstem\setup

Opens key: HKLM\software\wow6432node\policies\microsoft\windows nt\rpc

```
Opens key:
                                               HKLM\software\policies\microsoft\windows nt\rpc
   Opens key:
                                               HKLM\system\currentcontrolset\services\dnscache\parameters
   Opens kev:
                                               HKLM\software\wow6432node\policies\microsoft\windows nt\dnsclient
                                               HKLM\software\policies\microsoft\windows nt\dnsclient
   Opens key:
   Opens key:
                                              HKLM\software\wow6432node\policies\microsoft\system\dnsclient
   Opens key:
                                              HKLM\software\policies\microsoft\system\dnsclient
   Opens key:
                                               HKLM\system\currentcontrolset\control\sqmservicelist
                                               \begin{tabular}{ll} \textbf{HKLM} & \textbf{system} \\ \textbf{currentcontrolset} \\ \textbf{services} \\ \textbf{dnscache} \\ \textbf{parameters} \\ \textbf{dnscache} \\ \end{tabular}
   Opens key:
   Opens key:
                                               HKLM\system\currentcontrolset\services\dns
   Opens key:
                                               HKLM\software\wow6432node\policies\microsoft\windows
nt\dnsclient\dnspolicyconfig
   Opens key:
                                              HKLM\software\policies\microsoft\windows nt\dnsclient\dnspolicyconfig
   Opens key:
HKLM\system\currentcontrolset\services\dnscache\parameters\dnspolicyconfig
   Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}
   Opens key:
                                               HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces
   Opens key:
e1e01c1f69b5}
   Opens key:
HKLM \ system \ current control set \ services \ tcpip \ harameters \ interfaces \ \{846ee 342-7039-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-9d20-11de-
806e6f6e6963}
   Opens key:
806e6f6e6963}
   Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{a91d0a5e-390e-4979-9c38-
127795cce47a}
   Opens kev:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b9ec5865-2d36-4cb8-b474-
65fee5bae0b1}
   Opens key:
                                               HKLM\system\currentcontrolset\services\tcpip\linkage
   Oueries value:
                                              HKLM\software\microsoft\windows nt\currentversion\image file execution
options[disableusermodecallbackfilter]
                                              HKLM\system\currentcontrolset\control\session
   Oueries value:
manager[cwdillegalindllsearch]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
   Oueries value:
                                              HKLM\system\currentcontrolset\control\nls\customlocale[empty]
   Queries value:
HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback]
                                              HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type]
   Queries value:
                                              HKLM\system\currentcontrolset\control\mui\uilanguages\en-
   Oueries value:
us[alternatecodepage]
   Queries value:
                                              HKCU\control panel\desktop[preferreduilanguages]
   Queries value:
                                              HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
   Oueries value:
HKLM \label{lem:hklm} White the latest of 
                                              HKLM\system\currentcontrolset\control\nls\sorting\versions[]
   Oueries value:
                                              HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
   Oueries value:
   Queries value:
                                              HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
                                              HKLM\software\wow6432node\microsoft\windows
   Oueries value:
nt\currentversion\compatibility32[1b213953a4baf79fadfe9968cf3a1446]
                                              HKLM\software\wow6432node\microsoft\windows
   Oueries value:
nt\currentversion\windows[loadappinit_dlls]
                                              HKLM\software\microsoft\ole[pageallocatorusesystemheap]
   Oueries value:
                                              HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
   Queries value:
   Queries value:
HKLM\software\microsoft\sqmclient\windows[ceipenable]
   Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
                                               HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
   Oueries value:
   Queries value:
                                              HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
   Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[namespace_callout]
   Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
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]
   Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000001[packedcatalogitem]
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
   Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem]
   Oueries value:
```

Oueries value:

- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007[packedcatalogitem] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem] Oueries 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]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[librarypath]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[displaystring]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerid]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[addressfamily]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[supportednamespace]
 Queries value:
- $\label{lem:hklmsystem} HKLM \system \current controls et \services \winsock 2 \parameters \namespace_catalog 5 \catalog_entries \namespace_catal$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[version]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[storesserviceclassinfo]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[providerinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[librarypath]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[displaystring]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerid]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[addressfamily]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000002[supportednamespace]
 Oueries 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]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000002[storesserviceclassinfo]
 Oueries 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]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[displaystring]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[providerid]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[addressfamily]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[supportednamespace]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[enabled]
 Oueries value:
- $\label{lem:hklmsystem} HKLM \system \current controls et \services \winsock 2 \parameters \namespace_catalog 5 \catalog_entries \namespace_catal$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[storesserviceclassinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[providerinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[librarypath]
 Queries value:
- $\label{lem:hklmsystem} Hklm\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000004[displaystring] \\ Queries\ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000004[providerid]
 Oueries 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\0000000000004[supportednamespace]
 Queries value:
- $\label{lem:hklmsystem} HKLM \system \current controls et \services \winsock 2 \parameters \names pace_catalog 5 \catalog_entries \names \pace_catalog 5 \catalog_entries \pace_catalog 5 \catalog 6 \catalog 6 \catalog 6 \catalog 6 \catalog 6 \c$

```
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus namespace\_catalog 5 \setminus catalog\_entries \setminus 0000000000004 [version]
   Oueries value:
```

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog_\catalog_entries\00000000004[storesserviceclassinfo] Queries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus namespace_catalog \\ \setminus catalog_entries \setminus 0000000000004 [provider info]$ Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[librarypath] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[displaystring] Oueries value:

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space_catalog \ services \ winsock 2 \ parameters \ name space_catalog \ services \ winsock 2 \ parameters \ name space_catalog \ services \ winsock 2 \ parameters \ name space_catalog \ services \ winsock 2 \ parameters \ name space_catalog \ services \ winsock 2 \ parameters \ name space_catalog \ services \ winsock 2 \ parameters \ name space_catalog \ services \ winsock 2 \ parameters \ name space_catalog \ services \ winsock 2 \ parameters \ name space_catalog \ services \ name space_catalog \ name space_cat$ Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[addressfamily] Oueries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters \setminus names pace_catalog 5 \setminus catalog_entries \setminus 000000000005[supported names pace]$ Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[enabled] Queries value:

Queries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus namespace_catalog 5 \setminus catalog_entries \setminus 000000000005[storesserviceclass info]$ Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[providerinfo] Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000006[librarypath] Queries value:

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space_catalog 5 \ (catalog_entries \ 0000000000006 \ [displaystring]$ Queries value:

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space_catalog \ services \ winsock 2 \ parameters \ name space_catalog \ services \ winsock 2 \ parameters \ name space_catalog \ services \ winsock 2 \ parameters \ name space_catalog \ services \ winsock 2 \ parameters \ name space_catalog \ services \ winsock 2 \ parameters \ name space_catalog \ services \ winsock 2 \ parameters \ name space_catalog \ services \ winsock 2 \ parameters \ name space_catalog \ services \ winsock 2 \ parameters \ name space_catalog \ services \ name space_catalog \ name space_catalo$

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000006[addressfamily] Queries value:

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space_catalog 5 \ (catalog_entries \ 0000000000006 [supported name space]]$ Queries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap services \setminus catalog \le catalog \le catalog \le catalog = not in the control set \setminus services \setminus catalog \le catalo$

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000006[version] Queries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap amespace_catalog \\ \ \setminus catalog_entries \setminus 0000000000006[storesserviceclass info]$ Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]

Queries value: HKLM\system\currentcontrolset\services\winsock\parameters[transports]

HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[mapping]

Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]

HKLM\system\currentcontrolset\services\winsock\setup Queries value:

migration\providers\tcpip[winsock 2.0 provider id]

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]

Oueries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength] Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance]

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]

HKLM\software\microsoft\rpc[maxrpcsize] Oueries value:

Oueries value:

HKLM\system\currentcontrolset\control\computername\activecomputername[computername]

HKLM\system\setup[oobeinprogress] Queries value:

Oueries value: HKLM\system\setup[systemsetupinprogress]

HKLM\system\currentcontrolset\services\tcpip\parameters[hostname] Queries value: Oueries value: HKLM\svstem\currentcontrolset\services\tcpip\parameters[domain] Queries value: HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist]

Oueries value:

Queries value:

HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername]

Oueries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname]

HKLM\system\currentcontrolset\services\dnscache\parameters[usedomainnamedevolution]

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution] Oueries value:

Oueries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [prioritize record data]$

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata]

Oueries value:

HKLM\system\currentcontrolset\services\dnscache\parameters[allowunqualifiedquery]

Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[appendtomultilabelname] Oueries value: $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [screen badtlds]$ Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[screenunreachableservers] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[screendefaultservers] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall] HKLM\svstem\currentcontrolset\services\dnscache\parameters[useedns] Oueries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[dnssecurenamequeryfallback] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[enabledaforallnetworks] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[directaccessqueryorder] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching] HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile] Queries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[addrconfigcontrol] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationenabled] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerprimaryname] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername] Oueries value: $HKLM \backslash system \backslash current control set \backslash services \backslash tcpip \backslash parameters [enable adapter domain name registration]$ Queries value: Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerwanadapters] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationrefreshinterval] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationmaxaddresscount] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddressestoregister] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel] Queries value: $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [update top level domain zones]$ Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[downcasespncauseapiowneristoolazy] Queries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize] HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl] Oueries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxnegativecachettl] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[enablemulticast] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[multicastresponderflags] Queries value:

HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsenderflags] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsendermaxtimeout] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest] Oueries value: $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [use compartments]$ Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[cacheallcompartments] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[usenewregistration] Oueries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistrationonly] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquerytimeouts] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquickquerytimeouts] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts] Oueries value: HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{22873b3e-c4d3-495a-8165e1e01c1f69b5}[searchlist] Queries value: e1e01c1f69b5}[enabledhcp] Oueries value: e1e01c1f69b5}[registrationenabled] Queries value: e1e01c1f69b5}[registeradaptername] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165e1e01c1f69b5}[domain] Oueries value: e1e01c1f69b5}[dhcpdomain] Oueries value: HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{22873b3e-c4d3-495a-8165e1e01c1f69b5}[dhcpv6domain] Queries value: HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{22873b3e-c4d3-495a-8165e1e01c1f69b5}[nameserver] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165e1e01c1f69b5}[nameserver] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165e1e01c1f69b5}[dhcpnameserver] Queries value: 806e6f6e6963}[enabledhcp] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[registrationenabled] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[registeradaptername] Oueries value: 806e6f6e6963}[domain] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[dhcpdomain] Queries value: 806e6f6e6963}[nameserver] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[dhcpnameserver] Queries value: HKLM\system\currentcontrolset\services\tcpip\linkage[bind] Queries value: e1e01c1f69b5}[queryadaptername] HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165e1e01c1f69b5}[disableadapterdomainname]

Queries value:

Queries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '\{22873b3e-c4d3-495a-8165-e1e01c1f69b5\} \ [maxnumber of addresses to register]$

Oueries value

 $HKLM \ system \ current controls et \ services \ tcpip \ parameters \ interfaces \ \{22873b3e-c4d3-495a-8165-e1e01c1f69b5\} \ [enablemulticast]$

Queries value:

 $HKLM \ system \ current controls et \ services \ tcpip \ parameters \ interfaces \ \{846ee 342-7039-11de-9d20-806e6f6e6963\} \ [query adapter name]$

Queries value:

 $HKLM \ system \ current controls et \ services \ tcpip \ parameters \ interfaces \ \{846ee 342-7039-11de-9d20-806e6f6e6963\} \ [disable adapter domain name]$

Queries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '\{846ee 342-7039-11de-9d 20-806e6 f 666963\} \ [disable dynamic update]$

Queries value:

 $HKLM \ system \ current controls et \ services \ tcpip \ parameters \ interfaces \ \{846ee 342-7039-11de-9d20-806e6f6e6963\} \ [enable adapter domain name registration]$

Queries value:

 $HKLM \ system \ `current control set \ 's ervices \ 'tcpip \ parameters \ 'interfaces \ '\{846ee 342-7039-11de-9d 20-806e6 f 6e 6963\} \ [registration max address count]$

Oueries value

 $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{846ee 342-7039-11de-9d20-806e6f6e6963\} \ [maxnumber of addresses to register]$

Queries value:

 $\label{thm:hklm} HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{846ee 342-7039-11de-9d 20-806e6 f6e 6963\} \ [enable multicast]$

Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdl]]