cape

Info File Signatures Screenshots Network Dropped Payloads Behavior Volatility

Category	Started On	Completed On	Duration	Cuckoo Version
FILE	2023-07-20 10:41:31	2023-07-20 10:44:19	168 seconds	2.4-CAPE

Machine	Label	Manager	Started On	Shutdown On
cape3	win7x64_3	KVM	2023-07-20 10:41:33	2023-07-20 10:44:19

File Details

Filename	**tmp6adntozy**
File Type	**PE32+ executable (GUI) x86-64, for MS Windows**
File Size	**6412288 bytes**
MD5	9f8942b2ea33b0e94917bce84a3c0348
SHA1	53f9604dc9df82ce68a544400359e6ce3e8c5cff
SHA256	7f3802a43a160267fc8c9140b3fa607ed5b9673b586c0b4b29690d53a95007df [VT] [MWDB] [Bazaar]
SHA3-384	7a31317baa4fad315b030ff5a2c522171de6530a965721fca5ad08f429b1cee25d77556d831001f4713ff938592bafe2
CRC32	1BBF53AB
TLSH	T1525633AAB9A55D28D1FCC6FB743423C85492E1EDC5D5B1C5FB7D3298B2AD2E1420C3A0
Ssdeep	98304:qMd0w57FwW6s9li7x7NzYyyXZ2+TtX4/BgpPp6n4hjleFBvvvTnaL5KGxN:RzCWx941CrX/to/BM64rMvvTnazxN
CAPE Yara	• UPX - Author: Kevin Breen <kevin@techanarchy.net>
PE	Strings

Signatures

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

Hosts Involved

TCP Connections

UDP Connections

Dropped Files

Nothing to display.

Payloads

Nothing to display.

Behavior Summary

Mutexes
Nothing to display.

Executed Commands
- C:\Users\Louise\AppData\Local\Packages\Adobe.Reader_kjk3yPVltS80i\AppData\jusched.exe

Created Services
Nothing to display.

Started Services
Nothing to display.

Processes

registry filesystem process threading services device network synchronization crypto browser

tmp6adntozy.exe PID: 2060, Parent PID: 1984, Full Path: **C:\Users\Louise\AppData\Local\Temp\tmp6adntozy.exe** , Command Line: **"C:\Users\Louise\AppData\Local\Temp\tmp6adntozy.exe"**

jusched.exe PID: 1752, Parent PID: 2060, Full Path: **C:\Users\Louise\AppData\Local\Packages\Adobe.Reader_kjk3yPVltS80i\AppData\jusched.exe** , Command Line: **C:\Users\Louise\AppData\Local\Packages\Adobe.Reader_kjk3yPVltS80i\AppData\jusched.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
- \??\PHYSICALDRIVE0
- C:\Users\Louise\AppData\Local\Packages\Adobe.Reader_kjk3yPVltS80i\AppData
- C:\Users\Louise\AppData\Local\Packages\Adobe.Reader_kjk3yPVltS80i
- C:\Users\Louise\AppData\Local\Packages
- C:\Users\Louise\AppData\Local
- C:\Users\Louise\AppData\Local\Packages\Adobe.Reader_kjk3yPVltS80i\AppData\jusched.exe
- C:\Users\Louise\AppData\Local\Temp\tmp6adntozy.exe
- \??\NUL
- C:\Windows\sysnative\en-US\KERNELBASE.dll.mui

Read Files
Nothing to display.

Modified Files
Nothing to display.

Deleted Files
- C:\Users\Louise\AppData\Local\Temp\tmp6adntozy.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.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
- advapi32.dll.GetTokenInformation
- advapi32.dll.ConvertSidToStringSidW
- kernel32.dll.LocalFree
- 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.DeleteFileW
- kernel32.dll.RemoveDirectoryW
- kernel32.dll.GetFileAttributesW
- kernel32.dll.SetFileAttributesW
- advapi32.dll.RegCreateKeyExW
- advapi32.dll.RegSetValueExW
- advapi32.dll.RegCloseKey

- kernel32.dll.CreateProcessW