VALKYRIE COMODO

Summary

File Name: amadey.exe

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

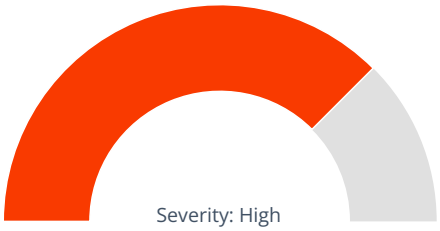
SHA1: 4bfee487fae3e4daf9eaaeea9c5e7469c4e94ec1

MD5: a7d7a53ac62cc85ecddf710da9243d64

MALWARE

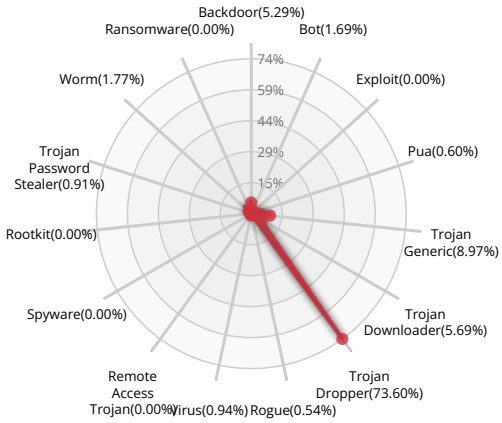
Valkyrie Final Verdict

DETECTION SECTION

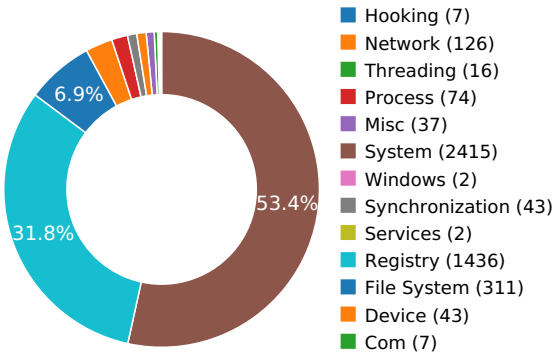


Verdict: Malware

CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW

VALKYRIE COMODO

Activity Details

INFORMATION DISCOVERY

Reads data out of its own binary image — Show sources

HIPS/ PFW/ OPERATING SYSTEM PROTECTION EVASION

Attempts to identify installed AV products by installation directory — Show sources

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

Creates RWX memory — Show sources

DATA OBFUSCATION

Drops a binary and executes it — Show sources

PERSISTENCE AND INSTALLATION BEHAVIOR

Attempts to interact with an Alternate Data Stream (ADS) — Show sources

MALWARE ANALYSIS SYSTEM EVASION

A process attempted to delay the analysis task by a long amount of time. — Show sources

Behavior Graph

VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

C:\Windows\System32\tzres.dll
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Program Files\Common Files\System\symsrv.dll
C:\Users\user\AppData\Local\Temp\A1D26E2
\Device\KsecDD
C:\Users\user\AppData\Local\Temp\CSpkp::Init - Aec init failed
C:\Windows\System32\CSpkp::Init - Aec init failed
C:\Windows\system\CSpkp::Init - Aec init failed
C:\Windows\CSpkp::Init - Aec init failed
C:\ProgramData\Oracle\Java\javapath\CSpkp::Init - Aec init failed
C:\Windows\System32\wbem\CSpkp::Init - Aec init failed
C:\Windows\System32\WindowsPowerShell\v1.0\CSpkp::Init - Aec init failed
C:\Program Files\Microsoft Network Monitor 3\CSpkp::Init - Aec init failed
C:\Program Files (x86)\Universal Extractor\CSpkp::Init - Aec init failed
C:\Program Files (x86)\Universal Extractor\bin\CSpkp::Init - Aec init failed
C:\Program Files (x86)\Windows Kits\8.1\Windows Performance Toolkit\CSpkp::Init - Aec init failed
C:\Python27\CSpkp::Init - Aec init failed
C:\Python27\Scripts\CSpkp::Init - Aec init failed
C:\tools\sysinternals\CSpkp::Init - Aec init failed
C:\tools\CSpkp::Init - Aec init failed
C:\tools\IDA_Pro_v6\python\CSpkp::Init - Aec init failed
C:\ProgramData\152122983033326607761225
C:\ProgramData\a5410c88f1\bween.exe
C:\ProgramData\a5410c88f1
C:\Users\user\AppData\Local\Temp\4bfee487fae3e4daf9eaaeea9c5e7469c4e94ec1.exe
\??\MountPointManager
C:\ProgramData\a5410c88f1\CSpkp::Init - Aec init failed
C:\Windows\SysWOW64\shell32.dll
C:\Windows\SysWOW64\ieframe.dll
C:\Program Files\Common Files\System\symsrv.dll.dat
C:\Users\user\AppData\Local\Temp\cmd.*
C:\Windows\System32\cmd.*

C:\
C:\Windows
C:\Windows\System32
C:\Windows\SysWOW64\cmd.exe
C:\Users\user\AppData\Local\Microsoft\Windows\Caches
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\cversions.1.db
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x000000000000004c.db
C:\Users\user\Desktop\desktop.ini
C:\Windows\SysWOW64\propsys.dll
C:\Windows\sysnative\propsys.dll
C:\Windows\System32\cmd.exe
C:\Windows\System32\cmd.exe:Zone.Identifier
C:\ProgramData\AVAST Software
C:\ProgramData\Avira
C:\ProgramData\Kaspersky Lab
C:\ProgramData\ESET
C:\ProgramData\Panda Security
C:\ProgramData\Doctor Web
C:\ProgramData\AVG
C:\ProgramData\360TotalSecurity
C:\ProgramData\Bitdefender
C:\ProgramData\Norton
C:\ProgramData\Sophos
C:\ProgramData\Comodo
C:\ProgramData\081f1236bf424f
C:\ProgramData\081f1236bf424f\cred.dll
C:\ProgramData\081f1236bf424f\scr.dll
C:\Users\user\AppData\Local\Temp
C:\Users
C:\Users\user
C:\Users\user\AppData
C:\Users\user\AppData\Local
C:\Users\user\AppData\Local\Temp\REG.*
C:\Users\user\AppData\Local\Temp\REG
C:\ProgramData\Oracle\Java\javapath\REG.*

C:\ProgramData\Oracle\Java\javapath\REG
C:\Windows\System32\REG.*
C:\Windows\System32\reg.COM
C:\Windows\System32\reg.exe
C:\Windows\SysWOW64\en-US\KERNELBASE.dll.mui

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Windows\AppInit_DLLs
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\SESSION MANAGER\SafeProcessSearchMode
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoPropertiesMyComputer
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoPropertiesRecycleBin
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoControlPanel
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoSetFolders
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoInternetIcon
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoCommonGroups
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{031E4825-7B94-4dc3-B131-E946B44C8DD5}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{04731B67-D933-450a-90E6-4ACD2E9408FE}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{11016101-E366-4D22-BC06-4ADA335C892B}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{26EE0668-A00A-44D7-9371-BEB064C98683}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{4336a54d-038b-4685-ab02-99bb52d3fb8b}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{450D8FBA-AD25-11D0-98A8-

0800361B1103}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{5399E694-6CE5-4D6C-8FCE-1D8870FDCBA0}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{645FF040-5081-101B-9F08-00AA002F954E}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{89D83576-6BD1-4c86-9454-BEB04E94C819}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{9343812e-1c37-4a49-a12e-4b2d810d956b}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{B4FB3F98-C1EA-428d-A78A-D1F5659CBA93}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{BD7A2E7B-21CB-41b2-A086-B309680C6B7E}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{daf95313-e44d-46af-be1b-cbacea2c3065}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{e345f35f-9397-435c-8f95-4e922c26259e}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{ED228FDF-9EA8-4870-83b1-96b02CFE0D52}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{F02C1A0D-BE21-4350-88B0-7367FC96EF3C}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\Attributes
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\CallForAttributes
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\RestrictedAttributes
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsFORDISPLAY
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HideFolderVerbs
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\UseDropHandler
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsFORPARSING
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsParseDisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\QueryForOverlay
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\MapNetDriveVerbs
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\QueryForInfoTip
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HideInWebView
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HideOnDesktopPerUser
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsAliasedNotifications
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsUniversalDelegate
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\NoFileFolderJunction
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\PinToNameSpaceTree
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HasNavigationEnum

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\NonEnum\{20D04FE0-3AEA-1069-A2D8-08002B30309D}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{208D2C60-3AEA-1069-A2D7-08002B30309D}\ShellFolder\Attributes
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{208D2C60-3AEA-1069-A2D7-08002B30309D}\ShellFolder\CallForAttributes
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{208D2C60-3AEA-1069-A2D7-08002B30309D}\ShellFolder\RestrictedAttributes
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{208D2C60-3AEA-1069-A2D7-08002B30309D}\ShellFolder\WantsFORDISPLAY
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{208D2C60-3AEA-1069-A2D7-08002B30309D}\ShellFolder\HideFolderVerbs
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{208D2C60-3AEA-1069-A2D7-08002B30309D}\ShellFolder\UseDropHandler
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{208D2C60-3AEA-1069-A2D7-08002B30309D}\ShellFolder\WantsFORPARSING
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{208D2C60-3AEA-1069-A2D7-08002B30309D}\ShellFolder\WantsParseDisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{208D2C60-3AEA-1069-A2D7-08002B30309D}\ShellFolder\QueryForOverlay
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{208D2C60-3AEA-1069-A2D7-08002B30309D}\ShellFolder\MapNetDriveVerbs
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{208D2C60-3AEA-1069-A2D7-08002B30309D}\ShellFolder\QueryForInfoTip
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{208D2C60-3AEA-1069-A2D7-08002B30309D}\ShellFolder\HideInWebView
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{208D2C60-3AEA-1069-A2D7-08002B30309D}\ShellFolder\HideOnDesktopPerUser
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{208D2C60-3AEA-1069-A2D7-08002B30309D}\ShellFolder\WantsAliasedNotifications
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{208D2C60-3AEA-1069-A2D7-08002B30309D}\ShellFolder\WantsUniversalDelegate
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{208D2C60-3AEA-1069-A2D7-08002B30309D}\ShellFolder\NoFileFolderJunction
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{208D2C60-3AEA-1069-A2D7-08002B30309D}\ShellFolder\PinToNameSpaceTree
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{208D2C60-3AEA-1069-A2D7-08002B30309D}\ShellFolder\HasNavigationEnum
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\NonEnum\{208D2C60-3AEA-1069-A2D7-08002B30309D}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{871C5380-42A0-1069-A2EA-08002B30309D}\ShellFolder\Attributes
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{871C5380-42A0-1069-A2EA-08002B30309D}\ShellFolder\CallForAttributes
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{871C5380-42A0-1069-A2EA-08002B30309D}\ShellFolder\RestrictedAttributes

MODIFIED FILES

C:\ProgramData\152122983033326607761225
C:\ProgramData\a5410c88f1\bween.exe
C:\ProgramData\081f1236bf424f\cred.dll
C:\ProgramData\081f1236bf424f\scr.dll

RESOLVED APIS

kernel32.dll.OpenProcess
kernel32.dll.TerminateProcess
kernel32.dll.WriteProcessMemory
kernel32.dll.VirtualAllocEx
advapi32.dll.AdjustTokenPrivileges

user32.dll.MessageBoxTimeoutW
wintrust.dll.WinVerifyTrust
kernel32.dll.CreateProcessInternalW
kernel32.dll.SortGetHandle
kernel32.dll.SortCloseHandle
ws2help.dll.WahReferenceContextByHandle
ntdll.dll.KiUserExceptionDispatcher
cryptbase.dll.SystemFunction036
uxtheme.dll.ThemeInitApiHook
user32.dll.IsProcessDPIAware
kernel32.dll.VirtualAlloc
kernel32.dll.VirtualProtect
kernel32.dll.LoadLibraryA
kernel32.dll.VirtualFree
kernel32.dll.VirtualQuery
kernel32.dll.TerminateThread
kernel32.dll.GetTempPathW
kernel32.dll.CreateMutexW
kernel32.dll.WaitForSingleObject
kernel32.dll.CreateFileW
kernel32.dll.GetVersionExW
kernel32.dll.SuspendThread
kernel32.dll.GetComputerNameExW
kernel32.dll.ResumeThread
kernel32.dll.GetModuleHandleA
kernel32.dll.Sleep
kernel32.dll.GetLastError
kernel32.dll.GetFileAttributesA
kernel32.dll.CreateFileA
kernel32.dll.CloseHandle
kernel32.dll.GetSystemInfo
kernel32.dll.LoadLibraryW
kernel32.dll.GetModuleFileNameW
kernel32.dll.HeapAlloc

kernel32.dll.GetThreadContext
kernel32.dll.GetProcAddress
kernel32.dll.LocalFree
kernel32.dll.ReadProcessMemory
kernel32.dll.GetComputerNameW
kernel32.dll.GetProcessHeap
kernel32.dll.GetModuleHandleW
kernel32.dll.FreeLibrary
kernel32.dll.CreateProcessA
kernel32.dll.CreateDirectoryA
kernel32.dll.SetThreadContext
kernel32.dll.WriteConsoleW
kernel32.dll.SetEndOfFile
kernel32.dll.HeapReAlloc
kernel32.dll.WriteFile
kernel32.dll.HeapFree
kernel32.dll.CreateThread
kernel32.dll.GetModuleFileNameA
kernel32.dll.HeapSize
kernel32.dll.GetTimeZoneInformation
kernel32.dll.FlushFileBuffers
kernel32.dll.GetStringTypeW
kernel32.dll.SetEnvironmentVariableW
kernel32.dll.FreeEnvironmentStringsW
kernel32.dll.GetEnvironmentStringsW
kernel32.dll.WideCharToMultiByte
kernel32.dll.GetCPInfo
kernel32.dll.UnhandledExceptionFilter
kernel32.dll.SetUnhandledExceptionFilter
kernel32.dll.GetCurrentProcess
kernel32.dll.IsProcessorFeaturePresent
kernel32.dll.IsDebuggerPresent
kernel32.dll.GetStartupInfoW
kernel32.dll.QueryPerformanceCounter
kernel32.dll.GetCurrentProcessId

kernel32.dll.GetCurrentThreadId
kernel32.dll.GetSystemTimeAsFileTime

DELETED REGISTRY KEYS

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName

REGISTRY KEYS

HKEY_LOCAL_MACHINE\software\microsoft\windows nt\currentversion\windows
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Windows\AppInit_DLLs
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\SESSION MANAGER\SafeProcessSearchMode
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Applications\4bfee487fae3e4daf9eaaeea9c5e7469c4e94ec1.exe
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Generation
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\Windows\CurrentVersion\ShellCompatibility\Applications\bween.exe
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoPropertiesMyComputer
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoPropertiesRecycleBin

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoControlPanel
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoSetFolders
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoInternetIcon
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\SideBySide
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoCommonGroups
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\Desktop\NameSpace\DelegateFolders
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\Desktop\NameSpace
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{031E4825-7B94-4dc3-B131-E946B44C8DD5}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{031E4825-7B94-4dc3-B131-E946B44C8DD5}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{04731B67-D933-450a-90E6-4ACD2E9408FE}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{04731B67-D933-450a-90E6-4ACD2E9408FE}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{11016101-E366-4D22-BC06-4ADA335C892B}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{11016101-E366-4D22-BC06-4ADA335C892B}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{26EE0668-A00A-44D7-9371-BEB064C98683}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{26EE0668-A00A-44D7-9371-BEB064C98683}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{4336a54d-038b-4685-ab02-99bb52d3fb8b}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{4336a54d-038b-4685-ab02-99bb52d3fb8b}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{450D8FBA-AD25-11D0-98A8-0800361B1103}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{450D8FBA-AD25-11D0-98A8-0800361B1103}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{5399E694-6CE5-4D6C-8FCE-1D8870FDCBA0}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{5399E694-6CE5-4D6C-8FCE-1D8870FDCBA0}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{59031a47-3f72-44a7-89c5-5595fe6b30ee}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{645FF040-5081-101B-9F08-00AA002F954E}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{645FF040-5081-101B-9F08-00AA002F954E}\SuppressionPolicy

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{89D83576-6BD1-4c86-9454-BEB04E94C819}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{89D83576-6BD1-4c86-9454-BEB04E94C819}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{9343812e-1c37-4a49-a12e-4b2d810d956b}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{9343812e-1c37-4a49-a12e-4b2d810d956b}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{B4FB3F98-C1EA-428d-A78A-D1F5659CBA93}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{B4FB3F98-C1EA-428d-A78A-D1F5659CBA93}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{BD7A2E7B-21CB-41b2-A086-B309680C6B7E}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{BD7A2E7B-21CB-41b2-A086-B309680C6B7E}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{daf95313-e44d-46af-be1b-cbacea2c3065}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{daf95313-e44d-46af-be1b-cbacea2c3065}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{e345f35f-9397-435c-8f95-4e922c26259e}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{e345f35f-9397-435c-8f95-4e922c26259e}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{ED228FDF-9EA8-4870-83b1-96b02CFE0D52}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{ED228FDF-9EA8-4870-83b1-96b02CFE0D52}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{F02C1A0D-BE21-4350-88B0-7367FC96EF3C}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{F02C1A0D-BE21-4350-88B0-7367FC96EF3C}\SuppressionPolicy
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Desktop\NameSpace
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Desktop\NameSpace\DelegateFolders
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\Desktop\NameSpace
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\Desktop\NameSpace\DelegateFolders
HKEY_CLASSES_ROOT\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\Attributes
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\CallForAttributes
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\RestrictedAttributes

EXECUTED COMMANDS

C:\ProgramData\a5410c88f1\bween.exe
"C:\Windows\System32\cmd.exe" /C REG ADD "HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders" /f /v Startup /t REG_SZ /d C:\ProgramData\a5410c88f1\
cmd /C REG ADD "HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders" /f /v Startup /t REG_SZ /d C:\ProgramData\a5410c88f1\
C:\Windows\system32\reg.exe REG ADD "HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders" /f /v Startup /t REG_SZ /d C:\ProgramData\a5410c88f1\

READ FILES

C:\Windows\System32\tzres.dll
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Program Files\Common Files\System\symsrv.dll
\Device\KsecDD
C:\ProgramData\152122983033326607761225
C:\ProgramData\a5410c88f1\bween.exe
C:\Users\user\AppData\Local\Temp\4bfee487fae3e4daf9eaaeea9c5e7469c4e94ec1.exe
C:\Windows\SysWOW64\shell32.dll
C:\Windows\SysWOW64\ieframe.dll
C:\
C:\Windows
C:\Windows\System32
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\cversions.1.db
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x000000000000004c.db
C:\Users\user\Desktop\desktop.ini
C:\ProgramData\081f1236bf424f\cred.dll
C:\ProgramData\081f1236bf424f\scr.dll
C:\Windows\SysWOW64\en-US\KERNELBASE.dll.mui

MUTEXES

152122983033326607761225
Local\ZoneAttributeCacheCounterMutex
Local\ZonesCacheCounterMutex
Local\ZonesLockedCacheCounterMutex
IESQMMUTEX_0_208

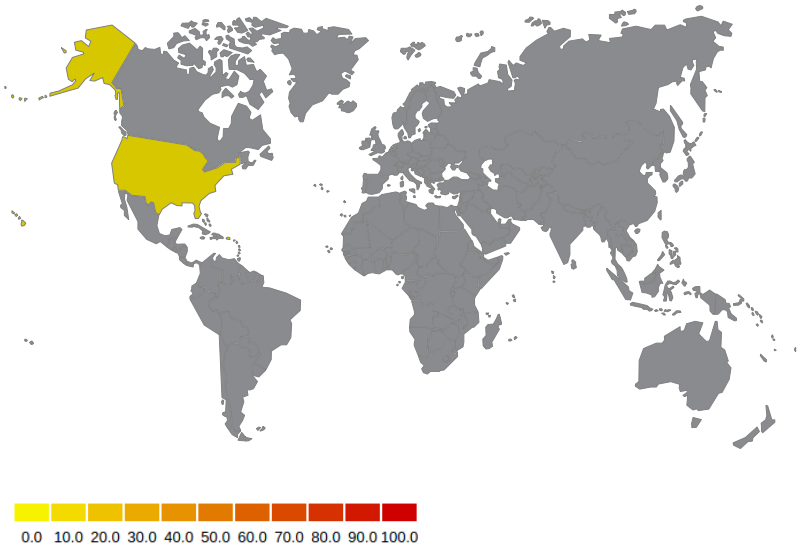
MODIFIED REGISTRY KEYS

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect

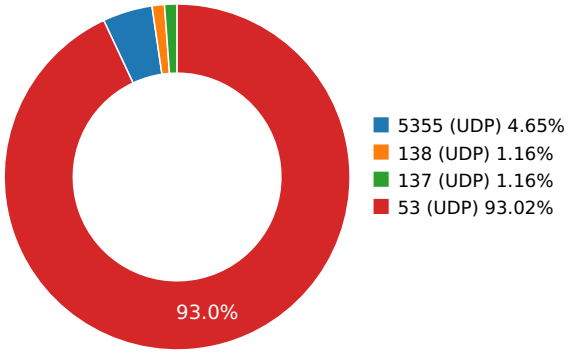
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\Startup

Network Behavior

CONTACTED IPS



NETWORK PORT DISTRIBUTION



Name	IP	Country	ASN	ASN Name	Trigger Process Type
	8.8.4.4	United States	15169	Google LLC	Malware Process
	8.8.8.8	United States	15169	Google LLC	Malware Process
					Malware Process
www.aieov.com	45.33.20.235	United States	63949	Akamai Technologies, Inc.	Malware Process
					Malware Process

DNS QUERIES

Request	Type
5isohu.com	A
jmucha.fun	A
www.aieov.com	A

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
7.128439188	Sandbox	224.0.0.252	5355
7.14226317406	Sandbox	224.0.0.252	5355
7.20607304573	Sandbox	192.168.56.255	137
7.50743317604	Sandbox	224.0.0.252	5355
9.78229999542	Sandbox	224.0.0.252	5355
10.3722991943	Sandbox	8.8.4.4	53
11.3602621555	Sandbox	8.8.8.8	53

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
13.2200469971	Sandbox	192.168.56.255	138
13.5503230095	Sandbox	8.8.4.4	53
14.547672987	Sandbox	8.8.8.8	53
24.779309988	Sandbox	8.8.8.8	53
25.7665250301	Sandbox	8.8.4.4	53
27.8388850689	Sandbox	8.8.8.8	53
28.8284139633	Sandbox	8.8.4.4	53
39.1654801369	Sandbox	8.8.8.8	53
40.1564509869	Sandbox	8.8.4.4	53
42.1031951904	Sandbox	8.8.8.8	53
43.0938880444	Sandbox	8.8.4.4	53
53.8704249859	Sandbox	8.8.8.8	53
54.8600711823	Sandbox	8.8.4.4	53
56.3499760628	Sandbox	8.8.8.8	53
57.3441259861	Sandbox	8.8.4.4	53
68.2460169792	Sandbox	8.8.8.8	53
69.2346131802	Sandbox	8.8.4.4	53
80.6175191402	Sandbox	8.8.8.8	53
81.6100451946	Sandbox	8.8.4.4	53
82.6561920643	Sandbox	8.8.8.8	53
83.6412651539	Sandbox	8.8.4.4	53
100.936346054	Sandbox	8.8.8.8	53
101.922600985	Sandbox	8.8.4.4	53
104.91676116	Sandbox	8.8.8.8	53
105.907229185	Sandbox	8.8.4.4	53
115.361483097	Sandbox	8.8.8.8	53
116.360136032	Sandbox	8.8.4.4	53
129.27610898	Sandbox	8.8.8.8	53
129.773238182	Sandbox	8.8.8.8	53
130.266350031	Sandbox	8.8.4.4	53
130.766164064	Sandbox	8.8.4.4	53
148.026664019	Sandbox	8.8.8.8	53
149.016381025	Sandbox	8.8.4.4	53
153.57178998	Sandbox	8.8.8.8	53
154.563889027	Sandbox	8.8.4.4	53
162.409013033	Sandbox	8.8.8.8	53
163.407029152	Sandbox	8.8.4.4	53

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
176.798009157	Sandbox	8.8.8.8	53
177.797140121	Sandbox	8.8.4.4	53
177.847620964	Sandbox	8.8.8.8	53
178.844577074	Sandbox	8.8.4.4	53
195.111328125	Sandbox	8.8.8.8	53
196.109985113	Sandbox	8.8.4.4	53
202.211158991	Sandbox	8.8.8.8	53
203.203536987	Sandbox	8.8.4.4	53
209.479840994	Sandbox	8.8.8.8	53
210.469871998	Sandbox	8.8.4.4	53
223.868177176	Sandbox	8.8.8.8	53
224.859731197	Sandbox	8.8.4.4	53
226.51100111	Sandbox	8.8.8.8	53
227.500899076	Sandbox	8.8.4.4	53
242.135495186	Sandbox	8.8.8.8	53
243.125540972	Sandbox	8.8.4.4	53
250.789303064	Sandbox	8.8.8.8	53
251.781556129	Sandbox	8.8.4.4	53
256.490233183	Sandbox	8.8.8.8	53
257.485217094	Sandbox	8.8.4.4	53
270.887237072	Sandbox	8.8.8.8	53
271.875416994	Sandbox	8.8.4.4	53
275.06733799	Sandbox	8.8.8.8	53
276.063439131	Sandbox	8.8.4.4	53
289.173009157	Sandbox	8.8.8.8	53
290.172751188	Sandbox	8.8.4.4	53
299.363840103	Sandbox	8.8.8.8	53
300.360061169	Sandbox	8.8.4.4	53
303.539348125	Sandbox	8.8.8.8	53
304.532278061	Sandbox	8.8.4.4	53
317.950067043	Sandbox	8.8.8.8	53
318.938089132	Sandbox	8.8.4.4	53
323.656213045	Sandbox	8.8.8.8	53
324.641093969	Sandbox	8.8.4.4	53
332.355468035	Sandbox	8.8.8.8	53
333.344280005	Sandbox	8.8.4.4	53
346.718199968	Sandbox	8.8.8.8	53

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
347.705048084	Sandbox	8.8.4.4	53
347.94887805	Sandbox	8.8.8.8	53
348.938286066	Sandbox	8.8.4.4	53
361.114176989	Sandbox	8.8.8.8	53
362.109645128	Sandbox	8.8.4.4	53

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
C:\ProgramData\152122983033326607761225	**Type :** empty **MD5 :** d41d8cd98f00b204e9800998ecf8427e **SHA-1 :** da39a3ee5e6b4b0d3255bfef95601890afd80709 **SHA-256 :** e3b0c44298fc1c149afbf4c8996fb92427ae41e46 **SHA-512 :** cf83e1357eefb8bdf1542850d66d8007d620e405 **Size :** 0.0 Kilobytes.
C:\ProgramData\A5410c88f1\Bween.Exe	**Type :** PE32 executable (console) Intel 80386, for MS Windows **MD5 :** 03282c8244929f69919172ad44e31f84 **SHA-1 :** 12975be32e08b2c41de734576269d8724489ceec **SHA-256 :** d9492cc815fbadc468eab21ade82e6e89c94a90b **SHA-512 :** 99b60116c3501755561e7e63ef737dea9b203f98 **Size :** 332.231 Kilobytes.

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	amadey.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
SHA1:	4bfee487fae3e4daf9eaaeea9c5e7469c4e94ec1
MD5:	a7d7a53ac62cc85ecddf710da9243d64
First Seen Date:	2024-10-07 21:53:11.782088 (10 days ago)
Number Of Clients Seen:	4
Last Analysis Date:	2024-10-07 21:54:22.097442 (10 days ago)
Human Expert Analysis Date:	2024-10-08 16:53:29.555860 (10 days ago)
Human Expert Analysis Result:	Malware

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Magic Literal Enum	1
File Type Enum	6
Debug Artifacts	[]
Number Of Sections	4
Trid	[]
Compilation Time Stamp	0x5B8FBD2F [Wed Sep 5 11:25:35 2018 UTC]
Entry Point	0x40b4ac (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	253952
Ssdeep	
Sha256	d20d9c4ca508991a5a3482ff1545ba5f39c96892538f3a50b720259f446dfee3
Exifinfo	[]
Mime Type	application/x-dosexec
Imphash	

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0xa6b2	0xb000	5.95248153087	bdb56d01ded2dcd8e4292f819605974f
.rdata	0xc000	0x1d3e	0x2000	4.75158560177	2d70851720d8f8a9f6108986b0b2db10
.data	0xe000	0x2a6d4	0x26000	6.05296926408	a6373ea6e32e2e27cbd57587d7de65ad
.rsrc	0x39000	0x9e50	0xa000	3.44029584982	da5219f474a3232b8c4660c5e4bc96a8

PE Resources

{u'lang': u'LANG_ENGLISH', u'name': u'RT_BITMAP', u'offset': 266360, u'sha256': u'3dbd6d218cf1ebe266ae51000d8c9192ac33ce14f43974d2f01ec9e414d0d0bb', u'type': u'data', u'size': 7640}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 234328, u'sha256': u'0435ca68145e22f9cbee997f643ad0093fa74fe558ebd44b30bbdee0dfbc9a95', u'type': u'dBase IV DBT of \\200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 4290769151, next used block 4294942975', u'size': 16936}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 251264, u'sha256': u'd280e3381b3bc87509f45a1db09a92fe59363f7111b87e245a4e724cc8a35031', u'type': u'data', u'size': 9640}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 260904, u'sha256': u'8cad298c32251e8df48bdb595d043c280c948cea8cb397babc57552859c4fc78', u'type': u'data', u'size': 4264}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 265168, u'sha256': u'0b312afd4a5d698137e6cd3bf881f03b821db2e293998d5bed0873d71498da7e', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1128}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_ICON', u'offset': 266296, u'sha256': u'822952416183dc59088127325e52faebc96d08a97d76bd9202cc4880de84f48e', u'type': u'MS Windows icon resource - 4 icons, 64x64', u'size': 62}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_MANIFEST', u'offset': 233920, u'sha256': u'9ac0a1988e871fb0c5001cc9f749c91a3840e7c8e2e3d00bc202f4d1b38e41b5', u'type': u'XML 1.0 document, ASCII text, with CRLF line terminators', u'size': 405}

CERTIFICATE VALIDATION

- Certificate Validation is not Applicable ?

SCREENSHOTS