ID: 668013
Sample Name: powershell.exe
Cookbook: default.jbs
Time: 08:42:44
Date: 18/07/2022
Version: 35.0.0 Citrine

Table of Contents

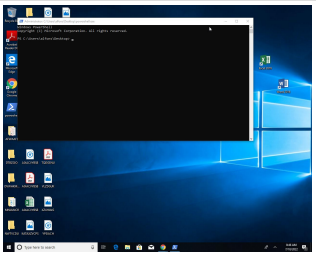
Windows Analysis Report

powershell.exe

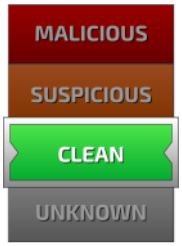
Overview

General Information

Sample Name:	powershell.exe
Analysis ID:	668013
MD5:	c32ca4acfcc635…
SHA1:	f5ee89bb1e4a0b..
SHA256:	73a3c4aef5de38..
Infos:	



Detection

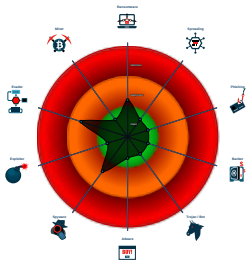


Score:	6
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

- Uses 32bit PE files
- Found a high number of Window / U…
- Queries the volume information (nam…
- Sample file is different than original …
- PE file contains strange resources
- Contains functionality to query local…
- May sleep (evasive loops) to hinder…
- Uses code obfuscation techniques (…
- Queries the installation date of Wind…
- Detected potential crypto function
- Contains long sleeps (>= 3 min)
- Enables debug privileges

Classification



Process Tree

- **System is w10x64**
- powershell.exe (PID: 6928 cmdline: "C:\Users\user\Desktop\powershell.exe" MD5: C32CA4ACFCC635EC1EA6ED8A34DF5FAC)
  - conhost.exe (PID: 6936 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **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

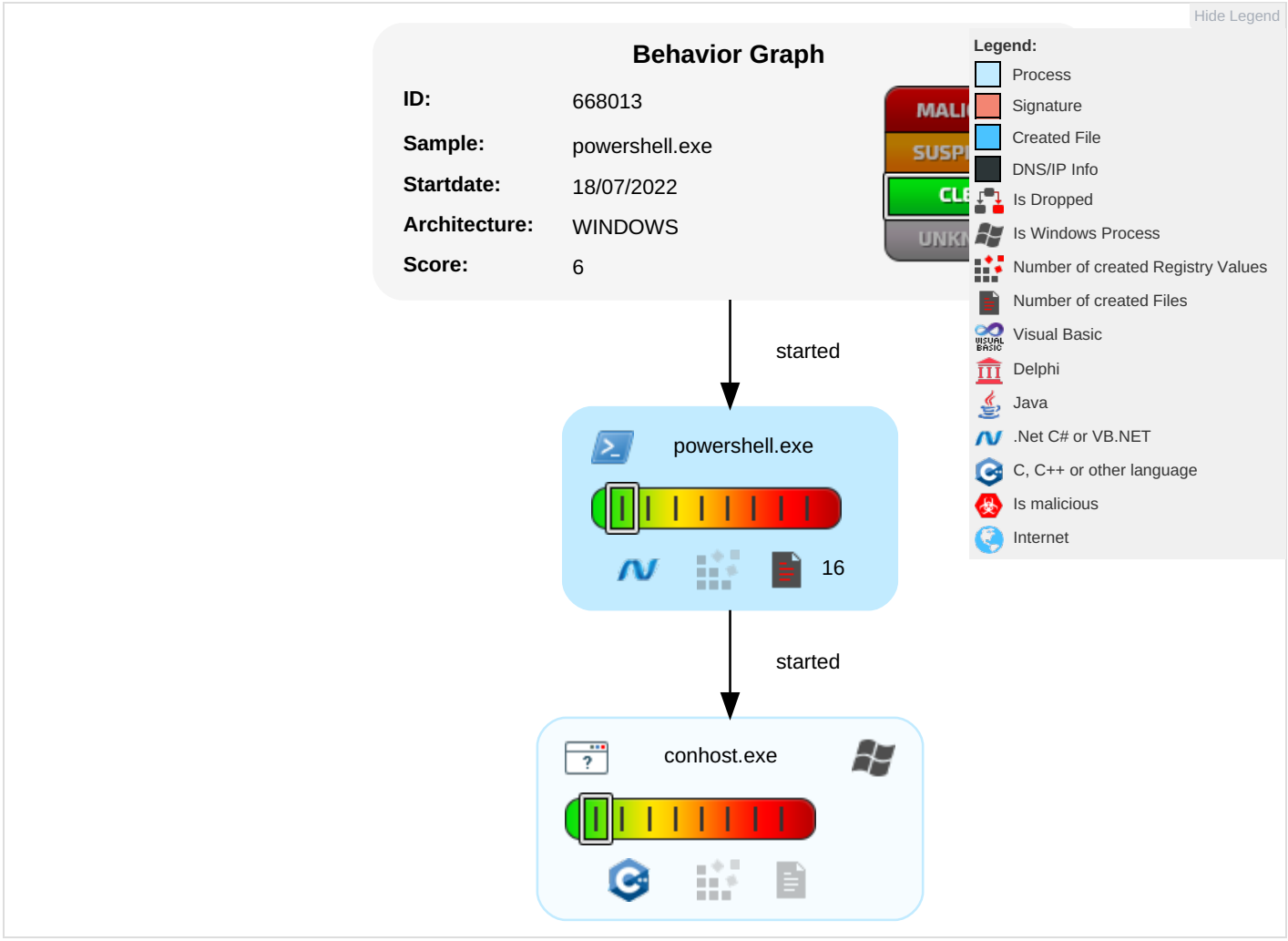
Joe Sandbox Signatures

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	Path Interception	1 Process Injection	1 Masquerading	OS Credential Dumping	1 System Time 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	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	LSASS Memory	1 Process 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)	2 1 Virtualization/Sandbox Evasion	Security Account Manager	2 1 Virtualization/Sandbox Evasion	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 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Obfuscated Files or Information	LSA Secrets	1 File and Directory Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	3 4 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

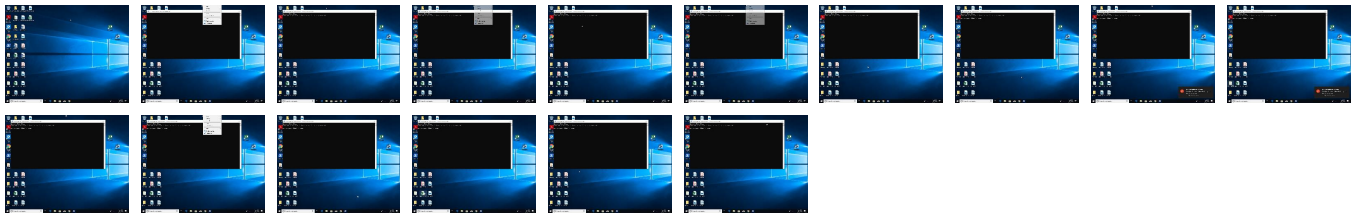
Behavior Graph

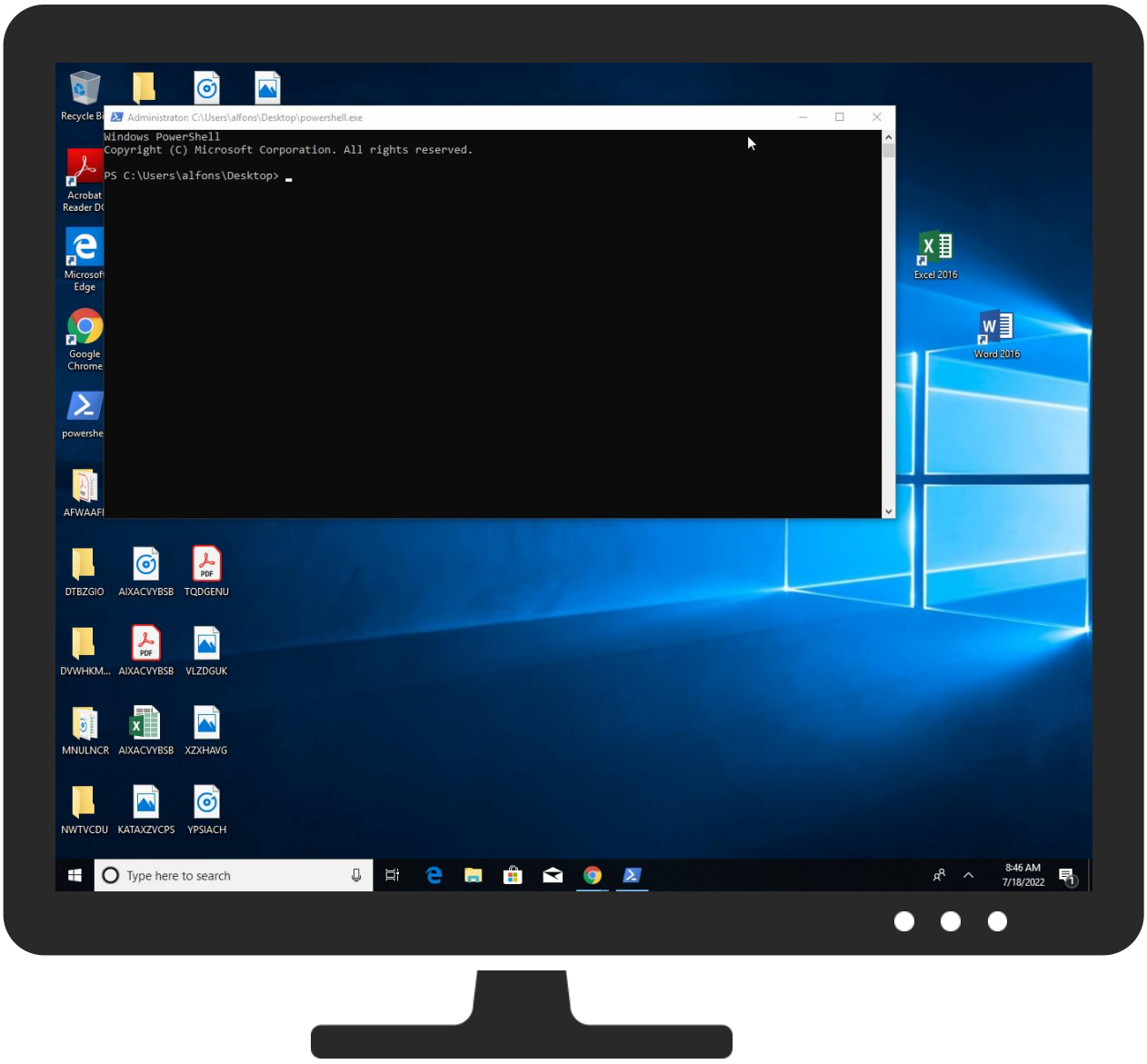


Screenshots

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
powershell.exe	0%	Virustotal		Browse
powershell.exe	0%	Metadefender		Browse
powershell.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://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000000.00000002.712431385.0000000005611000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	668013
Start date and time: 18/07/202208:42:44	2022-07-18 08:42:44 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 49s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	powershell.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	17
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
Detection:	CLEAN
Classification:	clean6.winEXE@2/2@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 6.8% (good quality ratio 5.9%) • Quality average: 62.8% • Quality standard deviation: 35.3%
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 • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115, 40.125.122.176, 20.54.89.106, 20.223.24.244, 52.152.110.14, 52.242.101.226
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, arc.msn.com, e12564.dspb.akamaiedge.net, licensing.mp.microsoft.com, consumer-displaycatalogrp-aks2aks-europe.md.mp.microsoft.com.akadns.net, login.live.com, store-images.s-microsoft.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net, glb.sls.prod.dcat.dsp.trafficmanager.net
- 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.

Simulations

Behavior and APIs

Time	Type	Description
08:44:27	API Interceptor	38x Sleep call for process: powershell.exe modified

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_sqblenui.nu5.psm1

Process:	C:\Users\user\Desktop\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_vyke4on2.1v5.ps1

Process:	C:\Users\user\Desktop\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

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:	powershell.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 00007FE154B40CC5h
jmp 00007FE154B4034Eh
jmp dword ptr [004121F4h]
cmp ecx, dword ptr [00411368h]
jne 00007FE154B40575h
retn 0000h
jmp 00007FE154B4073Bh
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 00007FE154B40581h
or dword ptr [esi], FFFFFFFFh
jmp 00007FE154B4059Bh
push 00000000h
call 00007FE154B405A2h
pop ecx
jmp 00007FE154B4055Eh
cmp dword ptr [esi], FFFFFFFFh
je 00007FE154B40563h
mov eax, dword ptr fs:[0000002Ch]
mov ecx, dword ptr [004116DCh]

Instruction
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	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 4294967295, next used block 4294967295	English	United States
RT_ICON	0x1ae30	0x25a8	data	English	United States
RT_ICON	0x1d3d8	0x1a68	data	English	United States
RT_ICON	0x1ee40	0x10a8	data	English	United States
RT_ICON	0x1fee8	0x988	data	English	United States

Name	RVA	Size	Type	Language	Country
RT_ICON	0x20870	0x6b8	data	English	United States
RT_ICON	0x20f28	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0x21408	0x668	data	English	United States
RT_ICON	0x21a70	0x2e8	dBase IV DBT of @.DBF, block length 512, next free block index 40, next free block 2296940798, next used block 15239304	English	United States
RT_ICON	0x21d58	0x1e8	data	English	United States
RT_ICON	0x21f40	0x128	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0x22068	0xea8	data	English	United States
RT_ICON	0x22f10	0x8a8	dBase IV DBT of @.DBF, block length 1024, next free block index 40, next free block 14019316, next used block 14479096	English	United States
RT_ICON	0x237b8	0x6c8	data	English	United States
RT_ICON	0x23e80	0x568	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0x243e8	0x42028	dBase IV DBT, blocks size 0, block length 8192, next free block index 40, next free block 0, next used block 0	English	United States
RT_ICON	0x66410	0x25a8	data	English	United States
RT_ICON	0x689b8	0x10a8	data	English	United States
RT_ICON	0x69a60	0x988	data	English	United States
RT_ICON	0x6a3e8	0x468	GLS_BINARY_LSB_FIRST	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	data	English	United States
RT_MANIFEST	0x135a0	0x6a3	XML 1.0 document text	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

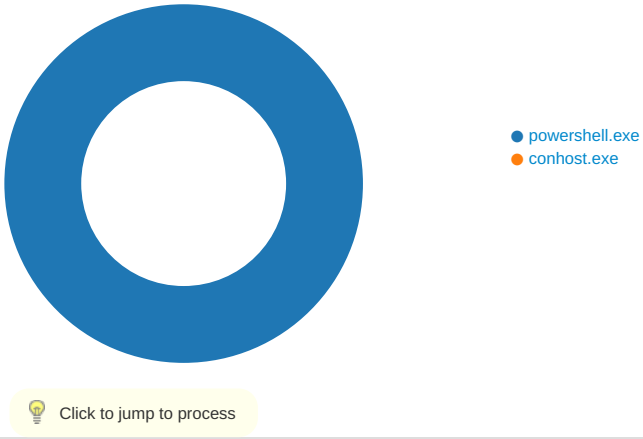
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

No network behavior found

Statistics

Behavior



System Behavior

Analysis Process: powershell.exe PID: 6928, Parent PID: 3464

General

Target ID:	0
Start time:	08:43:59
Start date:	18/07/2022
Path:	C:\Users\user\Desktop\powershell.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\powershell.exe"
Imagebase:	0xac0000
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

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E53CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E53CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6C755B28	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6C755B28	unknown
C:\Users\user\Documents\20220718	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C7FBEFF	CreateDirectoryW
C:\Users\user\Documents\20220718\PowerShell_transcript.065367.ZHZmPZos.20220718084404.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C7F1E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_vyke4on2.1v5.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C7F1E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_sqblenui.nu5.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C7F1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_vyke4on2.1v5.ps1	success or wait	1	6C7F6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_sqblenui.nu5.psm1	success or wait	1	6C7F6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	16	19	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C755B28	unknown
unknown	35	21	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C755B28	unknown
unknown	56	16	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C755B28	unknown
unknown	72	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C755B28	unknown
unknown	80	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C755B28	unknown
unknown	89	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C755B28	unknown
unknown	97	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C755B28	unknown
unknown	0	3	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C7F1B4F	WriteFile
unknown	3	582	75 6e 6b 6e 6f 77 6e	unknown	success or wait	9	6C7F1B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_vyke4on2.1v5.ps1	0	1	31	1	success or wait	1	6C7F1B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_sqblenui.nu5.psm1	0	1	31	1	success or wait	1	6C7F1B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E515705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E515705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E4703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E51CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E4703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E4703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E4703DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6E4703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E515705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E515705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E4703DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6C7F1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	1	6C7F1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6C7F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C7F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C7F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6C7F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6C7F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6C7F1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6C7F1B4F	ReadFile

Analysis Process: conhost.exe PID: **6936**, Parent PID: **6928**

General

Target ID:	1
Start time:	08:43:59
Start date:	18/07/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

No disassembly