cape

Info File Signatures Screenshots Network Dropped Payloads Behavior Volatility

Category	Started On	Completed On	Duration	Cuckoo Version
FILE	2023-07-20 10:33:55	2023-07-20 10:36:43	168 seconds	2.4-CAPE

Machine	Label	Manager	Started On	Shutdown On
cape1	win7x64_5	KVM	2023-07-20 10:33:56	2023-07-20 10:36:43

File Details

Filename	**tmpbxngrffp**
File Type	**PE32+ executable (GUI) x86-64, for MS Windows**
File Size	**6413824 bytes**
MD5	b49c653075331a6fa0d8e44e31dc5703
SHA1	4287b96b44782894058307ec9cd93a939adda5a5
SHA256	c7dca4b2f45bf67275cd8530b0f43a63a37ae25c474a52e37fc00ece67e5edbf [VT] [MWDB] [Bazaar]
SHA3-384	5e798420c322fa6ebfc6b9bc52a2c45f799c07620fd7d5466d4163411e9dbe12c35cb21bdf36ccf22cdfa78b0e75fff8
CRC32	9EB119B4
TLSH	T19C56334252F9A973D25A71B81DD1CD8D63C2143AC6C6D910C72A13FBBFB12296EBE0C5
Ssdeep	196608:nO6MXgtpVMkFnz7v7pLCmjlvO5o6/3PV+wF:nObgvVtjpmmjlWo9w
CAPE Yara	• UPX - Author: Kevin Breen <kevin@techanarchy.net>
PE	Strings

Signatures

Possible date expiration check, exits too soon after checking local time

Dynamic (imported) function loading detected

Reads data out of its own binary image

Created network traffic indicative of malicious activity

Screenshots

No screenshots available.

Network Analysis

TCP Connections

UDP Connections

Nothing to display.

Dropped Files

Nothing to display.

Payloads

Nothing to display.

Behavior Summary

Mutexes

Nothing to display.

Executed Commands

- C:\Users\Louise\AppData\Local\Packages\Microsoft.AsyncTextService_CkOpiRbdkmmxZ\AppData\sidebar.exe

Created Services

Nothing to display.

Started Services

Nothing to display.

Processes

registry filesystem process threading services device network synchronization crypto browser

tmpbxngrffp.exe PID: 2484, Parent PID: 1848, Full Path: **C:\Users\Louise\AppData\Local\Temp\tmpbxngrffp.exe** , Command Line: **"C:\Users\Louise\AppData\Local\Temp\tmpbxngrffp.exe"**

sidebar.exe PID: 3008, Parent PID: 2484, Full Path: **C:\Users\Louise\AppData\Local\Packages\Microsoft.AsyncTextService_CkOpiRbdkmmxZ\AppData\sidebar.exe** , Command Line: **C:\Users\Louise\AppData\Local\Packages\Microsoft.AsyncTextService_CkOpiRbdkmmxZ\AppData\sidebar.exe**

Accessed Files

- \Device\KsecDD
- C:\Windows\sysnative\WSHTCPIP.DLL
- C:\Windows\sysnative\wship6.dll
- C:\Windows\sysnative\wshqos.dll
- C:\Windows\sysnative\tzres.dll
- C:\Windows\sysnative\en-US\KERNELBASE.dll.mui
- \??\PHYSICALDRIVE0
- C:\Users\Louise\AppData\Local\Packages\Microsoft.AsyncTextService_CkOpiRbdkmmxZ\AppData
- C:\Users\Louise\AppData\Local\Packages\Microsoft.AsyncTextService_CkOpiRbdkmmxZ
- C:\Users\Louise\AppData\Local\Packages
- C:\Users\Louise\AppData\Local
- C:\Users\Louise\AppData\Local\Packages\Microsoft.AsyncTextService_CkOpiRbdkmmxZ\AppData\sidebar.exe
- C:\Users\Louise\AppData\Local\Temp\tmpbxngrffp.exe
- \??\NUL

Read Files

Nothing to display.

Modified Files

Nothing to display.

Deleted Files

- C:\Users\Louise\AppData\Local\Temp\tmpbxngrffp.exe

Registry Keys

- DisableUserModeCallbackFilter
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-1339698970-4093829097-1161395185-1000
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-1339698970-4093829097-1161395185-1000\ProfileImagePath
- HKEY_CURRENT_USER\Software\Microsoft\FixDrive\Registration\path
- HKEY_CURRENT_USER\Software\Microsoft\FixDrive\Registration\path
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\MicrosoftFixDrive
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\MicrosoftFixDrive

Read Registry Keys

- DisableUserModeCallbackFilter
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-1339698970-4093829097-1161395185-1000\ProfileImagePath

Modified Registry Keys

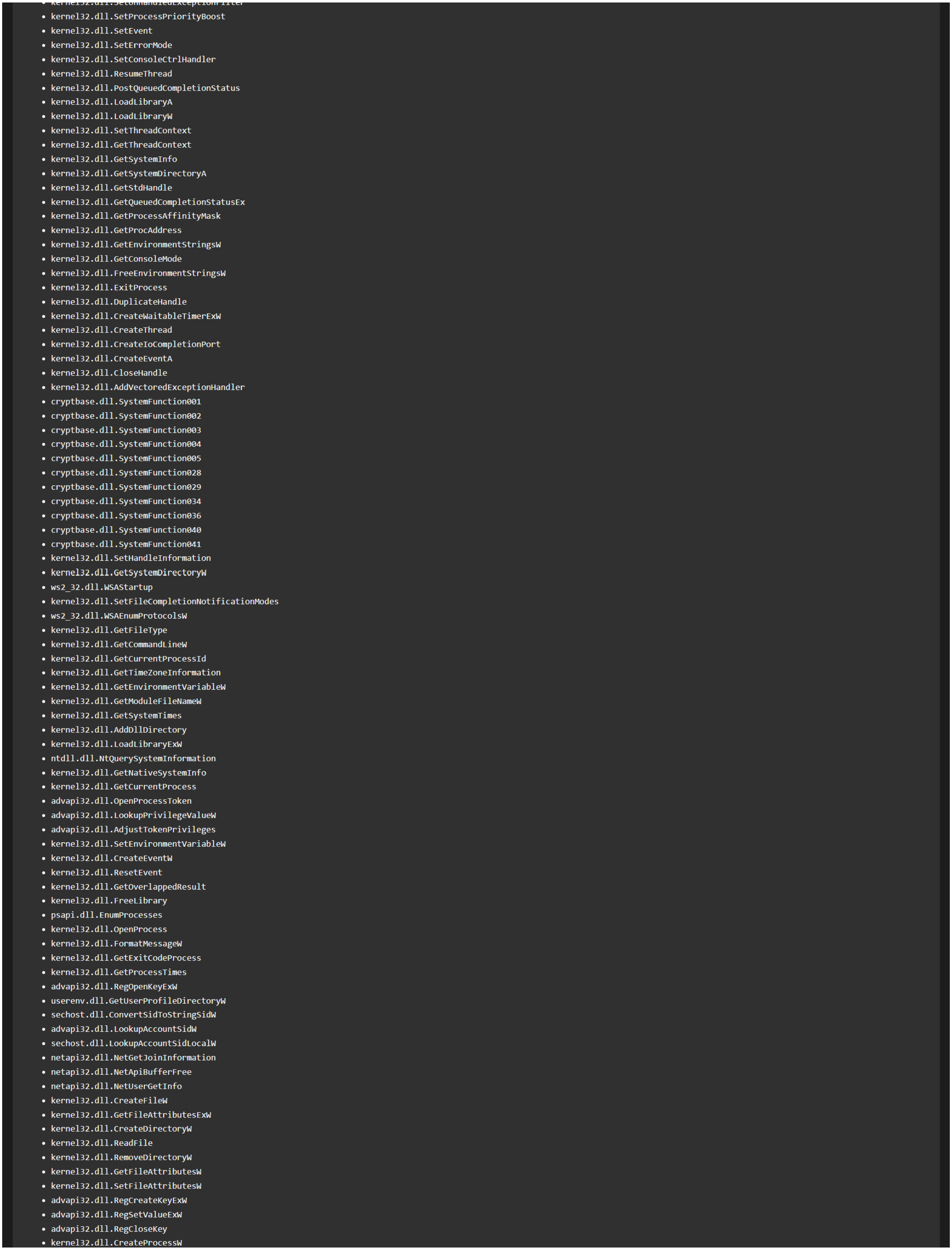
Nothing to display.

Deleted Registry Keys

Nothing to display.

Resolved APIs

- kernel32.dll.WriteFile
- kernel32.dll.WriteConsoleW
- kernel32.dll.WaitForMultipleObjects
- kernel32.dll.WaitForSingleObject
- kernel32.dll.VirtualQuery
- kernel32.dll.VirtualFree
- kernel32.dll.VirtualAlloc
- kernel32.dll.SwitchToThread
- kernel32.dll.SuspendThread
- kernel32.dll.Sleep
- kernel32.dll.SetWaitableTimer
- kernel32.dll.SetUnhandledExceptionFilter



- kernel32.dll.SetUnhandledExceptionFilter
- kernel32.dll.SetProcessPriorityBoost
- kernel32.dll.SetEvent
- kernel32.dll.SetErrorMode
- kernel32.dll.SetConsoleCtrlHandler
- kernel32.dll.ResumeThread
- kernel32.dll.PostQueuedCompletionStatus
- kernel32.dll.LoadLibraryA
- kernel32.dll.LoadLibraryW
- kernel32.dll.SetThreadContext
- kernel32.dll.GetThreadContext
- kernel32.dll.GetSystemInfo
- kernel32.dll.GetSystemDirectoryA
- kernel32.dll.GetStdHandle
- kernel32.dll.GetQueuedCompletionStatusEx
- kernel32.dll.GetProcessAffinityMask
- kernel32.dll.GetProcAddress
- kernel32.dll.GetEnvironmentStringsW
- kernel32.dll.GetConsoleMode
- kernel32.dll.FreeEnvironmentStringsW
- kernel32.dll.ExitProcess
- kernel32.dll.DuplicateHandle
- kernel32.dll.CreateWaitableTimerExW
- kernel32.dll.CreateThread
- kernel32.dll.CreateIoCompletionPort
- kernel32.dll.CreateEventA
- kernel32.dll.CloseHandle
- kernel32.dll.AddVectoredExceptionHandler
- cryptbase.dll.SystemFunction001
- cryptbase.dll.SystemFunction002
- cryptbase.dll.SystemFunction003
- cryptbase.dll.SystemFunction004
- cryptbase.dll.SystemFunction005
- cryptbase.dll.SystemFunction028
- cryptbase.dll.SystemFunction029
- cryptbase.dll.SystemFunction034
- cryptbase.dll.SystemFunction036
- cryptbase.dll.SystemFunction040
- cryptbase.dll.SystemFunction041
- kernel32.dll.SetHandleInformation
- kernel32.dll.GetSystemDirectoryW
- ws2_32.dll.WSAStartup
- kernel32.dll.SetFileCompletionNotificationModes
- ws2_32.dll.WSAEnumProtocolsW
- kernel32.dll.GetFileType
- kernel32.dll.GetCommandLineW
- kernel32.dll.GetCurrentProcessId
- kernel32.dll.GetTimeZoneInformation
- kernel32.dll.GetEnvironmentVariableW
- kernel32.dll.GetModuleFileNameW
- kernel32.dll.GetSystemTimes
- kernel32.dll.AddDllDirectory
- kernel32.dll.LoadLibraryExW
- ntdll.dll.NtQuerySystemInformation
- kernel32.dll.GetNativeSystemInfo
- kernel32.dll.GetCurrentProcess
- advapi32.dll.OpenProcessToken
- advapi32.dll.LookupPrivilegeValueW
- advapi32.dll.AdjustTokenPrivileges
- kernel32.dll.SetEnvironmentVariableW
- kernel32.dll.CreateEventW
- kernel32.dll.ResetEvent
- kernel32.dll.GetOverlappedResult
- kernel32.dll.FreeLibrary
- psapi.dll.EnumProcesses
- kernel32.dll.OpenProcess
- kernel32.dll.FormatMessageW
- kernel32.dll.GetExitCodeProcess
- kernel32.dll.GetProcessTimes
- advapi32.dll.RegOpenKeyExW
- userenv.dll.GetUserProfileDirectoryW
- sechost.dll.ConvertSidToStringSidW
- advapi32.dll.LookupAccountSidW
- sechost.dll.LookupAccountSidLocalW
- netapi32.dll.NetGetJoinInformation
- netapi32.dll.NetApiBufferFree
- netapi32.dll.NetUserGetInfo
- kernel32.dll.CreateFileW
- kernel32.dll.GetFileAttributesExW
- kernel32.dll.CreateDirectoryW
- kernel32.dll.ReadFile
- kernel32.dll.RemoveDirectoryW
- kernel32.dll.GetFileAttributesW
- kernel32.dll.SetFileAttributesW
- advapi32.dll.RegCreateKeyExW
- advapi32.dll.RegSetValueExW
- advapi32.dll.RegCloseKey
- kernel32.dll.CreateProcessW

CAPE Sandbox on Github

Back to top