ID: 708240
Sample Name: 6Sy6PrInNl.exe
Cookbook: default.jbs
Time: 07:56:16
Date: 23/09/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

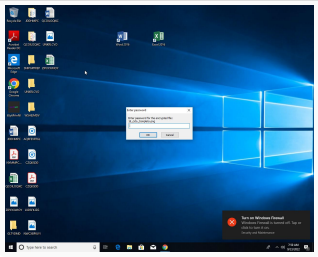
Windows Analysis Report

6Sy6PrInNl.exe

Overview

General Information

Sample Name:	6Sy6PrInNl.exe
Analysis ID:	708240
MD5:	cd1ffe7c3031165..
SHA1:	310fcf3a4328678..
SHA256:	842342b4db7bbc..
Tags:	exe morpheus pwtorun
Infos:	



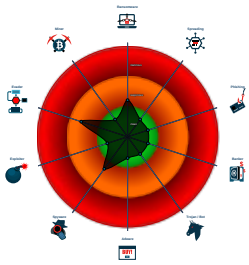
Detection

Score:	36
Range:	0 - 100
Whitelisted:	false
Confidence:	40%

Signatures

- Multi AV Scanner detection for subm…
- Uses 32bit PE files
- Tries to load missing DLLs
- Contains functionality to check if a d…
- Contains functionality to query local…
- Contains functionality to read the PE…
- Uses code obfuscation techniques (…
- File is packed with WinRar
- Found evasive API chain (date chec…
- PE file contains sections with non-s…
- Detected potential crypto function
- Contains functionality to query CPU…

Classification



Analysis Advice

Sample tries to load a library which is not present or installed on the analysis machine, adding the library might reveal more behavior
Sample may offer command line options, please run it with the 'Execute binary with arguments' cookbook (it's possible that the command line switches require additional characters like: "-", "/", "--")
Sample reads itself and does not show any behavior, likely it performs some host environment checks which are compared to an embedded key

Process Tree

- **System is w10x64**
- 6Sy6PrInNl.exe (PID: 2800 cmdline: "C:\Users\user\Desktop\6Sy6PrInNl.exe" MD5: CD1FFE7C30311659EA1BE07ED7923D65)
- **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

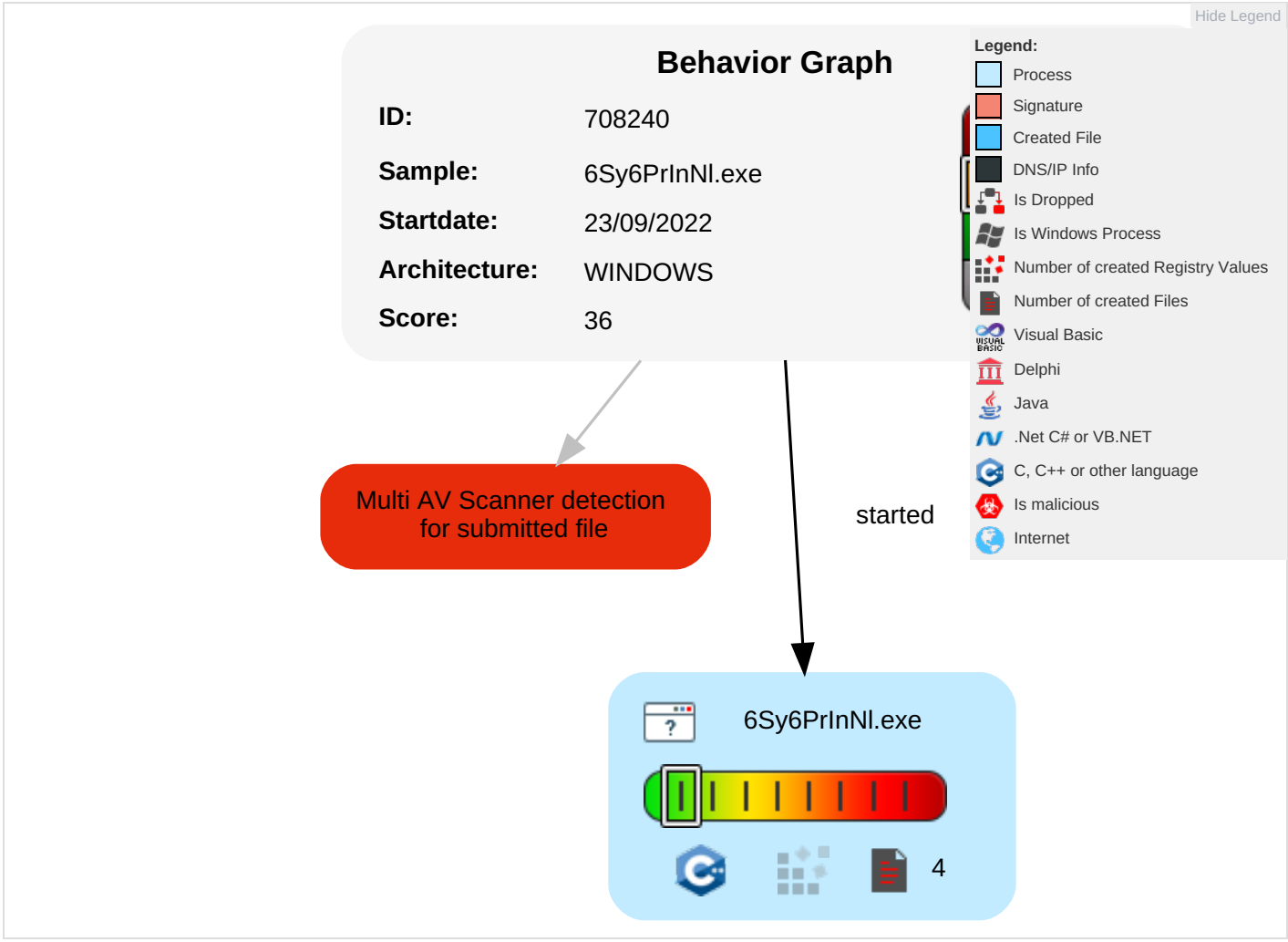
AV Detection

Multi AV Scanner detection for submitted file

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	2 Command and Scripting Interpreter	1 DLL Side-Loading	1 DLL Side-Loading	1 Masqueradi ng	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 Communic ation	Remotely Track Device Without Authorizati on	Modify System Partition
Default Accounts	1 Native API	Boot or Logon Initializatio n Scripts	Boot or Logon Initializatio n Scripts	1 Deobfuscat e/Decode Files or Information	LSASS Memory	2 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorizati on	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 Obfuscated Files or Information	Security Account Manager	2 File and Directory Discovery	SMB/Wind ows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganogra phy	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Software Packing	NTDS	2 5 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonati on	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 DLL Side-Loading	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communic ation		Manipulate App Store Rankings or Ratings

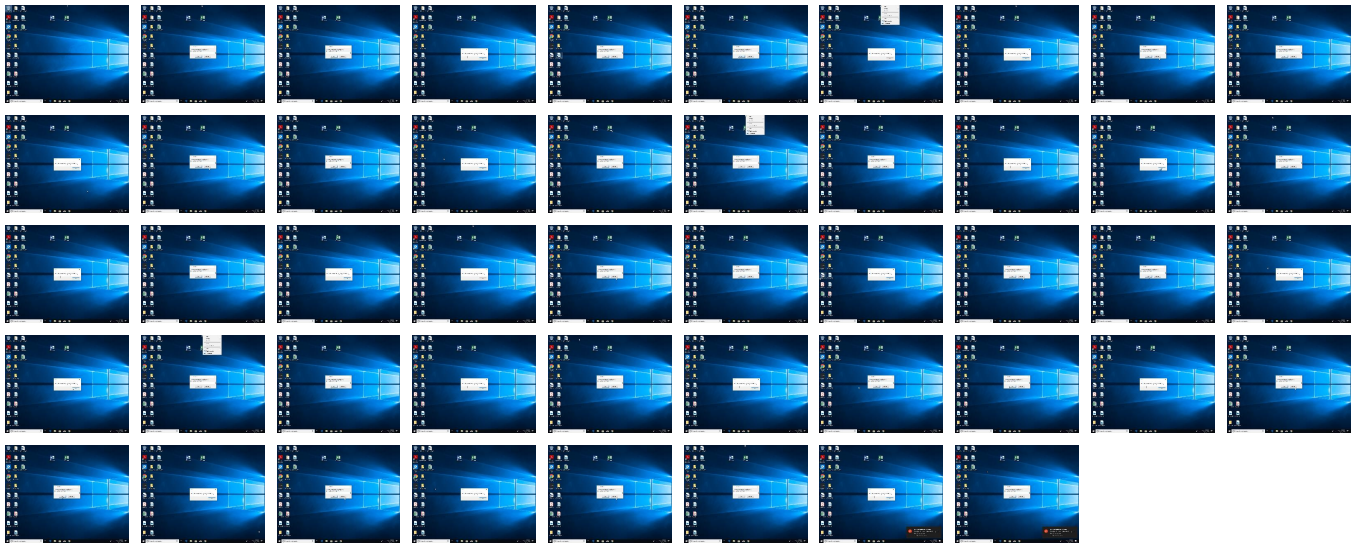
Behavior Graph



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
6Sy6PrInNI.exe	28%	ReversingLabs	Win32.Trojan.Generic	
6Sy6PrInNI.exe	30%	Virustotal		Browse
6Sy6PrInNI.exe	11%	Metadefender		Browse

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

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	708240
Start date and time:	2022-09-23 07:56:16 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	6Sy6PrInNl.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	12
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:	SUS
Classification:	sus36.winEXE@1/0@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 99.7% (good quality ratio 92%) • Quality average: 78.4% • Quality standard deviation: 29.8%
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): MpCmdRun.exe, RuntimeBroker.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): login.live.com, displaycatalog.mp.microsoft.com, arc.msn.com
- Not all processes where analyzed, report is missing behavior information

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

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.143158241689354
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:	6Sy6PrInNl.exe
File size:	788504
MD5:	cd1ffe7c30311659ea1be07ed7923d65
SHA1:	310fcf3a43286785eb88d742f5deeae150c661e9
SHA256:	842342b4db7bbc84d8e4da35f8d79d8b76a52815b7a22272f331ba906d2dba6c
SHA512:	588e21a2cefabfa2d20364e7b62d9d3448cc3c7295b34fffb481b64837ef49cb36510c36a75a300338d0d2f4b8ac42120ef26e4dab30ec2b946ceaf60f560170
SSDEEP:	12288:zToPWBv/cpGrU3yKszraraEoMgF/FEJJSJx:zTbBv5rUazram5MIx
TLSH:	8BF4E10EBAC198B2D073D9321A356725A53CB9201F668ADFE3DC465FDB215C0E7317A2
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....x_c.<>..<>..<>.....1>.....>.....$>...I..>>...I../>...I..+>...I...>..5F..7>..5F..;>..<>..)?...I...>...I..=>...I..=>...I..=>.

File Icon

Icon Hash:	008039c4c4384000

Static PE Info

General

Entrypoint:	0x41f530
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, GUARD_CF, TERMINAL_SERVER_AWARE
Time Stamp:	0x6220BF8D [Thu Mar 3 13:15:57 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	12e12319f1029ec4f8fcbed7e82df162

Entrypoint Preview
Instruction
call 00007F2D8070A4FBh
jmp 00007F2D80709E0Dh
int3
int3
int3
int3
int3
int3
push ebp
mov ebp, esp
push esi
push dword ptr [ebp+08h]
mov esi, ecx
call 00007F2D806FCC57h
mov dword ptr [esi], 004356D0h
mov eax, esi
pop esi
pop ebp
retn 0004h
and dword ptr [ecx+04h], 00000000h
mov eax, ecx
and dword ptr [ecx+08h], 00000000h
mov dword ptr [ecx+04h], 004356D8h
mov dword ptr [ecx], 004356D0h
ret
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
push ebp
mov ebp, esp

Instruction
push esi
mov esi, ecx
lea eax, dword ptr [esi+04h]
mov dword ptr [esi], 004356B8h
push eax
call 00007F2D8070D29Fh
test byte ptr [ebp+08h], 00000001h
pop ecx
je 00007F2D80709F9Ch
push 0000000Ch
push esi
call 00007F2D80709559h
pop ecx
pop ecx
mov eax, esi
pop esi
pop ebp
retn 0004h
push ebp
mov ebp, esp
sub esp, 0Ch
lea ecx, dword ptr [ebp-0Ch]
call 00007F2D806FCBD2h
push 0043BEF0h
lea eax, dword ptr [ebp-0Ch]
push eax
call 00007F2D8070CD59h
int3
push ebp
mov ebp, esp
sub esp, 0Ch
lea ecx, dword ptr [ebp-0Ch]
call 00007F2D80709F18h
push 0043C0F4h
lea eax, dword ptr [ebp-0Ch]
push eax
call 00007F2D8070CD3Ch
int3
jmp 00007F2D8070E7D7h
int3
int3
int3
int3
push 00422900h
push dword ptr fs:[00000000h]

Rich Headers

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x3d070	0x34	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x3d0a4	0x50	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x64000	0x4698c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xab000	0x233c	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x3b11c	0x54	.rdata

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x355f8	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x33000	0x278	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x3c5ec	0x120	.rdata
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	0x31bdc	0x31c00	False	0.5909380888819096	data	6.712962136932442	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x33000	0xaec0	0xb000	False	0.4579190340909091	data	5.261605615899847	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x3e000	0x24720	0x1000	False	0.451416015625	data	4.387459135575936	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.didat	0x63000	0x190	0x200	False	0.4453125	data	3.3327310103022305	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x64000	0x4698c	0x46a00	False	0.07180586283185841	data	2.00213285276512	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xab000	0x233c	0x2400	False	0.7749565972222222	data	6.623012966548067	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
PNG	0x64524	0xb45	PNG image data, 93 x 302, 8-bit/color RGB, non-interlaced	English	United States
PNG	0x6506c	0x15a9	PNG image data, 186 x 604, 8-bit/color RGB, non-interlaced	English	United States
RT_ICON	0x66618	0x42028	data		
RT_DIALOG	0xa8640	0x286	data	English	United States
RT_DIALOG	0xa88c8	0x13a	data	English	United States
RT_DIALOG	0xa8a04	0xec	data	English	United States
RT_DIALOG	0xa8af0	0x12e	data	English	United States
RT_DIALOG	0xa8c20	0x338	data	English	United States
RT_DIALOG	0xa8f58	0x252	data	English	United States
RT_STRING	0xa91ac	0x1e2	data	English	United States
RT_STRING	0xa9390	0x1cc	data	English	United States
RT_STRING	0xa955c	0x1b8	data	English	United States
RT_STRING	0xa9714	0x146	Hitachi SH big-endian COFF object file, not stripped, 17152 sections, symbol offset=0x73006500	English	United States
RT_STRING	0xa985c	0x46c	data	English	United States
RT_STRING	0xa9cc8	0x166	data	English	United States
RT_STRING	0xa9e30	0x152	data	English	United States
RT_STRING	0xa9f84	0x10a	data	English	United States
RT_STRING	0xaa090	0xbc	data	English	United States
RT_STRING	0xaa14c	0xd6	data	English	United States
RT_GROUP_ICON	0xaa224	0x14	data		
RT_MANIFEST	0xaa238	0x753	XML 1.0 document, ASCII text, with CRLF line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	GetLastError, SetLastError, FormatMessageW, GetCurrentProcess, DeviceIoControl, SetFileTime, CloseHandle, CreateDirectoryW, RemoveDirectoryW, CreateFileW, DeleteFileW, CreateHardLinkW, GetShortPathNameW, GetLongPathNameW, MoveFileW, GetFileType, GetStdHandle, WriteFile, ReadFile, FlushFileBuffers, SetEndOfFile, SetFilePointer, SetFileAttributesW, GetFileAttributesW, FindClose, FindFirstFileW, FindNextFileW, InterlockedDecrement, GetVersionExW, GetCurrentDirectoryW, GetFullPathNameW, FoldStringW, GetModuleFileNameW, GetModuleHandleW, FindResourceW, FreeLibrary, GetProcAddress, GetCurrentProcessId, ExitProcess, SetThreadExecutionState, Sleep, LoadLibraryW, GetSystemDirectoryW, CompareStringW, AllocConsole, FreeConsole, AttachConsole, WriteConsoleW, GetProcessAffinityMask, CreateThread, SetThreadPriority, InitializeCriticalSection, EnterCriticalSection, LeaveCriticalSection, DeleteCriticalSection, SetEvent, ResetEvent, ReleaseSemaphore, WaitForSingleObject, CreateEventW, CreateSemaphoreW, GetSystemTime, SystemTimeToTzSpecificLocalTime, TzSpecificLocalTimeToSystemTime, SystemTimeToFileTime, FileTimeToLocalFileTime, LocalFileTimeToFileTime, FileTimeToSystemTime, GetCPInfo, IsDBCSLeadByte, MultiByteToWideChar, WideCharToMultiByte, GlobalAlloc, LockResource, GlobalLock, GlobalUnlock, GlobalFree, LoadResource, SizeofResource, SetCurrentDirectoryW, GetExitCodeProcess, GetLocalTime, GetTickCount, MapViewOfFile, UnmapViewOfFile, CreateFileMappingW, OpenFileMappingW, GetCommandLineW, SetEnvironmentVariableW, ExpandEnvironmentStringsW, GetTempPathW, MoveFileExW, GetLocaleInfoW, GetTimeFormatW, GetDateFormatW, GetNumberFormatW, DecodePointer, SetFilePointerEx, GetConsoleMode, GetConsoleCP, HeapSize, SetStdHandle, GetProcessHeap, FreeEnvironmentStringsW, GetEnvironmentStringsW, GetCommandLineA, GetOEMCP, RaiseException, GetSystemInfo, VirtualProtect, VirtualQuery, LoadLibraryExA, IsProcessorFeaturePresent, IsDebuggerPresent, UnhandledExceptionFilter, SetUnhandledExceptionFilter, GetStartupInfoW, QueryPerformanceCounter, GetCurrentThreadId, GetSystemTimeAsFileTime, InitializeSListHead, TerminateProcess, LocalFree, RtlUnwind, EncodePointer, InitializeCriticalSectionAndSpinCount, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, LoadLibraryExW, QueryPerformanceFrequency, GetModuleHandleExW, GetModuleFileNameA, GetACP, HeapFree, HeapAlloc, HeapReAlloc, GetStringTypeW, LCMapStringW, FindFirstFileExA, FindNextFileA, IsValidCodePage
OLEAUT32.dll	SysAllocString, SysFreeString, VariantClear
gdiplus.dll	GdipAlloc, GdipDisposeImage, GdipCloneImage, GdipCreateBitmapFromStream, GdipCreateBitmapFromStreamICM, GdipCreateHBITMAPFromBitmap, GdiplusStartup, GdiplusShutdown, GdipFree

Possible Origin

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

Network Behavior

No network behavior found

Statistics

No statistics

System Behavior

Analysis Process: 6Sy6PrInNl.exe PID: **2800**, Parent PID: **1244**

General

Target ID:	0
Start time:	07:57:12
Start date:	23/09/2022
Path:	C:\Users\user\Desktop\6Sy6PrInNl.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\6Sy6PrInNl.exe"
Imagebase:	0x11d0000
File size:	788504 bytes
MD5 hash:	CD1FFE7C30311659EA1BE07ED7923D65
Has elevated privileges:	true

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

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	11DA2DF	CreateDirectoryW
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	11DA2DF	CreateDirectoryW
C:\Users\user\Desktop	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	11DA2DF	CreateDirectoryW
C:\Users\user\Desktop__tmp_rar_sfx_access_check_7003046	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	11D96EC	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop__tmp_rar_sfx_access_check_7003046	success or wait	1	11DA1F7	DeleteFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\6Sy6PrInNl.exe	unknown	8192	success or wait	98	11D97B3	ReadFile

Disassembly

No disassembly