VIRUSTOTAL

SUMMARY DETECTION DETAILS RELATIONS BEHAVIOR

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to **automate checks.**

Display grouped sandbox reports

CAPA	0	2	0	0	0	0
CAPE Sandbox	1	6	1	0	0	6
Microsoft Sysinter…	0	0	0	0	0	8
VirusTotal Jujubox	0	0	1	0	0	4
VirusTotal Observer	0	0	0	0	0	2
Zenbox	2	5	1	0	0	3

Activity Summary

Download Artifacts Full Reports Help

2 Detections

2 MALWARE 1 TROJAN

Mitre Signatures

1 LOW 23 INFO

IDS Rules

1 LOW

Sigma Rules

NOT FOUND

Dropped Files

NOT FOUND

Network comms

2 HTTP 2 DNS 8 IP 3 JA3

Behavior Tags

detect-debug-environment long-sleeps obfuscated

Dynamic Analysis Sandbox Detections

⚠ The sandbox CAPE Sandbox flags this file as: MALWARE

⚠ The sandbox Zenbox flags this file as: MALWARE TROJAN

MITRE ATT&CK Tactics and Techniques

Execution TA0002

Persistence TA0003

Privilege Escalation TA0004

Defense Evasion TA0005

Credential Access TA0006

Discovery TA0007

Command and Control TA0011

Malware Behavior Catalog Tree

Anti-Behavioral Analysis OB0001

Collection OB0003

Credential Access OB0005

Defense Evasion OB0006

Persistence OB0012

Privilege Escalation OB0013

Memory OC0002

Data OC0004

Communication OC0006

Capabilities

Open in CAPA explorer

Host-Interaction

Runtime

Load-Code

Data-Manipulation

Crowdsourced IDS rules

⚠ Matches rule ET INFO Observed ZeroSSL SSL/TLS Certificate

Network Communication

HTTP Requests

GET https://api.iqiyi.cn.com/WxAM 200

GET https://open.iqiyi.com/api?url=ILGGMENKAKAKHPCAPKOMFFHLGLAJAJJFEFDEIHBJJJBMDJCAFGKGOMD 200

DNS Resolutions

api.iqiyi.cn.com

www.microsoft.com

IP Traffic

TCP 43.135.9.96:443 (api.iqiyi.cn.com)
TCP 173.194.195.94:443
UDP a83f:8110:0:0:100:0:1800:0:53
UDP 192.168.0.10:137
TCP 20.99.186.246:443
TCP 184.25.191.235:443
TCP 23.216.81.152:80 (www.microsoft.com)
UDP 8.8.8.8:53

JA3 Digests

a0e9f5d64349fb13191bc781f81f42e1
98eaec8c8ef8baab245d0b65f788be91
37f463bf4616ecd445d4a1937da06e19

Memory Pattern Domains

- api.iqiyi.cn.com
- api.iqiyi.cn.com:44
- cevcsca2021.crl.certum.pl
- cevcsca2021.ocsp-certum.com0
- crl.certum.pl
- repository.certum.pl
- sectigo.com
- subca.ocsp-certum.com0
- www.certum.pl
- www.iqiyi.com
- www.iqiyi.comaz
- zerossl.crt.sectigo.com
- zerossl.ocsp.sectigo.com

Memory Pattern Urls

- http://api.iqiyi.cn.com/WxAM
- http://api.iqiyi.cn.com:443/WxAM
- http://cevcsca2021.crl.certum.pl/cevcsca2021.crl0w
- http://cevcsca2021.ocsp-certum.com07
- http://crl.certum.pl/ctnca.crl0k
- http://crl.certum.pl/ctnca2.crl0l
- http://crl.certum.pl/ctsca2021.crl0o
- http://repository.certum.pl/cevcsca2021.cer0
- http://repository.certum.pl/ctnca.cer09
- http://repository.certum.pl/ctnca2.cer09
- http://repository.certum.pl/ctsca2021.cer0A
- http://subca.ocsp-certum.com01
- http://subca.ocsp-certum.com02
- http://subca.ocsp-certum.com05
- http://www.certum.pl/CPS0
- http://www.iqiyi.com
- http://www.iqiyi.comaz
- http://zerossl.crt.sectigo.com/ZeroSSLECCDomainSecureSiteCA.crt0
- http://zerossl.ocsp.sectigo.com0
- https://api.iqiyi.cn.com/
- https://api.iqiyi.cn.com/:P
- https://api.iqiyi.cn.com/WxAM
- https://api.iqiyi.cn.com/WxAMLocalgr

https://api.iqiyi.cn.com/WxAMU

https://api.iqiyi.cn.com/WxAMwsPow

https://api.iqiyi.cn.com/api?url=BKMOMEGFHFAGKIOKJMMMMFFBOOFDJKIDPGNCEDNBKEJAMLJACMOG

https://api.iqiyi.cn.com/r

https://api.iqiyi.cn.com/r=U

https://sectigo.com/CPS0

https://www.certum.pl/CPS0

TLS

api.iqiyi.cn.com

api.iqiyi.cn.com

api.iqiyi.cn.com

Behavior Similarity Hashes

CAPA	a5612f4b6b4d61a7816c31766293459d
CAPE Sandbo…	a747c36d6e62d14398290f8b0677cbdb
Microsoft Sys…	2e1bab346f143334adf3cba5da1302c5
VirusTotal Juj…	79c49a018ad2606bdeaf9b5a84901db2
VirusTotal Ob…	2b60895a54b402fde8275afe12b164af
Zenbox	a656006571066b90f5ab11855c5f50f3

File system actions

Files Opened

C:\Users\<USER>\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\software.exe.log

C:\Users\<USER>\AppData\Local\Microsoft\Windows

C:\Users\<USER>\AppData\Local\Microsoft\Windows\INetCookies

C:\Users\<USER>\AppData\Local\Microsoft\Windows\INetCookies\ESE\

C:\Users\<USER>\Desktop

C:\Users\<USER>\Desktop\DPAPI.DLL

C:\Users\<USER>\Desktop\IPHLPAPI.DLL

C:\Users\<USER>\Desktop\ncrypt.dll

C:\Users\<USER>\Desktop\netutils.dll

C:\Users\<USER>\Desktop\software.INI

C:\Users\<USER>\Desktop\software.exe

C:\Users\<USER>\Desktop\software.exe.config

C:\Users\<USER>\Desktop\srvcli.dll

C:\Users\<USER>\Desktop\urlmon.dll
C:\Users\
C:\Users\<USER>\
C:\Users\<USER>\AppData\Local
C:\Users\<USER>\AppData\Local\Microsoft\Windows\History
C:\Users\<USER>\AppData\Local\Microsoft\Windows\History\History.IE5
C:\Users\<USER>\AppData\Local\Microsoft\Windows\Temporary Internet Files
C:\Users\<USER>\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5
C:\Users\<USER>\AppData\Local\Microsoft\Windows\Temporary Internet Files\counters.dat
C:\Users\<USER>\AppData\Roaming
C:\Users\<USER>\AppData\Roaming\Microsoft\SystemCertificates\My
C:\Users\<USER>\AppData\Roaming\Microsoft\SystemCertificates\My\CRLs\
C:\Users\<USER>\AppData\Roaming\Microsoft\SystemCertificates\My\CTLs\
C:\Users\<USER>\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\
C:\Users\<USER>\AppData\Roaming\Microsoft\Windows\Cookies
C:\Users\<USER>\Downloads\
C:\Users\<USER>\Downloads\hda.exe-.INI
C:\Users\<USER>\Downloads\hda.exe-.exe
C:\Users\<USER>\Downloads\hda.exe-.exe.config
C:\Users\Default\AppData\Roaming
C:\Users\azure
C:\Windows\Microsoft.NET\Framework64\
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\clr.dll
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\mscorwks.dll
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\SortDefault.nlp
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\clr.dll
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\clrjit.dll
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\config\machine.config
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\fusion.localgac
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscoreei.dll
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\nlssorting.dll
C:\Windows\SYSTEM32\MSCOREE.DLL.local
C:\Windows\System32\fveui.dll
C:\Windows\System32\fwpuclnt.dll
C:\Windows\System32\netprofm.dll
C:\Windows\System32\nlaapi.dll
C:\Windows\System32\npmproxy.dll

C:\Windows\System32\winrnr.dll
C:\Windows\System32\wship6.dll
C:\Windows\System32\wshqos.dll
C:\Windows\System32\wshtcpip.dll
C:\Windows\System32\wuaueng.dll
C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.24483_none_e372d88f30fbb845
C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.24483_none_e372d88f30fbb845\Comct
C:\Windows\WindowsShell.Manifest
C:\Windows\assembly\GAC\PublisherPolicy.tme
C:\Windows\assembly\NativeImages_v4.0.30319_64\HwyDL\
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\89bc329e
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\89bc329e
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\37a1d51f3591
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\37a1d51f3591
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\3597805b7d7
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\3597805b7d7
C:\Windows\assembly\pubpol9.dat
C:\Windows\system32\CRYPTSP.dll
C:\Windows\system32\GPAPI.dll
C:\Windows\system32\RpcRtRemote.dll
C:\Windows\system32\SSPICLI.DLL
C:\Windows\system32\Secur32.dll
C:\Windows\system32\VCRUNTIME140_CLR0400.dll
C:\Windows\system32\VERSION.dll
C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe
C:\Windows\system32\api-ms-win-core-xstate-l2-1-0.dll
C:\Windows\system32\api-ms-win-downlevel-advapi32-l2-1-0.dll
C:\Windows\system32\api-ms-win-downlevel-shlwapi-l2-1-0.dll
C:\Windows\system32\bcryptprimitives.dll
C:\Windows\system32\credssp.dll
C:\Windows\system32\dhcpcsvc.DLL
C:\Windows\system32\dhcpcsvc6.DLL
C:\Windows\system32\dnsapi.dll
C:\Windows\system32\drivers\etc\hosts
C:\Windows\system32\mswsock.dll
C:\Windows\system32\napinsp.dll
C:\Windows\system32\ncrypt.dll

C:\Windows\system32\p2pcollab.dll
C:\Windows\system32\pnrpnsp.dll
C:\Windows\system32\qagentrt.dll
C:\Windows\system32\rasadhlp.dll
C:\Windows\system32\rpcss.dll
C:\Windows\system32\rsaenh.dll
C:\Windows\system32\schannel.DLL
C:\Windows\system32\ucrtbase_clr0400.dll
C:\Windows\system32\webio.dll
C:\Windows\system32\winhttp.dll
C:\Windows\system32\wininet.DLL
\DEVICE\NETBT_TCPIP_{3DFCAD32-1CDE-44FB-A9E1-D91126365830}
\DEVICE\NETBT_TCPIP_{846EE342-7039-11DE-9D20-806E6F6E6963}
\DEVICE\NETBT_TCPIP_{C7276F17-2CF6-46AD-AADE-59B513373CC9}
\Device\Afd\Endpoint
\Device\RasAcd
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\file.exe.log
C:\Users\user\Desktop\file.exe
C:\Users\user\Desktop\file.exe.config
C:\Windows\AppPatch\sysmain.sdb
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Windows\SYSTEM32\CRYPTBASE.dll
C:\Windows\SYSTEM32\CRYPTSP.dll
C:\Windows\SYSTEM32\DNSAPI.dll
C:\Windows\SYSTEM32\DPAPI.DLL
C:\Windows\SYSTEM32\IPHLPAPI.DLL
C:\Windows\SYSTEM32\MSCOREE.DLL
C:\Windows\SYSTEM32\NTASN1.dll
C:\Windows\SYSTEM32\SspiCli.dll
C:\Windows\SYSTEM32\VCRUNTIME140_CLR0400.dll
C:\Windows\SYSTEM32\VERSION.dll
C:\Windows\SYSTEM32\WINNSI.DLL
C:\Windows\SYSTEM32\apphelp.dll
C:\Windows\SYSTEM32\bcrypt.dll
C:\Windows\SYSTEM32\dhcpcsvc.DLL
C:\Windows\SYSTEM32\dhcpcsvc6.DLL
C:\Windows\SYSTEM32\iertutil.dll
C:\Windows\SYSTEM32\mskeyprotect.dll
C:\Windows\SYSTEM32\ncrypt.dll
C:\Windows\SYSTEM32\ntdll.dll
C:\Windows\SYSTEM32\ondemandconnroutehelper.dll

C:\Windows\SYSTEM32\ucrtbase_clr0400.dll
C:\Windows\SYSTEM32\urlmon.dll
C:\Windows\SYSTEM32\winhttp.dll
C:\Windows\SYSTEM32\wininet.DLL
C:\Windows\System32\KERNEL32.dll
C:\Windows\System32\KERNELBASE.dll
C:\Windows\System32\drivers\etc\hosts
C:\Windows\System32\en-US\CRYPT32.dll.mui
C:\Windows\System32\en-US\wshqos.dll.mui
C:\Windows\System32\rasadhlp.dll
C:\Windows\assembly\pubpol66.dat
C:\Windows\system32\IMM32.DLL
C:\Windows\system32\NLAapi.dll
C:\Windows\system32\en-US\mswsock.dll.mui
C:\Windows\system32\ncryptsslp.dll
C:\Windows\system32\oleaut32.dll
Nsi

Files Written

C:\Windows\System32\Tasks\Microsoft\Windows\Application Experience\Microsoft Compatibility Appraiser
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies
C:\Users\user\AppData\Roaming

Files Deleted

C:\Windows\System32\wbem\Performance\WmiApRpl.h
C:\Windows\System32\wbem\Performance\WmiApRpl.ini

Registry actions

Registry Keys Opened

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Int Settings
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Inter Settings\AutoConfigURL
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Inter Settings\AutoDetect
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Inter Settings\CreateUriCacheSize

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Inter
Settings\MigrateProxy

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Inter
Settings\ProxyEnable

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Inter
Settings\ProxyOverride

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Inter
Settings\ProxyServer

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Inter
Settings\ZoneMap\AutoDetect

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Inter
Settings\ZoneMap\IntranetName

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Inter
Settings\ZoneMap\ProxyBypass

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Inter
Settings\ZoneMap\UNCAsIntranet

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Inter
Settings\Zones\0

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Inter
Settings\Zones\0\Flags

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Inter
Settings\Zones\1

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Inter
Settings\Zones\1\Flags

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Inter
Settings\Zones\2

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Inter
Settings\Zones\2\Flags

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Inter
Settings\Zones\3

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Inter
Settings\Zones\3\Flags

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Inter
Settings\Zones\4

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Inter
Settings\Zones\4\Flags

HKEY_CURRENT_USER\SOFTWARE\Policies\Microsoft\Windows\CurrentVersi
Settings\CreateUriCacheSize

HKEY_CURRENT_USER\Software\Microsoft\.NETFramework

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Intern
Settings\Lockdown_Zones\

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Intern
Settings\Lockdown_Zones\0

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Intern
Settings\Lockdown_Zones\1

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Intern Settings\Lockdown_Zones\2

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Intern Settings\Lockdown_Zones\3

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Intern Settings\Lockdown_Zones\4

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Intern Settings\ZoneMap\

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Intern Settings\Zones\

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Inter Settings\Zones\0

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Inter Settings\Zones\1

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Inter Settings\Zones\2

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Inter Settings\Zones\3

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Inter Settings\Zones\4

HKEY_CURRENT_USER\Software\Microsoft\windows\CurrentVersion\Intern Settings

HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\CurrentVersic Settings\Lockdown_Zones\

HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\CurrentVersic Settings\Lockdown_Zones\0

HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\CurrentVersic Settings\Lockdown_Zones\1

HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\CurrentVersic Settings\Lockdown_Zones\2

HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\CurrentVersic Settings\Lockdown_Zones\3

HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\CurrentVersic Settings\Lockdown_Zones\4

HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\CurrentVersic Settings\ZoneMap

HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\CurrentVersic Settings\ZoneMap\

HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\CurrentVersic Settings\Zones\

HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\CurrentVersic Settings\Zones\0

HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\CurrentVersic Settings\Zones\1

HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\CurrentVersic
Settings\Zones\3

HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\CurrentVersic
Settings\Zones\4

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\AppConte

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\DisableConfi

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\FeatureSIMD

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\InstallRoot

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\NGen\Policy\

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\OnlyUseLates

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\UseLegacyV2

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\UseRyuJIT

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NET Framework
Setup\NDP\v4\Full

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NET Framework
Setup\NDP\v4\Full\Release

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Image File Execution Options\DevOverrideEnable

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Inter
Settings\CreateUriCacheSize

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Ir
Settings\WinHttp

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Inter
Settings\WinHttpLowerCaseHost

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Inter
Settings\WinHttp\AutoProxyAutoLogonIfChallenged

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVers
Settings\CreateUriCacheSize

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVers
Settings\EnablePunycode

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVers
Settings\Security_HKLM_only

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Lsa\FipsAlgorithmP

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Lsa\FipsAlgorithmP

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Lsa\FipsAlgorithmP

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Lsa\FipsAlgorithmP

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\LanmanWorkstatio

HKEY_LOCAL_MACHINE\SYSTEM\Setup\SystemSetupInProgress

HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework

HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\NGen\Policy\v

HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\v4.0.30319\SKU

HKEY_LOCAL_MACHINE\Software\Microsoft\StrongName

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\software.exe

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Interne Settings\ZoneMap\

HKEY_LOCAL_MACHINE\Software\Microsoft\windows\CurrentVersion\Interne Settings

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersio Settings\

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersio Settings\Lockdown_Zones\

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersio Settings\Lockdown_Zones\0

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersio Settings\Lockdown_Zones\1

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersio Settings\Lockdown_Zones\2

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersio Settings\Lockdown_Zones\3

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersio Settings\Lockdown_Zones\4

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersi Settings\ZoneMap

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersio Settings\ZoneMap\

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersio Settings\Zones\

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersio Settings\Zones\0

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersio Settings\Zones\1

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersio Settings\Zones\2

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersio Settings\Zones\3

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersio Settings\Zones\4

HKEY_LOCAL_MACHINE\System\Setup

Policy\Standards

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Inter Settings\5.0\Cache

HKEY_CURRENT_USER\Software

HKEY_CURRENT_USER\Software\Microsoft\.NETFramework\Policy\Standard

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\AdminTabProcs

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ALLOW_REVERSE_SOLIDUS_IN_US

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ALWAYS_USE_DNS_FOR_SPN_KB3

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_BUFFERBREAKING_818408

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_BYPASS_CACHE_FOR_CREDPOLICY

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_CLIENTAUTHCERTFILTER

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_COMPAT_USE_CONNECTION_BASE

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_DIGEST_NO_EXTRAS_IN_URI

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_DISABLE_NOTIFY_UNVERIFIED_SP

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_DISABLE_UNICODE_HANDLE_CLOS

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_DISALLOW_NULL_IN_RESPONSE_I

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ENABLE_PROXY_CACHE_REFRESH_

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_EXCLUDE_INVALID_CLIENT_CERT_

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_FIX_CHUNKED_PROXY_SCRIPT_DC

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_HTTP_USERNAME_PASSWORD_DI

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_IGNORE_MAPPINGS_FOR_CREDPC

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_IGNORE_POLICIES_ZONEMAP_IF_I

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_INCLUDE_PORT_IN_SPN_KB90820

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_LOCALMACHINE_LOCKDOWN

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MIME_HANDLING

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_PERMIT_CACHE_FOR_AUTHENTIC

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_PRESERVE_SPACES_IN_FILENAME

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_RETURN_FAILED_CONNECT_CONT

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_SCH_SEND_AUX_RECORD_KB_261

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_SKIP_POST_RETRY_ON_INTERNET

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_USE_CNAME_FOR_SPN_KB911149

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_USE_UTF8_FOR_BASIC_AUTH_KB9

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ZONES_CHECK_ZONEMAP_POLICY

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\RETRY_HEADERONLYPOST_ONCONNECTION

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FrameMerging

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FrameTabWindow

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\SessionMerging

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\TabProcGrowth

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Security

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Security\DisableSecuritySettingsCheck

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Intern Settings

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Interne Settings\5.0\Cache\Content

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Interne Settings\5.0\Cache\Cookies

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Interne Settings\5.0\Cache\History

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Interne Settings\AutoConfigURL

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Interne Settings\AutoDetect

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Interne Settings\Connections

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Interne Settings\CreateUriCacheSize

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Interne Settings\EnableHttp1_1

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Interne Settings\EnablePunycode

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Interne Settings\ProxyEnable

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Interne Settings\ProxyHttp1.1

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Interne Settings\ProxyOverride

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Interne Settings\ProxyServer

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Interne Settings\SecureProtocols

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Interne Settings\Wpad

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Interne Settings\Wpad\WpadOverride

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Interne Settings\Zones

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\Policy\APTC

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\Policy\Servi

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NoClientChecks

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVers Settings\5.0\Cache

HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\CLRLoadLogDir

HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DisableConfigC

HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\FeatureSIMD

HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\InstallRoot

HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\NGen\Policy\v4

HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\OnlyUseLatestC

HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\Policy

HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\Policy\Standarc

HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\Policy\v4.0

HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\UseLegacyV2Ru

HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\UseRyuJIT

HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\v4.0.30319\SKU

HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\v4.0.30319\SKU

HKEY_LOCAL_MACHINE\Software\Microsoft\Fusion

HKEY_LOCAL_MACHINE\Software\Microsoft\Fusion\CacheLocation

HKEY_LOCAL_MACHINE\Software\Microsoft\Fusion\DisableMSIPeek

HKEY_LOCAL_MACHINE\Software\Microsoft\Fusion\DownloadCacheQuotaInI

HKEY_LOCAL_MACHINE\Software\Microsoft\Fusion\EnableLog

HKEY_LOCAL_MACHINE\Software\Microsoft\Fusion\FileInUseMillisecondsBet

HKEY_LOCAL_MACHINE\Software\Microsoft\Fusion\FileInUseRetryAttempts

HKEY_LOCAL_MACHINE\Software\Microsoft\Fusion\ForceLog

HKEY_LOCAL_MACHINE\Software\Microsoft\Fusion\LogFailures
HKEY_LOCAL_MACHINE\Software\Microsoft\Fusion\LogResourceBinds
HKEY_LOCAL_MACHINE\Software\Microsoft\Fusion\LoggingLevel
HKEY_LOCAL_MACHINE\Software\Microsoft\Fusion\PublisherPolicy\Default
HKEY_LOCAL_MACHINE\Software\Microsoft\Fusion\PublisherPolicy\Default\I
HKEY_LOCAL_MACHINE\Software\Microsoft\Fusion\PublisherPolicy\Default\I
HKEY_LOCAL_MACHINE\Software\Microsoft\Fusion\PublisherPolicy\Default\i
HKEY_LOCAL_MACHINE\Software\Microsoft\Fusion\PublisherPolicy\Default\I
HKEY_LOCAL_MACHINE\Software\Microsoft\Fusion\PublisherPolicy\Default\I
HKEY_LOCAL_MACHINE\Software\Microsoft\Fusion\PublisherPolicy\Default\I
HKEY_LOCAL_MACHINE\Software\Microsoft\Fusion\PublisherPolicy\Default\I
HKEY_LOCAL_MACHINE\Software\Microsoft\Fusion\PublisherPolicy\Default\I
HKEY_LOCAL_MACHINE\Software\Microsoft\Fusion\PublisherPolicy\Default\I
HKEY_LOCAL_MACHINE\Software\Microsoft\Fusion\PublisherPolicy\Default\v
HKEY_LOCAL_MACHINE\Software\Microsoft\Fusion\PublisherPolicy\Default\v
HKEY_LOCAL_MACHINE\Software\Microsoft\Fusion\PublisherPolicy\Default\v
HKEY_LOCAL_MACHINE\Software\Microsoft\Fusion\PublisherPolicy\Default\v
HKEY_LOCAL_MACHINE\Software\Microsoft\Fusion\PublisherPolicy\Default\v
HKEY_LOCAL_MACHINE\Software\Microsoft\Fusion\PublisherPolicy\Default\v
HKEY_LOCAL_MACHINE\Software\Microsoft\Fusion\UseLegacyIdentityForma
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ENABLE_PASSPORT_SESSION_STOI
HKEY_LOCAL_MACHINE\Software\Microsoft\OleAut
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DevOverrideEnable
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\hda.exe-.exe
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\PeerDist\Service
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-4270068108-2931534202-3907561125-1001
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Interne Settings\5.0\Cache
HKEY_LOCAL_MACHINE\Software\Policies
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Internet Explorer
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Internet Explorer\Main
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\PeerDist\Service

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersio Settings

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersio Settings\CreateUriCacheSize

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersio Settings\EnableHttp1_1

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersio Settings\EnablePunycode

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersio Settings\ProxyHttp1.1

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersio Settings\SecureProtocols

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProvider

HKEY_LOCAL_MACHINE\System\Setup\SystemSetupInProgress

Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings

Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings

Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-ed-de-51

Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{849213D7-2470-43FC-B1D0-C7C786E4E4E0}

Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{849213D7-2470-43FC-B1D0-C7C786E4E4E0}\52-54-00-ed-de-51

System\CurrentControlSet\Control\SecurityProviders\Schannel\UserContext

System\CurrentControlSet\Control\SecurityProviders\Schannel\UserContext

HKEY_CURRENT_USER\SOFTWARE\Policies\Microsoft\Windows\CurrentVersi Settings

HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\69\52C64B7E

HKEY_CURRENT_USER\Software\Microsoft\Fusion

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Download

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ENABLE_TOKEN_BINDING

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_URI_DISABLECACHE

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_USE_IETLDLIST_FOR_DOMAIN_DET

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explore

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explore

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explore

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explore Folders
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explore Shell Folders
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Interne Settings\5.0\Cache
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Interne Settings\5.0\Cache\Extensible Cache
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Interne Settings\ZoneMap\Domains\
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Interne Settings\ZoneMap\ProtocolDefaults\
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\WinTrus Providers\Software Publishing
- HKEY_CURRENT_USER\Software\Policies
- HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer
- HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Main
- HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl
- HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Security
- HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\CurrentVersion Settings
- HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\CurrentVersion Settings\ZoneMap\Domains\
- HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\CurrentVersion Settings\Zones\2
- HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Explorer
- HKEY_CURRENT_USER\ZoneMap\Ranges\
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AppID\file.exe
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{0358B920-0AC7-461F-98F4-58E32CD89148}
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{0358b920-0ac7-461f-98f4-58e32cd89148}\InprocHandler
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{0358b920-0ac7-461f-98f4-58e32cd89148}\InprocHandler32
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{0358b920-0ac7-461f-98f4-58e32cd89148}\InprocServer32
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{0358b920-0ac7-461f-98f4-58e32cd89148}\TreatAs
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{057EEE47-2572-4AA1-88D7-60CE2149E33C}
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{057EEE47-2572-4AA1-88D7-60CE2149E33C}\Elevation

HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{057EEE47-2572-4AA1-88D7-60CE2149E33C}\InprocHandler

HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{057EEE47-2572-4AA1-88D7-60CE2149E33C}\InprocHandler32

HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{057EEE47-2572-4AA1-88D7-60CE2149E33C}\InprocServer32

HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{057EEE47-2572-4AA1-88D7-60CE2149E33C}\LocalServer

HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{057EEE47-2572-4AA1-88D7-60CE2149E33C}\LocalServer32

HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{057EEE47-2572-4AA1-88D7-60CE2149E33C}\TreatAs

HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface\{00000134-0000-0000-C000-000000000046}

HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface\{00000134-0000-0000-C000-000000000046}\ProxyStubClsid32

HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface\{A168AADC-1674-49DA-AD4F-4F27DF8760D0}

HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface\{a168aadc-1674-49da-ad4f-4f27df8760d0}\ProxyStubClsid32

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\Policy\Standa

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\policy\standa

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\policy\v4.0

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\AppModel\Lookaside\Package

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Defaul

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Defaul

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Defaul

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Defaul

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Defaul

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Defaul

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Defaul

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Defaul

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Defaul

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Defaul

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Defaul

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ALLOW_REVERSE_SOLIDUS_IN_USE

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ALWAYS_USE_DNS_FOR_SPN_KB30

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_BUFFERBREAKING_818408

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_BYPASS_CACHE_FOR_CREDPOLICY_

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_COMPAT_USE_CONNECTION_BASEI

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_DIGEST_NO_EXTRAS_IN_URI

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_DISABLE_NOTIFY_UNVERIFIED_SPN

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_DISABLE_UNICODE_HANDLE_CLOSI

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_DISALLOW_NULL_IN_RESPONSE_H

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ENABLE_PASSPORT_SESSION_STOI

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ENABLE_TOKEN_BINDING

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_EXCLUDE_INVALID_CLIENT_CERT_K

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_FIX_CHUNKED_PROXY_SCRIPT_DOV

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_HTTP_USERNAME_PASSWORD_DIS/

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_IGNORE_MAPPINGS_FOR_CREDPOL

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_IGNORE_POLICIES_ZONEMAP_IF_ES

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_INCLUDE_PORT_IN_SPN_KB908209

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_LOCALMACHINE_LOCKDOWN

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MIME_HANDLING

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_PERMIT_CACHE_FOR_AUTHENTICA

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_PRESERVE_SPACES_IN_FILENAMES_

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_RETURN_FAILED_CONNECT_CONTE

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_SCH_SEND_AUX_RECORD_KB_2618

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_SKIP_POST_RETRY_ON_INTERNETW

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_URI_DISABLECACHE

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_USE_CNAME_FOR_SPN_KB911149

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_USE_IETLDLIST_FOR_DOMAIN_DET
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_USE_UTF8_FOR_BASIC_AUTH_KB9
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ZONES_CHECK_ZONEMAP_POLICY_
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\RETRY_HEADERONLYPOST_ONCONNECTIONR
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\OLE
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\OLEAUT
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\file.exe
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\msasn1
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Appl
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Expl {2B0F765D-C0E9-4171-908E-08A611B84FF6}
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Expl {2B0F765D-C0E9-4171-908E-08A611B84FF6}\PropertyBag
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Expl {352481E8-33BE-4251-BA85-6007CAEDCF9D}
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Expl {352481E8-33BE-4251-BA85-6007CAEDCF9D}\PropertyBag
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Expl {3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Expl {3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\PropertyBag
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Expl {5E6C858F-0E22-4760-9AFE-EA3317B67173}
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Expl {5E6C858F-0E22-4760-9AFE-EA3317B67173}\PropertyBag
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Expl {F1B32785-6FBA-4FCF-9D55-7B8E7F157091}
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Expl {F1B32785-6FBA-4FCF-9D55-7B8E7F157091}\PropertyBag
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Inter Settings
- HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Security
- HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\DNSClient\DnsPolicyConfig
- HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsStore
- HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Appx
- HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVers Settings

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Lsa\SspiCache\cred

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Dnscache\Interface{44C728A6-CC3C-434D-B238-E5B6541E3476}

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Tcpip\Parameters\I{3882a85b-858a-11eb-b9e1-806e6f6e6963}

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Winsock\Setup Migration\Providers\Tcpip

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Winsock\Setup Migration\Providers\Tcpip6

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\MUI\StringCach

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Segment Heap

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Policies\Microsoft\Crypt

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dnscache\Inter

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dnscache\Para

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dnscache\Para

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip6\Parame{3882A85B-858A-11EB-B9E1-806E6F6E6963}

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip6\Parame{44C728A6-CC3C-434D-B238-E5B6541E3476}

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Paramete{3882A85B-858A-11EB-B9E1-806E6F6E6963}

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Paramete{44C728A6-CC3C-434D-B238-E5B6541E3476}

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WinHttpAutoPr

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Winsock\Param

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Winsock\Setup Migration\Providers

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\crypt32

HKEY_LOCAL_MACHINE\Software

Registry Keys Set

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies\CachePrefix

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History\CachePrefix

Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings

Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable

{849213D7-2470-43FC-B1D0-C7C786E4E4E0}\WpadDecision

0

{849213D7-2470-43FC-B1D0-C7C786E4E4E0}\WpadDecisionReason

1

{849213D7-2470-43FC-B1D0-C7C786E4E4E0}\WpadNetworkName

Network 2

HKEY_USERS\S-1-5-21-4270068108-2931534202-3907561125-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.exe\Ope

Binary Data

\REGISTRY\A\{202606C4-CF72-D38C-F449-7915D54DDFBD}\Root\InventoryApplication\0000021f1df94e2c7570a94e3900
\REGISTRY\A\{202606C4-CF72-D38C-F449-7915D54DDFBD}\Root\InventoryApplication\0000c34c48b48a14753d8877e70
\REGISTRY\A\{202606C4-CF72-D38C-F449-7915D54DDFBD}\Root\InventoryDevicePnp\acpi/genuineintel_-_intel64_family_6_model_79_-_____intel(r)_xeon(r)_cpu_@_2.20ghz/_0\DriverVerVersion
\REGISTRY\A\{202606C4-CF72-D38C-F449-7915D54DDFBD}\Root\InventoryDevicePnp\acpi/genuineintel_-_intel64_family_6_model_79_-_____intel(r)_xeon(r)_cpu_@_2.20ghz/_1\DriverVerVersion
\REGISTRY\A\{202606C4-CF72-D38C-F449-7915D54DDFBD}\Root\InventoryDevicePnp\acpi/pnp0303/4&2c352a27&0\Dri
\REGISTRY\A\{202606C4-CF72-D38C-F449-7915D54DDFBD}\Root\InventoryDevicePnp\acpi/pnp0700/4&2c352a27&0\Dri
\REGISTRY\A\{202606C4-CF72-D38C-F449-7915D54DDFBD}\Root\InventoryDevicePnp\acpi/pnp0a03/0\DriverVerVersion
\REGISTRY\A\{202606C4-CF72-D38C-F449-7915D54DDFBD}\Root\InventoryDevicePnp\acpi/pnp0a06/pci_hotplug_resou
\REGISTRY\A\{202606C4-CF72-D38C-F449-7915D54DDFBD}\Root\InventoryDevicePnp\acpi/pnp0b00/4&2c352a27&0\Dri
\REGISTRY\A\{202606C4-CF72-D38C-F449-7915D54DDFBD}\Root\InventoryDevicePnp\acpi/pnp0f13/4&2c352a27&0\Driv
\REGISTRY\A\{202606C4-CF72-D38C-F449-7915D54DDFBD}\Root\InventoryDevicePnp\acpi/qemu0002/3&267a616a&0\D
\REGISTRY\A\{202606C4-CF72-D38C-F449-7915D54DDFBD}\Root\InventoryDevicePnp\hdaudio/func_01&ven_1af4&dev_
\REGISTRY\A\{202606C4-CF72-D38C-F449-7915D54DDFBD}\Root\InventoryDevicePnp\pci/ven_1af4&dev_1001&subsys_
\REGISTRY\A\{202606C4-CF72-D38C-F449-7915D54DDFBD}\Root\InventoryDevicePnp\pci/ven_1af4&dev_1002&subsys_
\REGISTRY\A\{202606C4-CF72-D38C-F449-7915D54DDFBD}\Root\InventoryDevicePnp\pci/ven_1af4&dev_1003&subsys_
\REGISTRY\A\{202606C4-CF72-D38C-F449-7915D54DDFBD}\Root\InventoryDevicePnp\pci/ven_1b36&dev_0100&subsys_
\REGISTRY\A\{202606C4-CF72-D38C-F449-7915D54DDFBD}\Root\InventoryDevicePnp\pci/ven_8086&dev_100e&subsys_
\REGISTRY\A\{202606C4-CF72-D38C-F449-7915D54DDFBD}\Root\InventoryDevicePnp\pci/ven_8086&dev_1237&subsys_

\REGISTRY\A\{202606C4-CF72-D38C-F449-7915D54DDFBD}\Root\InventoryDevicePnp\pci/ven_8086&dev_2668&subsys_
\REGISTRY\A\{202606C4-CF72-D38C-F449-7915D54DDFBD}\Root\InventoryDevicePnp\pci/ven_8086&dev_2934&subsys_
\REGISTRY\A\{202606C4-CF72-D38C-F449-7915D54DDFBD}\Root\InventoryDevicePnp\pci/ven_8086&dev_2935&subsys_
\REGISTRY\A\{202606C4-CF72-D38C-F449-7915D54DDFBD}\Root\InventoryDevicePnp\pci/ven_8086&dev_2936&subsys_
\REGISTRY\A\{202606C4-CF72-D38C-F449-7915D54DDFBD}\Root\InventoryDevicePnp\pci/ven_8086&dev_293a&subsys_
\REGISTRY\A\{202606C4-CF72-D38C-F449-7915D54DDFBD}\Root\InventoryDevicePnp\pci/ven_8086&dev_7000&subsys_
\REGISTRY\A\{202606C4-CF72-D38C-F449-7915D54DDFBD}\Root\InventoryDevicePnp\pci/ven_8086&dev_7010&subsys_
\REGISTRY\A\{202606C4-CF72-D38C-F449-7915D54DDFBD}\Root\InventoryDevicePnp\pciide/idechannel/4&403bef5&0&
\REGISTRY\A\{202606C4-CF72-D38C-F449-7915D54DDFBD}\Root\InventoryDevicePnp\pciide/idechannel/4&403bef5&0&

Process and service actions

Processes Created

"C:\Users\<USER>\Desktop\software.exe"
%SAMPLEPATH%\hda.exe
"C:\Users\user\Desktop\file.exe"

Shell Commands

"%SAMPLEPATH%\hda.exe"

Processes Injected

\\?\C:\Windows\system32\wbem\WMIADAP.EXE

Processes Terminated

1872 - C:\Windows\system32\DeviceDisplayObjectProvider.exe -Embedding
2180 - taskhost.exe SYSTEM
2508 - C:\Windows\system32\compattel\DiagTrackRunner.exe /UploadEtlFilesOnly
276 - C:\Windows\system32\schtasks.exe /delete /f /TN "Microsoft\Windows\Customer Experience Improvement Program\Uploader"
2944 - C:\Windows\System32\slui.exe -Embedding
856 - C:\Windows\system32\sc.exe start w32time task_started

Services Opened

dnsCache

Processes Tree

3216 - "C:\Users\<USER>\Desktop\software.exe"

2420 - %WINDIR%\explorer.exe

2124 - %SAMPLEPATH%\hda.exe

928 - hda.exe-.exe

8140 - "C:\Users\user\Desktop\file.exe"

Synchronization mechanisms & Signals

Mutexes Created

Local\ZonesCacheCounterMutex

Local\ZonesLockedCacheCounterMutex

Modules loaded

Runtime Modules

%SAMPLEPATH%\hda.exe

ADVAPI32.dll

API-MS-WIN-Service-Management-L1-1-0.dll

API-MS-WIN-Service-Management-L2-1-0.dll

API-MS-WIN-Service-winsvc-L1-1-0.dll

API-MS-Win-Security-LSALookup-L1-1-0.dll

API-MS-Win-Security-SDDL-L1-1-0.dll

C:\Windows\Microsoft.NET\Framework64\v4.0.30319\clr.dll

C:\Windows\Microsoft.NET\Framework64\v4.0.30319\clrjit.dll

C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscoree.dll

C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscoreei.dll

C:\Windows\Microsoft.NET\Framework64\v4.0.30319\nlssorting.dll

C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ole32.dll

C:\Windows\Microsoft.Net\assembly\GAC_64\mscorlib\v4.0_4.0.0.0__b77a5c

C:\Windows\System32\fwpuclnt.dll

C:\Windows\System32\netprofm.dll

C:\Windows\System32\npmproxy.dll

C:\Windows\System32\winrnr.dll

C:\Windows\System32\wship6.dll

C:\Windows\System32\wshqos.dll

C:\Windows\System32\wshtcpip.dll

C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\89bc329e8
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\37a1d51f35918
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\3597805b7d7c
C:\Windows\system32\NLAapi.dll
C:\Windows\system32\bcryptprimitives.dll
C:\Windows\system32\combase.dll
C:\Windows\system32\mswsock.dll
C:\Windows\system32\napinsp.dll
C:\Windows\system32\oleaut32.dll
C:\Windows\system32\pnrpnsp.dll
C:\Windows\system32\rsaenh.dll
C:\Windows\system32\schannel.DLL
C:\Windows\system32\wininet.dll
C:\Windows\system32\ws2_32
CLBCatQ.DLL
CRYPT32.dll
CRYPTBASE.dll
CRYPTSP.dll
Comctl32.dll
DNSAPI.dll
GPAPI.dll
IPHLPAPI.DLL
OLEAUT32.dll
RPCRT4.dll
RpcRtRemote.dll
SHLWAPI.dll
Secur32.dll
SspiCli.dll
USER32.dll
USERENV.dll
VERSION.dll
WININET.dll
WINTRUST.dll
WS2_32.dll
advapi32
api-ms-win-appmodel-runtime-l1-1-0.dll
api-ms-win-appmodel-runtime-l1-1-2.dll
api-ms-win-core-fibers-l1-1-1
api-ms-win-core-localization-l1-2-1
api-ms-win-core-quirks-l1-1-0.dll
api-ms-win-core-synch-l1-2-0

api-ms-win-core-xstate-l2-1-0.dll
api-ms-win-downlevel-advapi32-l1-1-0.dll
api-ms-win-downlevel-advapi32-l2-1-0.dll
api-ms-win-downlevel-ole32-l1-1-0.dll
api-ms-win-downlevel-shlwapi-l2-1-0.dll
bcrypt.dll
credssp.dll
dhcpcsvc.DLL
dhcpcsvc6.DLL
kernel32
kernel32.dll
mscoree.dll
ncrypt.dll
ntdll
ole32.dll
profapi.dll
rasadhlp.dll
shell32.dll
urlmon.dll
winhttp.dll
wininet

Highlighted actions

Calls Highlighted

GetAdaptersAddresses
GetTickCount
IsDebuggerPresent
Sleep

Cryptographical Plain Text

/0xe9/0x4f/0xff/
/0xeb/0xb3/0xe9/0xe4/0x01/0x00/0x00/0xe8/0x82/0xff/0xff/0xff/0x2f/0x57/0x
00/0x40/0x00/0x41/0xb8/0x00/0x10/0x00/0x00/0x41/0xb9/0x40/0x00/0x00/0x
0x00/0x00□□□□□□□□
0xfc/0x48/0x83/0xe4/0xf0/0xe8/0xc8/0x00/0x00/0x00/0x41/0x51/0x41/0x50/0
0xff/0xff/0x5d/0x6a/0x00/0x49/0xbe/0x77/0x69/0x6e/0x69/0x6e/0x65/0x74/0x
2e/0x38/0x30/0x0
a/0x48/0x8b/0x12

c/0x01/0x00/0x00

d/0x0a/0x00/0x35/0x4f/0x21/0x50/0x25/0x40/0x41/0x50/0x5b/0x34/0x5c/0x5

xc9/0xba/0x00/0x

Decoded Text

{'CobaltStrikeBeacon': {'BeaconType': [['HTTPS']], 'Port': [443], 'SleepTime': [2
['30819f300d06092a864886f70d010101050003818d0030818902818100acaebe
'C2Server': ['api.iqiyi.cn.com,/api'], 'UserAgent': ['Mozilla/5.0 (Windows NT 10
'.jpg']], 'SpawnTo': ['00000000000000000000000000000000'], 'PipeName': [''],
settings'], 'Watermark': [0], 'bStageCleanup': ['False'], 'bCFGCaution': ['False']

{"C2Server": "http://api.iqiyi.cn.com:443/WxAM", "User Agent": "User-Agent:
Mozilla/5.0 (Windows NT 10.06; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/80.0.845.80\r\n"}

{"Headers": "User-Agent: Mozilla/5.0 (Windows NT 10.06; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.845.80\r\n", "Type":
"Metasploit Download", "URL": "http://api.iqiyi.cn.com/WxAM"}

Highlighted Text

"Optional update delivery is not working"