VALKYRIE COMODO

Summary

File Name: s927397.exe

File Type: PE32 executable (GUI) Intel 80386, for MS Windows

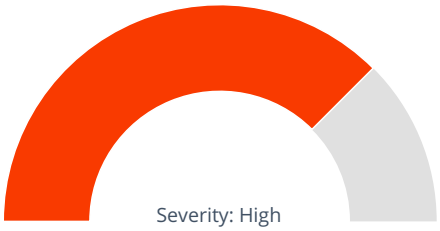
SHA1: f753a02962c14d6c7af61b620b8521500e0b4e81

MD5: 8deb4b389108c7990660db88b0dd5862

MALWARE

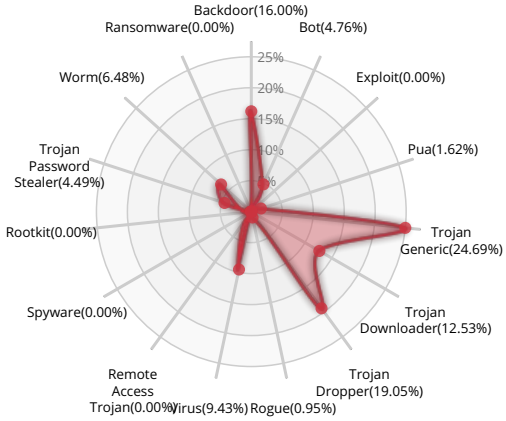
Valkyrie Final Verdict

DETECTION SECTION

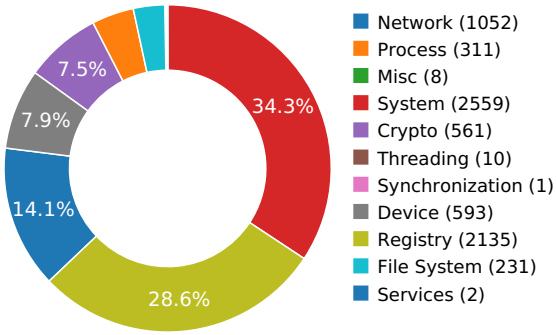


Verdict: Malware

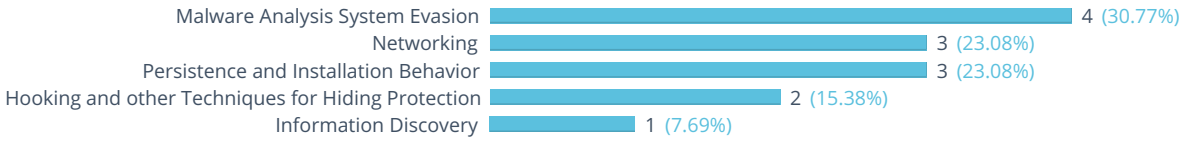
CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW



VALKYRIE COMODO

Activity Details

INFORMATION DISCOVERY

Attempts to remove evidence of file being downloaded from the Internet	Show sources

NETWORKING

Attempts to connect to a dead IP:Port (14 unique times)	Show sources
HTTP traffic contains suspicious features which may be indicative of malware related traffic	Show sources
Performs some HTTP requests	Show sources

MALWARE ANALYSIS SYSTEM EVASION

Detects Sandboxie through the presence of a library	
Checks the presence of disk drives in the registry, possibly for anti-virtualization	
Detects VirtualBox through the presence of a registry key	
Creates a hidden or system file	Show sources

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

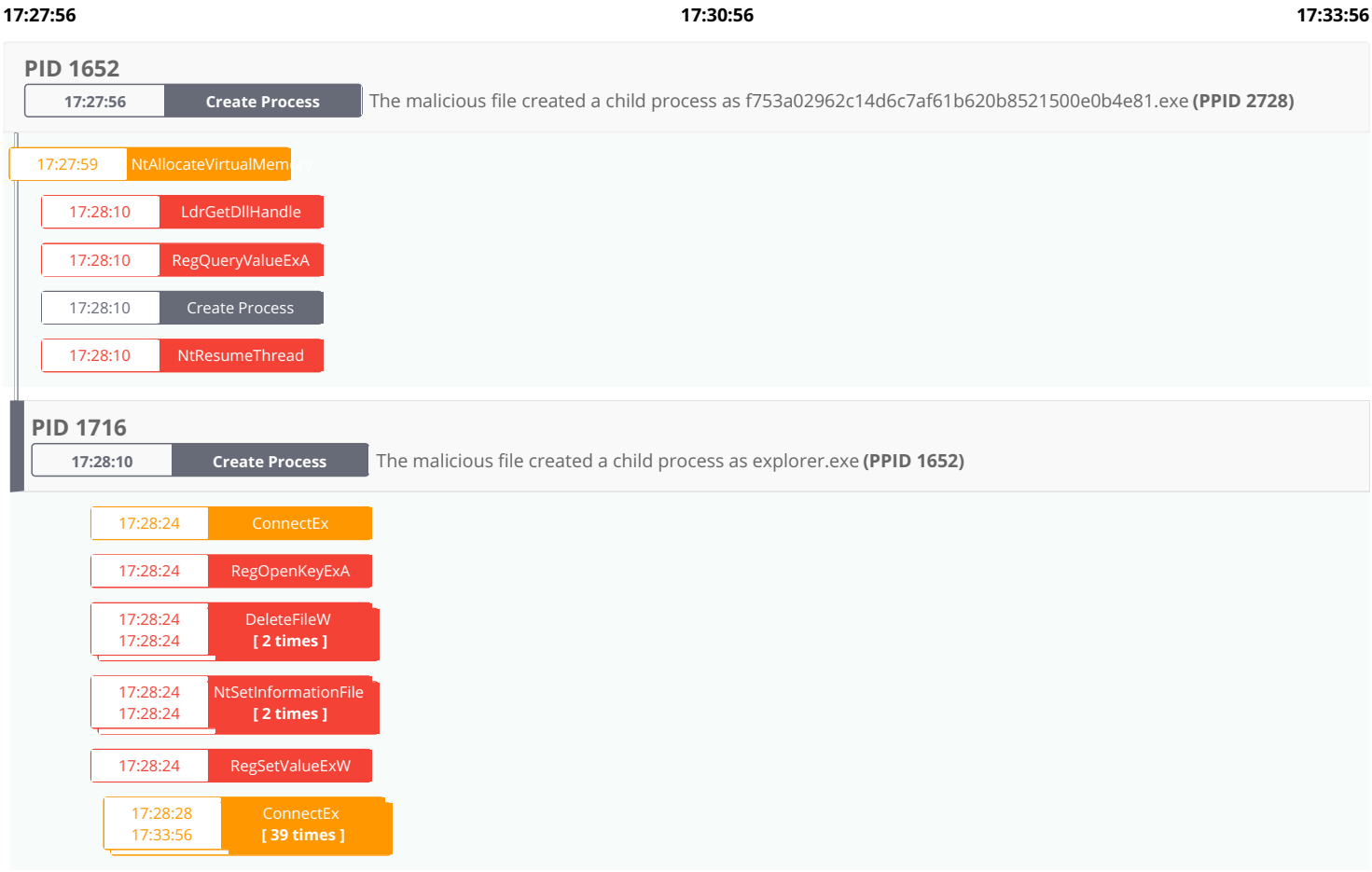
Creates RWX memory	
Executed a process and injected code into it, probably while unpacking	Show sources

PERSISTENCE AND INSTALLATION BEHAVIOR

Deletes its original binary from disk	
Installs itself for autorun at Windows startup	Show sources
Creates a copy of itself	Show sources

VALKYRIE COMODO

Behavior Graph



VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

C:\Users\user\AppData\Local\Temp\winhttp.DLL
C:\Windows\System32\winhttp.dll
C:\Users\user\AppData\Local\Temp\webio.dll
C:\Windows\System32\webio.dll
C:\Users\user\AppData\Local\Temp\dnsapi.DLL
C:\Windows\System32\dnsapi.dll
C:\
C:\Windows\SysWOW64\winhttp.dll
C:\Windows\SysWOW64\webio.dll
C:\Windows\SysWOW64\dnsapi.dll
C:\Users\user\AppData\Roaming\Microsoft\rwufbuia
C:\Users\user\AppData\Roaming\Microsoft\rwufbuia\cafadrev.exe
C:\Users\user\AppData\Local\Temp\f753a02962c14d6c7af61b620b8521500e0b4e81.exe
C:\Users\user\AppData\Roaming\Microsoft\rwufbuia\cafadrev.exe:Zone.Identifier
C:\Windows\System32\advapi32.dll
C:\Users\user\AppData\Roaming\Microsoft\rwufbuia\rwufbuia
C:\Windows\System32\p2pcollab.dll
C:\Windows\System32\qagentrt.dll
C:\Windows\SysWOW64\en-US\dnsapi.DLL.mui
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates*
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\1233B8D21D2ECB0483D16253D1FF3964BD09EF0C
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\16B1DD478BCE71A0FB1822E8F4F30AB467BBEFD4
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\2064A97B987412930E2994D60AE7EB72D89BC4F7
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\37998502C2CC1852F8774DAF543DD76D10D6FD93
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\418C30DD41197CBAABF21675F8559794F5551115
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\44E5AE16D06F9FBB92D6D9444B5C65C0F331D0EC
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\4FDDCB932603534677ECAE8C7D0FD914FD443E83
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\5D247FE955609769879FB1DD016537EEF650B8EC
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\6A8C669D7D1D5759CE7C1E0C5BE286257C31F366
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\744CDF45BF43EF285758286CAC89AF786F938342
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\761F091EA5F80A98B0D89734231D300CF9C027E8
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\7A5F1A5DE6AA551C795CC508128C6D894FA2C502

C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\8291DA84F9266F6D0ED367AF8BE3FA722529EB91
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\871E3CD70B6F8EE3C1E7BE4C7BEF4FFCCE673E32
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\8A82FE0617F4170E0BF052CF6BABFC628DA51919
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\8B943CF0CAEF7F6F04E98C9405960323B23C516D
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\9317D002FC43BDA932B8397B6E729B83D48EEB8D
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\95EEF9A37407C5B87BCF95D69B01DCFDAFD07635
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\A092A81885DDD5AAD1EC1A803D7183779D81B6F9
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\BAED8A8C5A147CFA78E686BB4A8E5829C2F934F5
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\C8A51E044BF5AF39158BB24E414E8FDCD2891C3A
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\FB45378AB288E369B22C860D123A809F530D5CC1
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\CRLs*
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\CTLs*

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\crypt32\DebugHeapFlags
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\DisableImprovedZoneCheck
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Security_HKLM_only
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Disk\Enum\0
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\ffffcce24
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\svcVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Version
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\OLE\MaximumAllowedAllocationSize
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00\WpadDecision
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00\WpadDecisionTime
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\WpadExpirationDays
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\7-Zip\HelpLink
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\7-Zip\URLInfoAbout
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook\HelpLink
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook\URLInfoAbout
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Connection Manager\HelpLink
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Connection Manager\URLInfoAbout
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DirectDrawEx\HelpLink
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DirectDrawEx\URLInfoAbout
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DXM_Runtime\HelpLink

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DXM_Runtime\URLInfoAbout
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Fontcore\HelpLink
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Fontcore\URLInfoAbout
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE40\HelpLink
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE40\URLInfoAbout
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE4Data\HelpLink
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE4Data\URLInfoAbout
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE5BAKEX\HelpLink
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE5BAKEX\URLInfoAbout
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IEData\HelpLink
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IEData\URLInfoAbout
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MobileOptionPack\HelpLink
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MobileOptionPack\URLInfoAbout
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MPlayer2\HelpLink
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MPlayer2\URLInfoAbout
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Oracle VM VirtualBox Guest Additions\HelpLink
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Oracle VM VirtualBox Guest Additions\URLInfoAbout
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Sandboxie\HelpLink
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Sandboxie\URLInfoAbout
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\SchedulingAgent\HelpLink
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\SchedulingAgent\URLInfoAbout
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Totalcmd64\HelpLink
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Totalcmd64\URLInfoAbout
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\WIC\HelpLink
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\WIC\URLInfoAbout
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{0D3E9E15-DE7A-300B-96F1-B4AF12B96488}\HelpLink
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{0D3E9E15-DE7A-300B-96F1-B4AF12B96488}\URLInfoAbout
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{2ACBF1FA-F5C3-4B19-A774-B22A31F231B9}_is1\HelpLink
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{2ACBF1FA-F5C3-4B19-A774-B22A31F231B9}_is1\URLInfoAbout
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{5247E16E-BCF8-95AB-1653-B3F8FBF8B3F1}\HelpLink
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{5247E16E-BCF8-95AB-1653-B3F8FBF8B3F1}\URLInfoAbout
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{77F3D72C-465F-BD51-890E-CC3914B1365F}\HelpLink
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{77F3D72C-465F-BD51-890E-CC3914B1365F}\URLInfoAbout
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{8C5B5A11-CBF8-451B-B201-77FAB0D0B77D}\HelpLink
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{8C5B5A11-CBF8-451B-B201-77FAB0D0B77D}\URLInfoAbout

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90120000-002A-0000-1000-0000000FF1CE}\HelpLink
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90120000-002A-0000-1000-0000000FF1CE}\URLInfoAbout
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90120000-002A-0409-1000-0000000FF1CE}\HelpLink
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90120000-002A-0409-1000-0000000FF1CE}\URLInfoAbout
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90120000-0116-0409-1000-0000000FF1CE}\HelpLink
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90120000-0116-0409-1000-0000000FF1CE}\URLInfoAbout
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{92FB6C44-E685-45AD-9B20-CADF4CABA132} - 1033\HelpLink
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{92FB6C44-E685-45AD-9B20-CADF4CABA132} - 1033\URLInfoAbout
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{963E5FEB-1367-46B9-851D-A957F1A3747F}\HelpLink
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{963E5FEB-1367-46B9-851D-A957F1A3747F}\URLInfoAbout
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{96F4525A-470D-F15C-796E-58D9988C3E5F}\HelpLink
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{96F4525A-470D-F15C-796E-58D9988C3E5F}\URLInfoAbout
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{BC958BD2-5DAC-3862-BB1A-C1BE0790438D}\HelpLink
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{BC958BD2-5DAC-3862-BB1A-C1BE0790438D}\URLInfoAbout
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{BD6F5371-DAC1-30F0-9DDE-CAC6791E28C3}\HelpLink
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{BD6F5371-DAC1-30F0-9DDE-CAC6791E28C3}\URLInfoAbout
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\SecurityProviders\SCHANNEL\UserContextLockCount
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\SecurityProviders\SCHANNEL\UserContextListCount
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\OID\EncodingType 0\CryptDllFindOIDInfo\1.3.6.1.4.1.311.44.3.4!7\Name
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\MUI\StringCacheSettings\StringCacheGeneration

MODIFIED FILES

C:\Users\user\AppData\Roaming\Microsoft\rwufbuia\cafadrev.exe
C:\Users\user\AppData\Roaming\Microsoft\rwufbuia

RESOLVED APIS

kernel32.dll.FlsAlloc
kernel32.dll.FlsGetValue
kernel32.dll.FlsSetValue
kernel32.dll.FlsFree
kernel32.dll.InitializeCriticalSectionAndSpinCount
kernel32.dll.VirtualAlloc
cryptsp.dll.CryptAcquireContextA
cryptsp.dll.CryptCreateHash
cryptsp.dll.CryptHashData

cryptsp.dll.CryptGetHashParam
cryptsp.dll.CryptDestroyHash
cryptsp.dll.CryptReleaseContext
ole32.dll.CoInitializeEx
cryptbase.dll.SystemFunction036
advapi32.dll.RegDeleteTreeA
advapi32.dll.RegDeleteTreeW
ole32.dll.CoTaskMemAlloc
ole32.dll.StringFromIID
nsi.dll.NsiAllocateAndGetTable
cfgmgr32.dll.CM_Open_Class_Key_ExW
iphlpapi.dll.ConvertInterfaceGuidToLuid
iphlpapi.dll.GetIfEntry2
iphlpapi.dll.GetIpForwardTable2
iphlpapi.dll.GetIpNetEntry2
iphlpapi.dll.FreeMibTable
ole32.dll.CoTaskMemFree
nsi.dll.NsiFreeTable
ole32.dll.CoUninitialize
oleaut32.dll.#500
shlwapi.dll.StrCmpNW
ws2_32.dll.GetAddrInfoW
ws2_32.dll.WSASocketW
ws2_32.dll.#2
ws2_32.dll.#21
ws2_32.dll.#9
ws2_32.dll.WSAIoctl
ws2_32.dll.FreeAddrInfoW
ws2_32.dll.#6
ws2_32.dll.#5
ws2_32.dll.WSARecv
ws2_32.dll.WSASend
schannel.dll.SpUserModeInitialize
advapi32.dll.RegCreateKeyExW
advapi32.dll.RegQueryValueExW

advapi32.dll.RegCloseKey
secur32.dll.FreeContextBuffer
ncrypt.dll.SslOpenProvider
ncrypt.dll.GetSChannelInterface
bcryptprimitives.dll.GetHashInterface
ncrypt.dll.SslIncrementProviderReferenceCount
ncrypt.dll.SslImportKey
bcryptprimitives.dll.GetCipherInterface
ncrypt.dll.SslLookupCipherSuiteInfo
user32.dll.LoadStringW
ncrypt.dll.BCryptOpenAlgorithmProvider
ncrypt.dll.BCryptGetProperty
ncrypt.dll.BCryptCreateHash
ncrypt.dll.BCryptHashData
ncrypt.dll.BCryptFinishHash
ncrypt.dll.BCryptDestroyHash
crypt32.dll.CertGetCertificateChain
userenv.dll.GetUserProfileDirectoryW
sechost.dll.ConvertSidToStringSidW
sechost.dll.ConvertStringSidToSidW
userenv.dll.RegisterGPNotification
gpapi.dll.RegisterGPNotificationInternal
sechost.dll.OpenSCManagerW
sechost.dll.OpenServiceW
sechost.dll.CloseServiceHandle
sechost.dll.QueryServiceConfigW
cryptsp.dll.CryptGetKeyParam
cryptsp.dll.CryptDestroyKey
cryptsp.dll.CryptVerifySignatureA
bcryptprimitives.dll.GetAsymmetricEncryptionInterface
ncrypt.dll.BCryptImportKeyPair
ncrypt.dll.BCryptVerifySignature

DELETED FILES

C:\Users\user\AppData\Roaming\Microsoft\rwufbuia\cafadrev.exe

C:\Users\user\AppData\Roaming\Microsoft\rwufbuia\cafadrev.exe:Zone.Identifier

C:\Users\user\AppData\Local\Temp\f753a02962c14d6c7af61b620b8521500e0b4e81.exe

REGISTRY KEYS

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\crypt32

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\crypt32\DebugHeapFlags

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\DisableImprovedZoneCheck

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Security_HKLM_only

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Disk\Enum

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Disk\Enum\0

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\GRE_Initialize

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles

HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\ffffcce24

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\svcVersion

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Version

HKEY_LOCAL_MACHINE\Software\Microsoft\Ole

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\OLE\MaximumAllowedAllocationSize

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Class\{4d36e972-e325-11ce-bfc1-08002be10318}

HKEY_CURRENT_USER\Software\Microsoft\windows\CurrentVersion\Internet Settings\Wpad

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00\WpadDecision

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00\WpadDecisionTime

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\WpadExpirationDays

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\7-Zip

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\7-Zip\HelpLink

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\7-Zip\URLInfoAbout

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook\HelpLink

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook\URLInfoAbout

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\Connection Manager

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Connection Manager\HelpLink

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Connection Manager\URLInfoAbout
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\DirectDrawEx
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DirectDrawEx\HelpLink
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DirectDrawEx\URLInfoAbout
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\DXM_Runtime
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DXM_Runtime\HelpLink
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DXM_Runtime\URLInfoAbout
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\Fontcore
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Fontcore\HelpLink
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Fontcore\URLInfoAbout
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\IE40
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE40\HelpLink
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE40\URLInfoAbout
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\IE4Data
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE4Data\HelpLink
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE4Data\URLInfoAbout
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\IE5BAKEX
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE5BAKEX\HelpLink
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE5BAKEX\URLInfoAbout
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\IEData
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IEData\HelpLink
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IEData\URLInfoAbout
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\MobileOptionPack
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MobileOptionPack\HelpLink
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MobileOptionPack\URLInfoAbout
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\MPlayer2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MPlayer2\HelpLink
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MPlayer2\URLInfoAbout
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\Oracle VM VirtualBox Guest Additions
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Oracle VM VirtualBox Guest Additions\HelpLink
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Oracle VM VirtualBox Guest Additions\URLInfoAbout
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\Sandboxie
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Sandboxie\HelpLink
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Sandboxie\URLInfoAbout
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\SchedulingAgent

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\SchedulingAgent\HelpLink
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\SchedulingAgent\URLInfoAbout
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\Totalcmd64
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Totalcmd64\HelpLink
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Totalcmd64\URLInfoAbout
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\WIC
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\WIC\HelpLink
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\WIC\URLInfoAbout
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{0D3E9E15-DE7A-300B-96F1-B4AF12B96488}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{0D3E9E15-DE7A-300B-96F1-B4AF12B96488}\HelpLink

READ FILES

C:\Windows\System32\winhttp.dll
C:\Windows\System32\webio.dll
C:\Windows\System32\dnsapi.dll
C:\Windows\SysWOW64\winhttp.dll
C:\Windows\SysWOW64\webio.dll
C:\Windows\SysWOW64\dnsapi.dll
C:\Users\user\AppData\Local\Temp\f753a02962c14d6c7af61b620b8521500e0b4e81.exe
C:\Users\user\AppData\Roaming\Microsoft\rwufbuia\cafadrev.exe
C:\Users\user\AppData\Roaming\Microsoft\rwufbuia
C:\Users\user\AppData\Roaming\Microsoft\rwufbuia\rwufbuia
C:\Windows\System32\p2pcollab.dll
C:\Windows\SysWOW64\en-US\dnsapi.DLL.mui
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\1233B8D21D2ECB0483D16253D1FF3964BD09EF0C
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\16B1DD478BCE71A0FB1822E8F4F30AB467BBEFD4
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\2064A97B987412930E2994D60AE7EB72D89BC4F7
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\37998502C2CC1852F8774DAF543DD76D10D6FD93
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\418C30DD41197CBAABF21675F8559794F5551115
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\44E5AE16D06F9FBB92D6D9444B5C65C0F331D0EC
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\4FDDCB932603534677ECAE8C7D0FD914FD443E83
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\5D247FE955609769879FB1DD016537EEF650B8EC
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\6A8C669D7D1D5759CE7C1E0C5BE286257C31F366
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\744CDF45BF43EF285758286CAC89AF786F938342
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\761F091EA5F80A98B0D89734231D300CF9C027E8

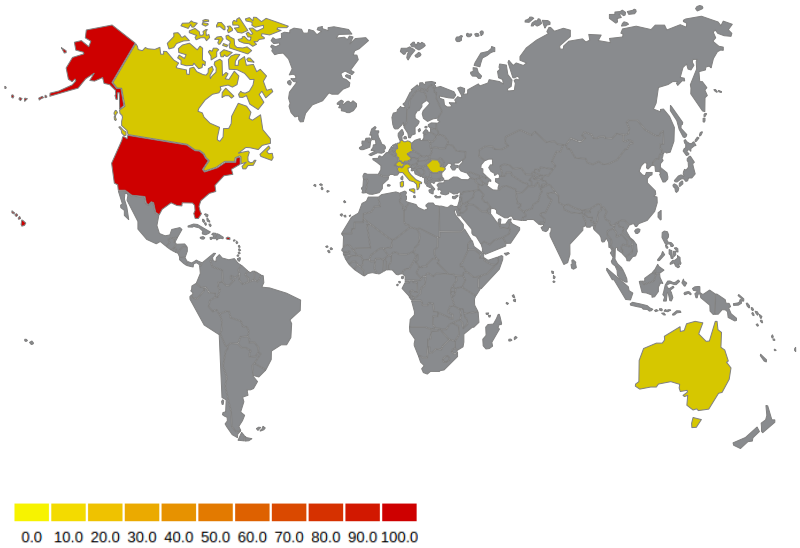
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\7A5F1A5DE6AA551C795CC508128C6D894FA2C502
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\8291DA84F9266F6D0ED367AF8BE3FA722529EB91
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\871E3CD70B6F8EE3C1E7BE4C7BEF4FFCCE673E32
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\8A82FE0617F4170E0BF052CF6BABFC628DA51919
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\8B943CF0CAEF7F6F04E98C9405960323B23C516D
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\9317D002FC43BDA932B8397B6E729B83D48EEB8D
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\95EEF9A37407C5B87BCF95D69B01DCFDAFD07635
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\A092A81885DDD5AAD1EC1A803D7183779D81B6F9
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\BAED8A8C5A147CFA78E686BB4A8E5829C2F934F5
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\C8A51E044BF5AF39158BB24E414E8FDCD2891C3A
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\FB45378AB288E369B22C860D123A809F530D5CC1

MODIFIED REGISTRY KEYS

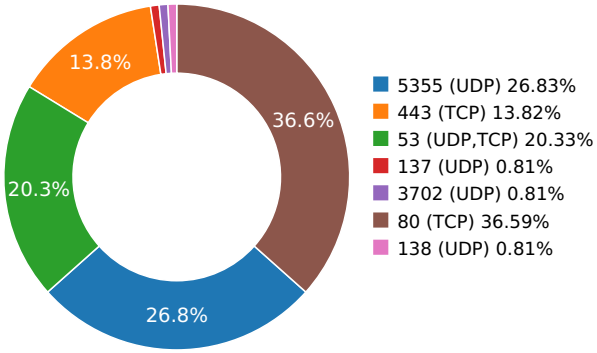
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\Wow6432Node
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\LanguageList
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\p2pcollab.dll,-8042
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\dnsapi.dll,-103

Network Behavior

CONTACTED IPS



NETWORK PORT DISTRIBUTION



Name	IP	Country	ASN	ASN Name	Trigger Process Type
	8.8.4.4	United States	15169	Level 3 Communications, Inc.	Malware Process
	142.4.204.111	United States	16276	OVH Hosting, Inc.	Malware Process
	185.121.177.177	Antarctica	204136	FuslVZ OpenNIC Anycast DNS...	Malware Process
	23.196.34.38	United States	2828	Akamai Technologies, Inc.	Malware Process
	23.197.16.48	United States	20940	Akamai Technologies, Inc.	Malware Process
	23.197.40.133	United States	20940	Akamai Technologies, Inc.	Malware Process
	23.53.120.202	United States	16625	Akamai Technologies, Inc.	Malware Process
	23.53.121.101	United States	16625	Akamai Technologies, Inc.	Malware Process
	27.100.36.191	Australia	36351	HostUS ==========...	Malware Process
	31.3.135.232	Switzerland	199662	Exion Networks SA	Malware Process
	45.63.25.55	United States	20473	Choopa, LLC	Malware Process
	89.18.27.34	Romania	39306	SC OPTIC BRIDGE SRL Aleea M...	Malware Process
	5.9.49.12	Germany	24940	Hetzner Online AG Datacente...	Malware Process
	47.91.77.235	Canada	45102	Alibaba.com LLC	Malware Process
	198.251.86.12	United States	53667	FranTech Solutions	Malware Process
	193.183.98.154	Italy	34971	Iperweb Ltd	Malware Process
go.microsoft.com	104.88.12.34	United States	2914	Akamai Technologies, Inc.	Malware Process
support.microsoft.com	104.88.14.19	United States	2914	Akamai Technologies, Inc.	Malware Process
trac.mpc-hc.org	37.34.55.187	Netherlands	35470	XL Internet Services B.V.	Malware Process
msdn.microsoft.com	157.56.148.19	United States	8075	Microsoft Corporation	Malware Process
mpc-hc.org	37.34.55.187	Netherlands	35470	XL Internet Services B.V.	Malware Process
www.ghisler.com	64.131.64.240	United States	25847	ServInt	Malware Process
www.virtualbox.org	137.254.60.32	United States	792	Oracle Corporation	Malware Process

Name	IP	Country	ASN	ASN Name	Trigger Process Type
www.bing.com	204.79.197.200	United States	8068	Microsoft Corporation	Malware Process

HTTP PACKETS

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
www.bing.com	80	GET	1.1	Mozilla/4.0 (compatible; MS...	1	32.4237539768
Path: / **URI:** http://www.bing.com/						
www.virtualbox.org	80	POST	1.1	Mozilla/4.0 (compatible; MS...	1	36.2847509384
Path: / **URI:** http://www.virtualbox.org/						
www.virtualbox.org	80	POST	1.1	Mozilla/4.0 (compatible; MS...	1	44.1909899712
Path: / **URI:** http://www.virtualbox.org/						
www.virtualbox.org	80	POST	1.1	Mozilla/4.0 (compatible; MS...	1	52.9087920189
Path: / **URI:** http://www.virtualbox.org/						
go.microsoft.com	80	POST	1.1	Mozilla/4.0 (compatible; MS...	1	59.7847869396
Path: /fwlink/?LinkId=286133 **URI:** http://go.microsoft.com/fwlink/?LinkId=286133						
support.microsoft.com	80	GET	1.1	Mozilla/4.0 (compatible; MS...	4	59.8728809357
Path: / **URI:** http://support.microsoft.com/						
go.microsoft.com	80	POST	1.1	Mozilla/4.0 (compatible; MS...	1	124.057663918
Path: /fwlink/?LinkId=133405 **URI:** http://go.microsoft.com/fwlink/?LinkId=133405						
msdn.microsoft.com	80	GET	1.1	Mozilla/4.0 (compatible; MS...	5	124.404417038
Path: /vstudio **URI:** http://msdn.microsoft.com/vstudio						
go.microsoft.com	80	POST	1.1	Mozilla/4.0 (compatible; MS...	1	132.896775961
Path: /fwlink/?LinkId=133405 **URI:** http://go.microsoft.com/fwlink/?LinkId=133405						
go.microsoft.com	80	POST	1.1	Mozilla/4.0 (compatible; MS...	1	141.61273694
Path: /fwlink/?LinkId=133405 **URI:** http://go.microsoft.com/fwlink/?LinkId=133405						
www.ghisler.com	80	POST	1.1	Mozilla/4.0 (compatible; MS...	1	149.79460597
Path: / **URI:** http://www.ghisler.com/						
go.microsoft.com	80	POST	1.1	Mozilla/4.0 (compatible; MS...	1	155.953285933

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
Path: /fwlink/?LinkId=133405 **URI:** http://go.microsoft.com/fwlink/?LinkId=133405						
www.virtualbox.org	80	POST	1.1	Mozilla/4.0 (compatible; MS...	1	228.848814964
Path: / **URI:** http://www.virtualbox.org/						
www.virtualbox.org	80	POST	1.1	Mozilla/4.0 (compatible; MS...	1	239.641303062
Path: / **URI:** http://www.virtualbox.org/						
go.microsoft.com	80	POST	1.1	Mozilla/4.0 (compatible; MS...	1	247.087513924
Path: /fwlink/?LinkId=286133 **URI:** http://go.microsoft.com/fwlink/?LinkId=286133						
go.microsoft.com	80	POST	1.1	Mozilla/4.0 (compatible; MS...	1	254.694878101
Path: /fwlink/?LinkId=286133 **URI:** http://go.microsoft.com/fwlink/?LinkId=286133						
go.microsoft.com	80	POST	1.1	Mozilla/4.0 (compatible; MS...	1	261.065455914
Path: /fwlink/?LinkId=286133 **URI:** http://go.microsoft.com/fwlink/?LinkId=286133						
www.virtualbox.org	80	POST	1.1	Mozilla/4.0 (compatible; MS...	1	268.128782034
Path: / **URI:** http://www.virtualbox.org/						
www.ghisler.com	80	POST	1.1	Mozilla/4.0 (compatible; MS...	1	275.660758018
Path: / **URI:** http://www.ghisler.com/						
www.virtualbox.org	80	POST	1.1	Mozilla/4.0 (compatible; MS...	1	342.30073905
Path: / **URI:** http://www.virtualbox.org/						
go.microsoft.com	80	POST	1.1	Mozilla/4.0 (compatible; MS...	1	349.771625042
Path: /fwlink/?LinkId=133405 **URI:** http://go.microsoft.com/fwlink/?LinkId=133405						
www.ghisler.com	80	POST	1.1	Mozilla/4.0 (compatible; MS...	1	364.705796957
Path: / **URI:** http://www.ghisler.com/						

DNS QUERIES

Request	Type
www.bing.com	A
Answers - www-bing-com.a-0001.a-msedge.net (CNAME) - 204.79.197.200 (A) - a-0001.a-msedge.net (CNAME) - 13.107.21.200 (A)	
www.virtualbox.org	A
Answers - 137.254.60.32 (A)	
go.microsoft.com	A
Answers - go.microsoft.com.edgekey.net (CNAME) - 23.197.16.48 (A) - e11290.dspg.akamaiedge.net (CNAME) - 23.53.121.101 (A) - 23.196.34.38 (A)	
support.microsoft.com	A
Answers - e3843.g.akamaiedge.net (CNAME) - ev.support.microsoft.com.edgekey.net (CNAME) - 23.197.40.133 (A) - 23.53.120.202 (A)	
mpc-hc.org	A
Answers - 37.34.55.187 (A)	
msdn.microsoft.com	A
Answers - msdn.microsoft.akadns.net (CNAME) - 157.56.148.19 (A)	
www.ghisler.com	A
Answers - 64.131.64.240 (A) - ghisler.com (CNAME)	
trac.mpc-hc.org	A
Answers - mpc-hc.org (CNAME)	

TCP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
32.4237539768	Sandbox	204.79.197.200	80
36.2847509384	Sandbox	137.254.60.32	80
36.4852440357	Sandbox	137.254.60.32	443

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
44.1909899712	Sandbox	137.254.60.32	80
44.3196299076	Sandbox	137.254.60.32	443
52.9087920189	Sandbox	137.254.60.32	80
53.0139739513	Sandbox	137.254.60.32	443
59.7847869396	Sandbox	23.197.16.48	80
59.8728809357	Sandbox	23.197.40.133	80
59.9376940727	Sandbox	23.197.40.133	443
90.6607248783	Sandbox	89.18.27.34	53
117.175990105	Sandbox	37.34.55.187	443
124.057663918	Sandbox	23.53.121.101	80
124.404417038	Sandbox	157.56.148.19	80
124.516299963	Sandbox	157.56.148.19	443
132.896775961	Sandbox	23.53.121.101	80
141.61273694	Sandbox	23.53.121.101	80
149.79460597	Sandbox	64.131.64.240	80
164.377612114	Sandbox	37.34.55.187	443
172.009668112	Sandbox	37.34.55.187	443
179.027077913	Sandbox	37.34.55.187	443
189.772787094	Sandbox	31.3.135.232	53
193.584675074	Sandbox	89.18.27.34	53
194.384663105	Sandbox	185.121.177.177	53
215.878561974	Sandbox	27.100.36.191	53
216.37460494	Sandbox	45.63.25.55	53
216.635715008	Sandbox	142.4.204.111	53
221.885915041	Sandbox	37.34.55.187	443
228.848814964	Sandbox	137.254.60.32	80
228.977545023	Sandbox	137.254.60.32	443
239.641303062	Sandbox	137.254.60.32	80
239.773968935	Sandbox	137.254.60.32	443
247.087513924	Sandbox	23.196.34.38	80
247.28245306	Sandbox	23.53.120.202	80
247.319762945	Sandbox	23.53.120.202	443
254.694878101	Sandbox	23.53.121.101	80
261.065455914	Sandbox	23.53.121.101	80
268.128782034	Sandbox	137.254.60.32	80
268.285707951	Sandbox	137.254.60.32	443
275.660758018	Sandbox	64.131.64.240	80

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
306.363467932	Sandbox	89.18.27.34	53
314.558212996	Sandbox	185.121.177.177	53
336.162167072	Sandbox	27.100.36.191	53
336.644699097	Sandbox	45.63.25.55	53
336.903470993	Sandbox	142.4.204.111	53
342.30073905	Sandbox	137.254.60.32	80
342.398343086	Sandbox	137.254.60.32	443
349.771625042	Sandbox	23.53.121.101	80
349.859850883	Sandbox	157.56.148.19	80
350.000142097	Sandbox	157.56.148.19	443
357.78777194	Sandbox	37.34.55.187	443
364.705796957	Sandbox	64.131.64.240	80

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
3.07305693626	Sandbox	224.0.0.252	5355
3.0734770298	Sandbox	224.0.0.252	5355
3.07978892326	Sandbox	192.168.56.255	137
3.08306193352	Sandbox	239.255.255.250	3702
5.62590289116	Sandbox	224.0.0.252	5355
9.12563109398	Sandbox	192.168.56.255	138
29.6069800854	Sandbox	224.0.0.252	5355
32.3137230873	Sandbox	8.8.4.4	53
33.5003728867	Sandbox	224.0.0.252	5355
36.17406106	Sandbox	8.8.4.4	53
41.4072880745	Sandbox	224.0.0.252	5355
50.1409609318	Sandbox	224.0.0.252	5355
56.9695820808	Sandbox	224.0.0.252	5355
59.6726610661	Sandbox	8.8.4.4	53
59.8189439774	Sandbox	8.8.4.4	53
63.8600831032	Sandbox	224.0.0.252	5355
114.376115084	Sandbox	224.0.0.252	5355
117.063308001	Sandbox	8.8.4.4	53
121.359613895	Sandbox	224.0.0.252	5355
124.001270056	Sandbox	8.8.4.4	53
124.203885078	Sandbox	8.8.4.4	53
130.125643969	Sandbox	224.0.0.252	5355

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
138.859689951	Sandbox	224.0.0.252	5355
147.016885996	Sandbox	224.0.0.252	5355
149.750701904	Sandbox	8.8.4.4	53
153.329449892	Sandbox	224.0.0.252	5355
161.531898022	Sandbox	224.0.0.252	5355
169.203346014	Sandbox	224.0.0.252	5355
176.235024929	Sandbox	224.0.0.252	5355
184.031753063	Sandbox	224.0.0.252	5355
219.062673092	Sandbox	224.0.0.252	5355
226.031487942	Sandbox	224.0.0.252	5355
236.813230038	Sandbox	224.0.0.252	5355
244.40644598	Sandbox	224.0.0.252	5355
247.047878027	Sandbox	8.8.4.4	53
247.225509882	Sandbox	8.8.4.4	53
251.922944069	Sandbox	224.0.0.252	5355
254.640990973	Sandbox	8.8.4.4	53
258.328453064	Sandbox	224.0.0.252	5355
265.31396389	Sandbox	224.0.0.252	5355
272.907044888	Sandbox	224.0.0.252	5355
279.62579298	Sandbox	224.0.0.252	5355
339.516716957	Sandbox	224.0.0.252	5355
346.969206095	Sandbox	224.0.0.252	5355
349.703707933	Sandbox	8.8.4.4	53
354.954014063	Sandbox	224.0.0.252	5355
357.672751904	Sandbox	8.8.4.4	53
361.984838963	Sandbox	224.0.0.252	5355
368.953433037	Sandbox	224.0.0.252	5355

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Roaming\Microsoft\Rwufbuia\Cafadrev.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 8deb4b389108c7990660db88b0dd5862 **SHA-1 :** f753a02962c14d6c7af61b620b8521500e0b4e81 **SHA-256 :** 1b6a98a7ba4e5fac878f2f8f284fa748c889fa4e4a **SHA-512 :** 79c7c4c4a9fed85be3d19d82f7897e845a1bb3c7 **Size :** 122.88 Kilobytes.

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	s927397.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	f753a02962c14d6c7af61b620b8521500e0b4e81
MD5:	8deb4b389108c7990660db88b0dd5862
First Seen Date:	2017-04-01 23:57:12.857246 (2 years ago)
Number Of Clients Seen:	10
Last Analysis Date:	2017-08-18 08:08:16.405370 (about a year ago)
Human Expert Analysis Result:	No human expert analysis verdict given to this sample yet.

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
File Type Enum	6
Number Of Sections	5
Compilation Time Stamp	0x58DF44C4 [Sat Apr 1 06:12:20 2017 UTC]
Entry Point	0x404177 (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	122880
Sha256	1b6a98a7ba4e5fac878f2f8f284fa748c889fa4e4a9a0905748144fffd890f4b
Mime Type	application/x-dosexec

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0xbf4d	0xc000	6.57299922548	e727ceb8eb9cd28fb0dafb4a43602f36
.rdata	0xd000	0x3e1e	0x4000	5.56526368978	fef5f402e7de1879d042f453e4a7408a
.data	0x11000	0x6128	0x1000	2.38953148986	5d51cd838df221f08b42306e4d8f5fe3
.tls	0x18000	0x9d9a	0xa000	5.62874338227	2db20fc5266f35810c1401a953e0b7bd
.rsrc	0x22000	0x1dc0	0x2000	3.17472017684	6dc3ae349ee7de576c052553d9e113fc

CERTIFICATE VALIDATION

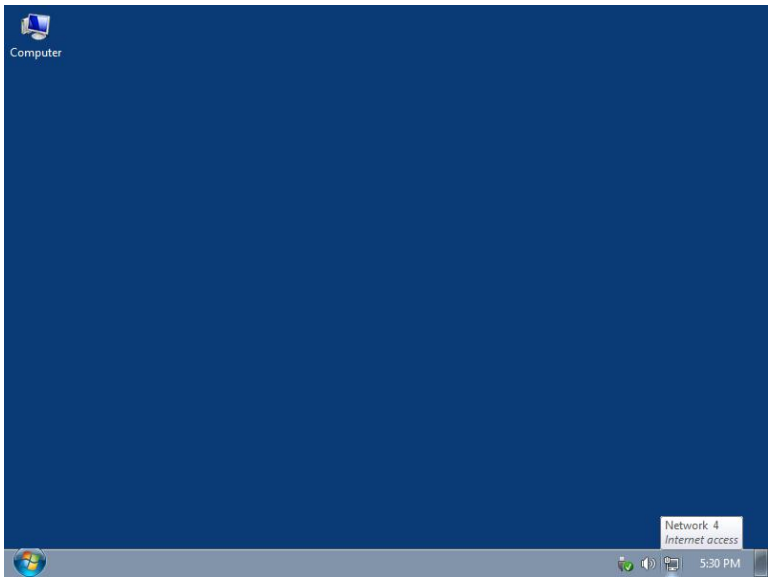
- Certificate Validation is not Applicable ?

SCREENSHOTS

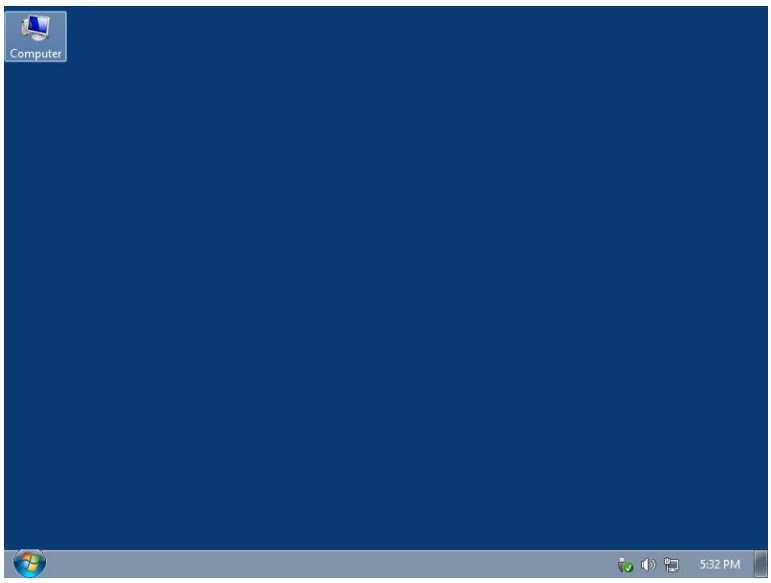

Computer
5:30 PM


Computer
5:32 PM


Computer
5:32 PM


Computer
Network 4
Internet access
5:30 PM


Computer
5:27 PM


Computer
5:32 PM


Computer
5:32 PM