ID: 829696
Sample Name: onedrive.bat.exe
Cookbook: default.jbs
Time: 00:09:28
Date: 19/03/2023
Version: 37.0.0 Beryl

Table of Contents

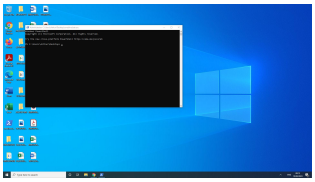
Windows Analysis Report

onedrive.bat.exe

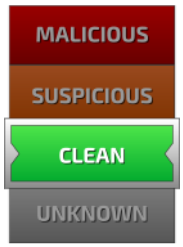
Overview

General Information

Sample Name:	onedrive.bat.exe
Analysis ID:	829696
MD5:	c32ca4acfcc63…
SHA1:	f5ee89bb1e4a0..
SHA256:	73a3c4aef5de3..
Infos:	



Detection

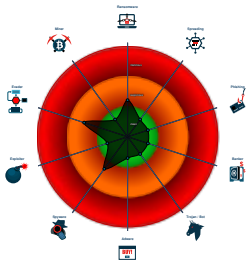


Score:	0
Range:	0 - 100
Whitelisted:	true
Confidence:	100%

Signatures

- Uses 32bit PE files
- Found a high number of Window / U…
- Queries the volume information (nam…
- Sample file is different than original …
- Tries to load missing DLLs
- Uses code obfuscation techniques (…
- Queries the installation date of Wind…
- Detected potential crypto function
- Sample execution stops while proce…
- Enables debug privileges

Classification



Process Tree

- **System is w10x64native**
- onedrive.bat.exe (PID: 4720 cmdline: C:\Users\user\Desktop\onedrive.bat.exe MD5: C32CA4ACFCC635EC1EA6ED8A34DF5FAC)
  - conhost.exe (PID: 6244 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

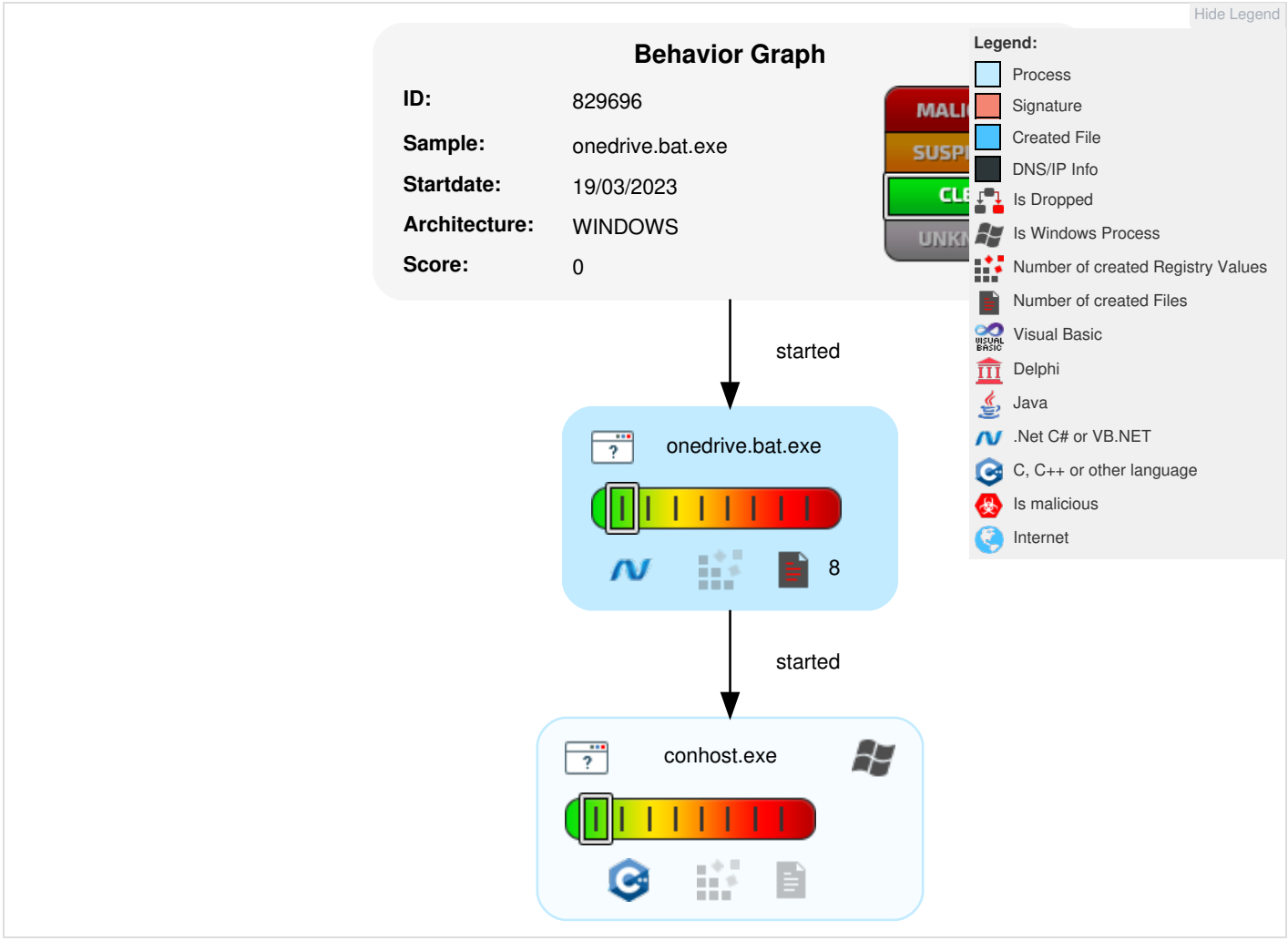
Joe Sandbox Signatures

There are no malicious signatures, click here to show all signatures.

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	1 DLL Side-Loading	2 Process Injection	1 Disable or Modify Tools	OS Credential Dumping	1 Process Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 DLL Side-Loading	2 Process Injection	LSASS Memory	1 Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 DLL Side-Loading	Security Account Manager	2 2 System Information Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Obfuscated Files or Information	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud

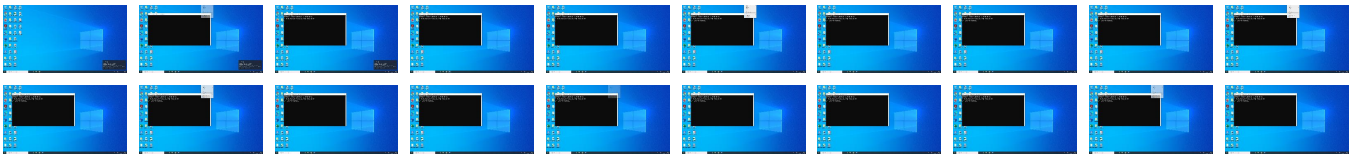
Behavior Graph

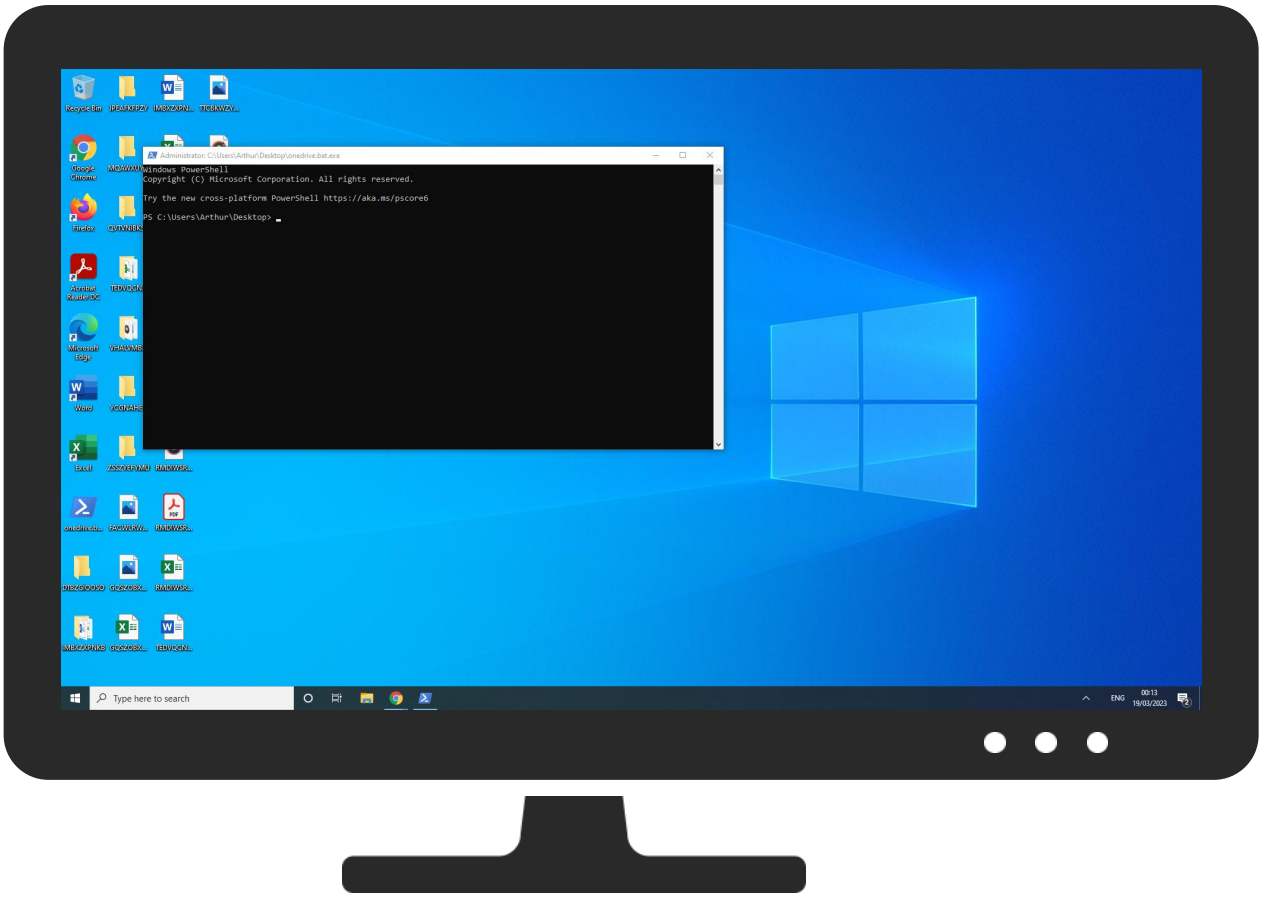


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
onedrive.bat.exe	0%	Virustotal		Browse
onedrive.bat.exe	0%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://aka.ms/pscore6LR	onedrive.bat.exe, 00000002.00000002.1051 94211165.00000000048D3000.00000004.00000 800.00020000.00000000.sdmp	false		high
http://https://aka.ms/pscore6lB	onedrive.bat.exe, 00000002.00000002.1051 94211165.00000000048F1000.00000004.00000 800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	onedrive.bat.exe, 00000002.00000002.1051 94211165.00000000048D3000.00000004.00000 800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	829696
Start date and time:	2023-03-19 00:09:28 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 26s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit 20H2 Native **physical Machine for testing VM-aware malware** (Office 2019, IE 11, Chrome 93, Firefox 91, Adobe Reader DC 21, Java 8 Update 301
Number of analysed new started processes analysed:	6
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample file name:	onedrive.bat.exe
Detection:	CLEAN
Classification:	clean5.winEXE@2/2@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, backgroundTaskHost.exe
- Excluded domains from analysis (whitelisted): wdcpalt.microsoft.com, client.wns.windows.com, login.live.com, ctldl.windowsupdate.com, wdcp.microsoft.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtReadVirtualMemory calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_tw0strn3.bud.ps1

Process:	C:\Users\user\Desktop\onedrive.bat.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.038920595031593
Encrypted:	false
SSDEEP:	3:Si2NPqzAYMLAKVpKGOyzKtFS:SnqbKAKWGX
MD5:	D17FE0A3F47BE24A6453E9EF58C94641
SHA1:	6AB83620379FC69F80C0242105DDFFD7D98D5D9D
SHA-256:	96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7
SHA-512:	5B592E58F26C264604F98F6AA12860758CE606D1C63220736CF0C779E4E18E3CEC8706930A16C38B20161754D1017D1657D35258E58CA22B18F5B232880DEC82
Malicious:	false
Reputation:	high, very likely benign file
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_u2wwjpve.24z.psm1

Process:	C:\Users\user\Desktop\onedrive.bat.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.038920595031593
Encrypted:	false
SSDEEP:	3:Si2NPqzAYMLAKVpKGOyzKtFS:SnqbKAKWGX
MD5:	D17FE0A3F47BE24A6453E9EF58C94641

SHA1:	6AB83620379FC69F80C0242105DDFFD7D98D5D9D
SHA-256:	96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7
SHA-512:	5B592E58F26C264604F98F6AA12860758CE606D1C63220736CF0C779E4E18E3CEC8706930A16C38B20161754D1017D1657D35258E58CA22B18F5B232880DEC82
Malicious:	false
Reputation:	high, very likely benign file
Preview:	# PowerShell test file to determine AppLocker lockdown mode

Static File Info

General

File type:	PE32 executable (console) Intel 80386, for MS Windows
Entropy (8bit):	5.502549953174867
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	onedrive.bat.exe
File size:	433152
MD5:	c32ca4acfcc635ec1ea6ed8a34df5fac
SHA1:	f5ee89bb1e4a0b1c3c7f1e8d05d0677f2b2b5919
SHA256:	73a3c4aef5de385875339fc2eb7e58a9e8a47b6161bdc6436bf78a763537be70
SHA512:	6e43dca1b92faace0c910cbf9308cf082a38dd39da32375fad72d6517dea93e944b5e5464cf3c69a61eabf47b2a3e5aa014d6f24efa1a379d4c81c32fa39ddbc
SSDEEP:	6144:MF45pGVc4sqEoWwO9sV1yZywi/PzNKXzJ7BapCK5d3klRzULOnWyjLsPhAQzqO:95pGVcwW2KXzJ4pdd3klnnWosPhnzq
TLSH:	B5947C8367D45295EC3FC431DC3745610622BCBDDBD09BDB99C8B6390A702D09A3EA6B
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.......".z.fg..fg..fg..x5..dg..o...lg..r...eg..r...}g..fg...g..r...cg..r...og..r...ng..r...gg..r...gg..Richfg.....

File Icon

Icon Hash:	14ec98b2b8e4d600

Static PE Info

General

Entrypoint:	0x40afc0
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows cui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, GUARD_CF, TERMINAL_SERVER_AWARE
Time Stamp:	0x30F12F73 [Mon Jan 8 14:51:31 1996 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	10
OS Version Minor:	0
File Version Major:	10
File Version Minor:	0
Subsystem Version Major:	10
Subsystem Version Minor:	0
Import Hash:	194427a488ed1dd0a91731658b071667

Entrypoint Preview

Instruction
call 00007F70DC413925h
jmp 00007F70DC412FAEh
jmp dword ptr [004121F4h]

Instruction
cmp ecx, dword ptr [00411368h]
jne 00007F70DC4131D5h
retn 0000h
jmp 00007F70DC41339Bh
int3
int3
mov edi, edi
push ebp
mov ebp, esp
push esi
mov esi, 004113A4h
push esi
call dword ptr [004120E8h]
mov ecx, dword ptr [00411360h]
mov eax, dword ptr [ebp+08h]
inc ecx
mov dword ptr [00411360h], ecx
push esi
mov dword ptr [eax], ecx
mov eax, dword ptr fs:[0000002Ch]
mov ecx, dword ptr [004116DCh]
mov ecx, dword ptr [eax+ecx*4]
mov eax, dword ptr [00411360h]
mov dword ptr [ecx+00000004h], eax
call dword ptr [00412078h]
push 004113A8h
call dword ptr [00412070h]
pop esi
pop ebp
ret
mov edi, edi
push ebp
mov ebp, esp
push esi
push edi
mov edi, 004113A4h
push edi
call dword ptr [004120E8h]
mov esi, dword ptr [ebp+08h]
cmp dword ptr [esi], 00000000h
jne 00007F70DC4131E1h
or dword ptr [esi], FFFFFFFFh
jmp 00007F70DC4131FBh
push 00000000h
call 00007F70DC413202h
pop ecx
jmp 00007F70DC4131BEh
cmp dword ptr [esi], FFFFFFFFh
je 00007F70DC4131C3h
mov eax, dword ptr fs:[0000002Ch]
mov ecx, dword ptr [004116DCh]
mov ecx, dword ptr [eax+ecx*4]
mov eax, dword ptr [00411360h]
mov dword ptr [ecx+00000004h], eax
push edi
call dword ptr [00412078h]
pop edi
pop esi

Rich Headers

Programming Language:	• [IMP] VS2008 build 21022 • [IMP] VS2008 SP1 build 30729

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x12208	0xb4	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x13000	0x57d88	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x6b000	0x127c	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x4900	0x54	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x1694	0x18	.text
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x15e8	0xac	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x12000	0x204	.idata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xf35c	0xf400	False	0.457367443647541	data	5.675599809360563	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0x11000	0x938	0x400	False	0.439453125	data	4.3874403980662935	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.idata	0x12000	0xcd8	0xe00	False	0.44614955357142855	data	5.292395568542356	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x13000	0x57d88	0x57e00	False	0.3494065611664296	data	5.3056762942545195	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x6b000	0x127c	0x1400	False	0.7013671875	data	6.257290188908493	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
MUI	0x6acb0	0xd8	data	English	United States
RT_ICON	0x13c48	0x2fbe	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_ICON	0x16c08	0x4228	Device independent bitmap graphic, 64 x 128 x 32, image size 16896	English	United States
RT_ICON	0x1ae30	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9600	English	United States
RT_ICON	0x1d3d8	0x1a68	Device independent bitmap graphic, 40 x 80 x 32, image size 6720	English	United States
RT_ICON	0x1ee40	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4224	English	United States
RT_ICON	0x1fee8	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 2400	English	United States
RT_ICON	0x20870	0x6b8	Device independent bitmap graphic, 20 x 40 x 32, image size 1680	English	United States
RT_ICON	0x20f28	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1088	English	United States
RT_ICON	0x21408	0x668	Device independent bitmap graphic, 48 x 96 x 4, image size 1152	English	United States
RT_ICON	0x21a70	0x2e8	Device independent bitmap graphic, 32 x 64 x 4, image size 512	English	United States

Name	RVA	Size	Type	Language	Country
RT_ICON	0x21d58	0x1e8	Device independent bitmap graphic, 24 x 48 x 4, image size 288	English	United States
RT_ICON	0x21f40	0x128	Device independent bitmap graphic, 16 x 32 x 4, image size 128	English	United States
RT_ICON	0x22068	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 2304, 256 important colors	English	United States
RT_ICON	0x22f10	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 1024, 256 important colors	English	United States
RT_ICON	0x237b8	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 576, 256 important colors	English	United States
RT_ICON	0x23e80	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 256, 256 important colors	English	United States
RT_ICON	0x243e8	0x42028	Device independent bitmap graphic, 256 x 512 x 32, image size 270336	English	United States
RT_ICON	0x66410	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9600	English	United States
RT_ICON	0x689b8	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4224	English	United States
RT_ICON	0x69a60	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 2400	English	United States
RT_ICON	0x6a3e8	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1088	English	United States
RT_GROUP_ICON	0x21390	0x76	data	English	United States
RT_GROUP_ICON	0x6a850	0xbc	data	English	United States
RT_VERSION	0x6a910	0x39c	OpenPGP Secret Key	English	United States
RT_MANIFEST	0x135a0	0x6a3	XML 1.0 document, ASCII text, with CRLF line terminators	English	United States

Imports

DLL	Import
msvcrt.dll	_onexit, __dllonexit, _unlock, _lock, _initterm, __setusermatherr, __p__fmode, _cexit, _exit, exit, __set_app_type, __wgetmainargs, ?terminate@@YAXXZ, __p__commode, ??1type_info@@UAE@XZ, _controlfp, _XcptFilter, _except_handler4_common, memcmp, _vsnwprintf, _wcsicmp, _wcsnicmp, bsearch, fclose, _wfopen, _itow_s, wcstoul, wcschr, __uncaught_exception, memmove, memcpy, _CxxThrowException, ?what@exception@@UBEPBDXZ, ??1exception@@UAE@XZ, ??0exception@@QAE@ABV0@@Z, ??0exception@@QAE@ABQBDH@Z, ??0exception@@QAE@ABQBD@Z, _callnewh, malloc, wcsncmp, wcsrchr, free, _purecall, ??3@YAXPAX@Z, memcpy_s, ??_V@YAXPAX@Z, __CxxFrameHandler3, _amsg_exit, memset
ATL.DLL	
KERNEL32.dll	CreateFileMappingW, FreeLibrary, LoadResource, FindResourceExW, UnmapViewOfFile, GetVersionExW, GetLocaleInfoW, GetUserDefaultUILanguage, GetSystemDefaultUILanguage, SearchPathW, MapViewOfFile, GetTickCount, GetSystemTimeAsFileTime, LoadLibraryExW, GetCurrentProcessId, QueryPerformanceCounter, TerminateProcess, SetUnhandledExceptionFilter, UnhandledExceptionFilter, SleepConditionVariableSRW, WakeAllConditionVariable, GetModuleFileNameW, ReleaseSRWLockExclusive, Sleep, IsWow64Process, SetConsoleTitleW, GetFileType, VerifyVersionInfoW, GetProcAddress, GetModuleHandleW, GetCurrentThreadId, GetModuleHandleExW, GetStartupInfoW, VerSetConditionMask, FindFirstFileW, SetErrorMode, LocalFree, CompareStringW, WriteConsoleW, SetLastError, GetLastError, GetCurrentProcess, GetStdHandle, WriteFile, FormatMessageW, ExpandEnvironmentStringsW, GetFileAttributesW, CreateFileW, FindClose, SetThreadUILanguage, AcquireSRWLockExclusive, CloseHandle
OLEAUT32.dll	SysAllocString, SafeArrayPutElement, VariantClear, SafeArrayCreate, SysFreeString, SysStringLen
ADVAPI32.dll	RegOpenKeyExW, RegEnumKeyExW, RegQueryValueExW, RegCloseKey, RegGetValueW
OLE32.dll	CoUninitialize, CoInitializeEx, CoInitialize, PropVariantClear, CoTaskMemAlloc, CoCreateInstance
USER32.dll	LoadStringW
mscoree.dll	CorBindToRuntimeEx

Possible Origin

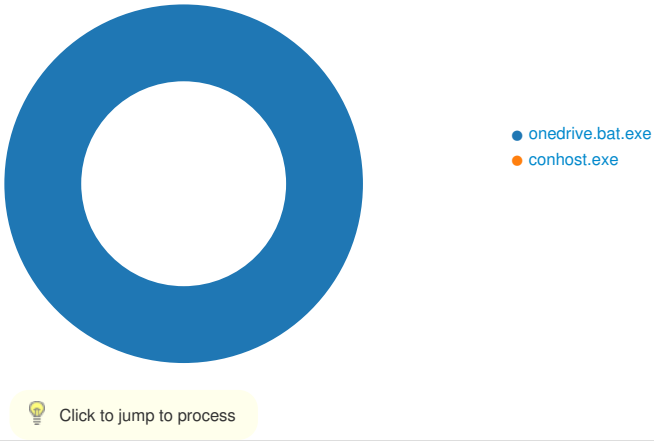
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Report size exceeds maximum size, go to the download page of this report and download PCAP to see all network behavior.

Statistics

Behavior



System Behavior

Analysis Process: onedrive.bat.exe PID: **4720**, Parent PID: **4708**

General

Target ID:	2
Start time:	00:11:22
Start date:	19/03/2023
Path:	C:\Users\user\Desktop\onedrive.bat.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\onedrive.bat.exe
Imagebase:	0x500000
File size:	433152 bytes
MD5 hash:	C32CA4ACFCC635EC1EA6ED8A34DF5FAC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities

Analysis Process: conhost.exe PID: **6244**, Parent PID: **4720**

General

Target ID:	3
Start time:	00:11:22
Start date:	19/03/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff744690000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly