ID: 408913
Sample Name: kS5hYPcgm8.dll
Cookbook: default.jbs
Time: 08:08:08
Date: 09/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

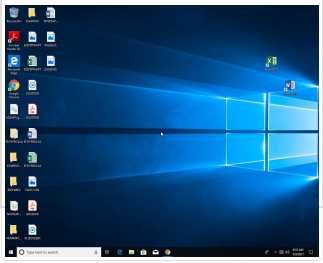
Analysis Report kS5hYPcgm8.dll

Overview

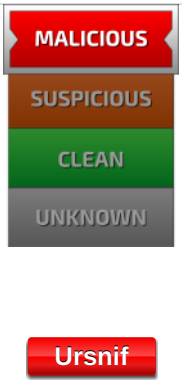
General Information

Sample Name:	kS5hYPcgm8.dll
Analysis ID:	408913
MD5:	68fc6441db6c553..
SHA1:	c67a6a85716e0f1..
SHA256:	802a752fca3ded0..
Tags:	dll Gozi
Infos:	

Most interesting Screenshot:



Detection



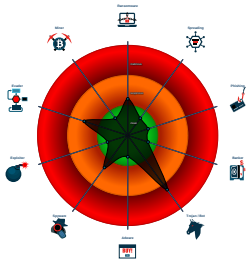
Ursnif

Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected Ursnif
- Contains functionality to call native f…
- Contains functionality to check if a d…
- Contains functionality to dynamically…
- Contains functionality to open a port…
- Contains functionality to query CPU …
- Contains functionality to query locale…
- Contains functionality to read the PEB
- Creates a process in suspended mo…
- Detected potential crypto function
- Found potential string decryption / a…

Classification



Startup

- **System is w10x64**
- loaddll32.exe (PID: 2212 cmdline: loaddll32.exe 'C:\Users\user\Desktop\kS5hYPcgm8.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 4356 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\kS5hYPcgm8.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 1556 cmdline: rundll32.exe 'C:\Users\user\Desktop\kS5hYPcgm8.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - cmd.exe (PID: 5700 cmdline: C:\Windows\system32\cmd.exe /c cd Island MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 6148 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - cmd.exe (PID: 6240 cmdline: C:\Windows\system32\cmd.exe /c cd Matter m MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 6260 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - rundll32.exe (PID: 1140 cmdline: rundll32.exe C:\Users\user\Desktop\kS5hYPcgm8.dll,Connectdark MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - cmd.exe (PID: 2576 cmdline: C:\Windows\system32\cmd.exe /c cd Island MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 4228 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - cmd.exe (PID: 6204 cmdline: C:\Windows\system32\cmd.exe /c cd Matter m MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 6248 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - rundll32.exe (PID: 6324 cmdline: rundll32.exe C:\Users\user\Desktop\kS5hYPcgm8.dll,Mindlake MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - cmd.exe (PID: 6336 cmdline: C:\Windows\system32\cmd.exe /c cd Island MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 6348 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - cmd.exe (PID: 6396 cmdline: C:\Windows\system32\cmd.exe /c cd Matter m MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 6404 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - rundll32.exe (PID: 6388 cmdline: rundll32.exe C:\Users\user\Desktop\kS5hYPcgm8.dll,Porthigh MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - cmd.exe (PID: 6416 cmdline: C:\Windows\system32\cmd.exe /c cd Island MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 6428 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - cmd.exe (PID: 6500 cmdline: C:\Windows\system32\cmd.exe /c cd Matter m MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 6512 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - rundll32.exe (PID: 6488 cmdline: rundll32.exe C:\Users\user\Desktop\kS5hYPcgm8.dll,Problemscale MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - cmd.exe (PID: 6524 cmdline: C:\Windows\system32\cmd.exe /c cd Island MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 6728 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - cmd.exe (PID: 6936 cmdline: C:\Windows\system32\cmd.exe /c cd Matter m MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 7036 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - rundll32.exe (PID: 6720 cmdline: rundll32.exe C:\Users\user\Desktop\kS5hYPcgm8.dll,WingGrass MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - cmd.exe (PID: 6908 cmdline: C:\Windows\system32\cmd.exe /c cd Island MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 6924 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - cmd.exe (PID: 7060 cmdline: C:\Windows\system32\cmd.exe /c cd Matter m MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 7104 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - cmd.exe (PID: 6888 cmdline: C:\Windows\system32\cmd.exe /c cd Island MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - cmd.exe (PID: 6944 cmdline: C:\Windows\system32\cmd.exe /c cd Matter m MD5: F3BDBE3BB6F734E357235F4D5898582D)
- **cleanup**

Malware Configuration

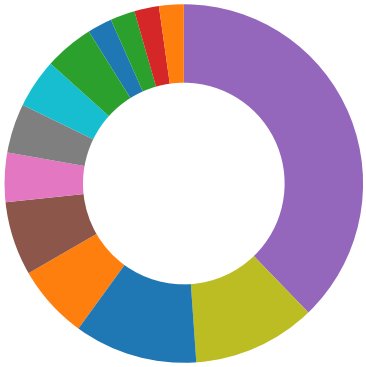
No configs have been found

Yara Overview

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected Ursnif

E-Banking Fraud:

Yara detected Ursnif

Hooking and other Techniques for Hiding and Protection:

Yara detected Ursnif

Stealing of Sensitive Information:

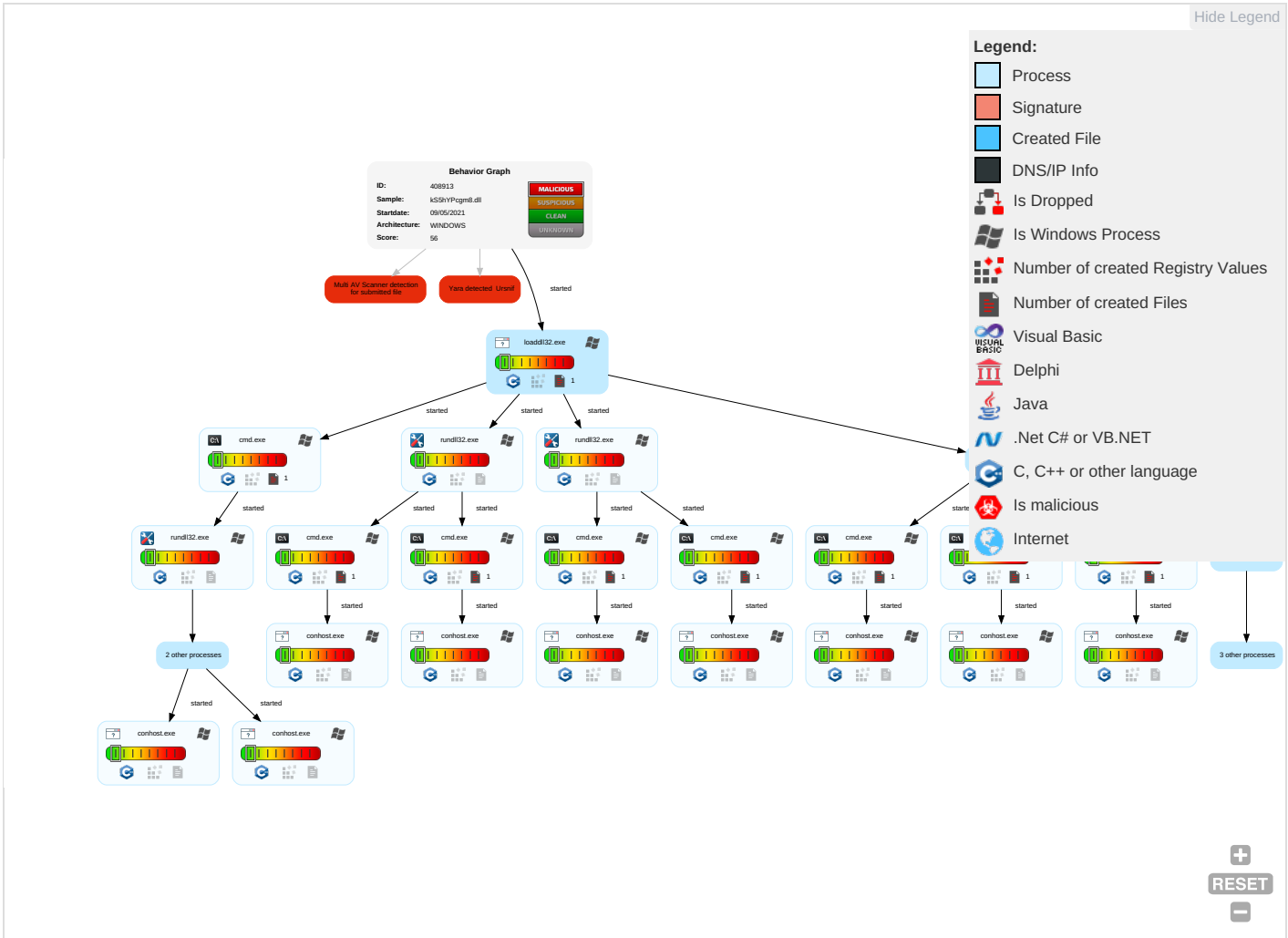
Yara detected Ursnif

Remote Access Functionality:

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
Valid Accounts	Native API 1	Path Interception	Process Injection 1 2	Rundll32 1	OS Credential Dumping	System Time Discovery 2	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Remotely Track Devic Without Authorizatic
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1 2	LSASS Memory	Security Software Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorizatic
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Deobfuscate/Decode Files or Information 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	System Information Discovery 2 3	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	

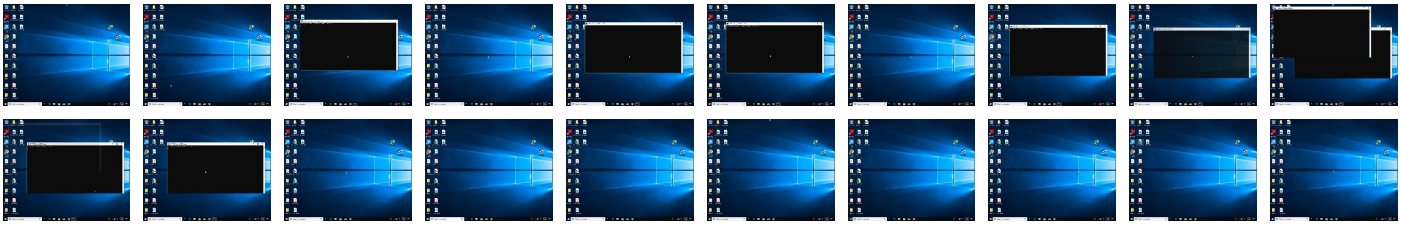
Behavior Graph



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
kS5hYPcgm8.dll	51%	Virustotal		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

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	408913
Start date:	09.05.2021
Start time:	08:08:08
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 5s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	kS5hYPcgm8.dll
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:	37
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:	MAL
Classification:	mal56.troj.winDLL@55/0@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 10.2% (good quality ratio 9.5%) • Quality average: 73.1% • Quality standard deviation: 27.3%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .dll
Warnings:	Show All • Report size exceeded maximum capacity and may have missing behavior information.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

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 (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.790056221303965
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.60% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	kS5hYPcgm8.dll
File size:	960000
MD5:	68fc6441db6c5539573adf08f210c39b
SHA1:	c67a6a85716e0f1439cae1c1cdf259c271515e85
SHA256:	802a752fca3ded051f0655c68012c769232d098d4a57c9887da39fa89070235a
SHA512:	e20656f24256170306d05c8604d8d22989304327993d0180a9e9e1d8d699fa6ff66d835c1fa5e120e4bfbd6c802b59f142d53dbb6e86844808b1338b301d5316
SSDEEP:	24576:HQfpzjXPgf28CJV4X+IBIJ3cazaLwj1mCG9CpNiLi:IFDgyJV4OaIRj150CpNiLi
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....t...0...0...0....{i.3...9...#...b...4...b...=...b...=....{r.&...0.....b.....b...1...b.b.1...0...1...b...1...Rich0.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x1040052
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x1000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5AC512FB [Wed Apr 4 18:01:31 2018 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	7a79d10b1d4343a18a4f6e25e165b4ae

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
cmp dword ptr [ebp+0Ch], 01h
jne 00007F2D188B94F7h
call 00007F2D188B9ED2h
push dword ptr [ebp+10h]
push dword ptr [ebp+0Ch]
push dword ptr [ebp+08h]
call 00007F2D188B939Fh
add esp, 0Ch
pop ebp
retn 000Ch
mov ecx, dword ptr [ebp-0Ch]
mov dword ptr fs:[00000000h], ecx
pop ecx
pop edi
pop edi
pop esi
pop ebx
mov esp, ebp
pop ebp
push ecx
ret
mov ecx, dword ptr [ebp-10h]
xor ecx, ebp
call 00007F2D188B8D06h
jmp 00007F2D188B94D0h
mov ecx, dword ptr [ebp-14h]
xor ecx, ebp
call 00007F2D188B8CF5h
jmp 00007F2D188B94BFh
push eax
push dword ptr fs:[00000000h]
lea eax, dword ptr [esp+0Ch]
sub esp, dword ptr [esp+0Ch]
push ebx
push esi

Instruction
push edi
mov dword ptr [eax], ebp
mov ebp, eax
mov eax, dword ptr [010E506Ch]
xor eax, ebp
push eax
push dword ptr [ebp-04h]
mov dword ptr [ebp-04h], FFFFFFFFh
lea eax, dword ptr [ebp-0Ch]
mov dword ptr fs:[00000000h], eax
ret
push eax
push dword ptr fs:[00000000h]
lea eax, dword ptr [esp+0Ch]
sub esp, dword ptr [esp+0Ch]
push ebx
push esi
push edi
mov dword ptr [eax], ebp
mov ebp, eax
mov eax, dword ptr [010E506Ch]
xor eax, ebp
push eax
mov dword ptr [ebp-10h], eax
push dword ptr [ebp-04h]
mov dword ptr [ebp-04h], FFFFFFFFh
lea eax, dword ptr [ebp-0Ch]
mov dword ptr fs:[00000000h], eax
ret
push eax
inc dword ptr fs:[eax]

Rich Headers

Programming Language:	• [IMP] VS2008 SP1 build 30729

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0xe35b0	0x9c	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0xe364c	0x8c	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xfd000	0x9d0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xfe000	0x5074	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xde820	0x54	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0xde878	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8a000	0x26c	.rdata
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	0x883dc	0x88400	False	0.544626218463	data	6.71833205917	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8a000	0x5a440	0x5a600	False	0.658643456086	data	5.95813601066	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xe5000	0x17ebc	0x1c00	False	0.184291294643	data	4.04646123564	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rsrc	0xfd000	0x9d0	0xa00	False	0.396484375	data	3.77819611332	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xfe000	0x5074	0x5200	False	0.726133765244	data	6.63977268899	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_DIALOG	0xfd1c0	0x10e	data	English	United States
RT_DIALOG	0xfd2d0	0xc0	dBase III DBT, next free block index 4294901761	English	United States
RT_DIALOG	0xfd390	0x126	data	English	United States
RT_DIALOG	0xfd4b8	0xf0	data	English	United States
RT_DIALOG	0xfd5a8	0xba	data	English	United States
RT_DIALOG	0xfd664	0xec	data	English	United States
RT_DIALOG	0xfd750	0x124	data	English	United States
RT_MANIFEST	0xfd874	0x15a	ASCII text, with CRLF line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	SetEnvironmentVariableA, FreeEnvironmentStringsW, GetEnvironmentStringsW, GetCommandLineW, GetProcessHeap, CreateFileW, SetStdHandle, ReadConsoleW, WriteConsoleW, HeapSize, SetEndOfFile, SetEnvironmentVariableW, GetOEMCP, IsValidCodePage, FindNextFileW, FindNextFileA, FindFirstFileExW, FindFirstFileExA, FindClose, GetTimeZoneInformation, OutputDebugStringA, OutputDebugStringW, WaitForSingleObjectEx, CreateSemaphoreA, GetSystemTimeAsFileTime, TlsGetValue, VirtualProtectEx, TlsAlloc, GetSystemDirectoryA, GetTempPathA, Sleep, GetCommandLineA, GetModuleHandleA, InitializeCriticalSection, SetSystemPowerState, EnterCriticalSection, VirtualProtect, GetModuleFileNameA, MultiByteToWideChar, GetLastError, FormatMessageW, WideCharToMultiByte, GetStringTypeW, LeaveCriticalSection, DeleteCriticalSection, SetLastError, InitializeCriticalSectionAndSpinCount, CreateEventW, SwitchToThread, TlsSetValue, TlsFree, GetTickCount, GetModuleHandleW, GetProcAddress, EncodePointer, DecodePointer, CompareStringW, LCMapStringW, GetLocaleInfoW, GetCPInfo, UnhandledExceptionFilter, SetUnhandledExceptionFilter, GetCurrentProcess, TerminateProcess, IsProcessorFeaturePresent, IsDebuggerPresent, GetStartupInfoW, QueryPerformanceCounter, GetCurrentProcessId, GetCurrentThreadId, InitializeSListHead, RtlUnwind, RaiseException, InterlockedPushEntrySList, InterlockedFlushSList, FreeLibrary, LoadLibraryExW, ExitProcess, GetModuleHandleExW, GetModuleFileNameW, HeapAlloc, HeapFree, GetCurrentThread, GetACP, GetStdHandle, GetFileType, CloseHandle, WaitForSingleObject, GetExitCodeProcess, CreateProcessA, CreateProcessW, GetFileAttributesExW, WriteFile, GetConsoleCP, GetConsoleMode, GetDateFormatW, GetTimeFormatW, IsValidLocale, GetUserDefaultLCID, EnumSystemLocalesW, FlushFileBuffers, ReadFile, SetFilePointerEx, HeapReAlloc, SetConsoleCtrlHandler, CreateThread
USER32.dll	SetFocus, GetCursorPos, RegisterClassExA, GetFocus, GetClassInfoExA, GetKeyNameTextA, GetWindowTextLengthA, CallWindowProcA, IsDlgButtonChecked, DestroyIcon, AppendMenuA, DrawIconEx, DrawEdge
GDI32.dll	BitBlt, DeleteDC, CreatePen, DeleteObject, CreateDCA, GetObjectA, DPtoLP
ole32.dll	OleUninitialize, OleSetContainedObject, OleInitialize
SHLWAPI.dll	PathFindFileNameA, PathAddBackslashW, PathStripToRootA
DCIMAN32.dll	DCICreatePrimary, DCIOpenProvider, GetDCRegionData, DCISetDestination, DCICloseProvider, DCICreateOverlay, GetWindowRegionData, DCIEndAccess, WinWatchDidStatusChange, DCICreateOffscreen, DCISetSrcDestClip, DCIDestroy, DCIDraw, DCISetClipList, DCIEnum, DCIBeginAccess, WinWatchClose

Exports

Name	Ordinal	Address
Connectdark	1	0x1021c64
Mindlake	2	0x1020de0
Porthigh	3	0x1021c2c
Problemscale	4	0x1021bf8
WingGrass	5	0x1021b0a

Possible Origin

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

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

System Behavior

Analysis Process: loaddll32.exe PID: 2212 Parent PID: 5620

General

Start time:	08:08:58
Start date:	09/05/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\kS5hYPcgm8.dll'
Imagebase:	0xeb0000
File size:	116736 bytes
MD5 hash:	542795ADF7CC08EFCF675D65310596E8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 4356 Parent PID: 2212

General

Start time:	08:08:58
Start date:	09/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\kS5hYPcgm8.dll',#1
Imagebase:	0x150000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 1140 Parent PID: 2212

General

Start time:	08:08:59
Start date:	09/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\kS5hYPcgm8.dll,Connectdark
Imagebase:	0xbe0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: 1556 Parent PID: 4356

General

Start time:	08:08:59
Start date:	09/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\kS5hYPcgm8.dll',#1
Imagebase:	0xbe0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: 2576 Parent PID: 1140

General

Start time:	08:08:59
Start date:	09/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c cd Island
Imagebase:	0x150000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 5700 Parent PID: 1556

General

Start time:	08:08:59
Start date:	09/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c cd Island
Imagebase:	0x150000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 4228 Parent PID: 2576

General

Start time:	08:08:59
Start date:	09/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: 6148 Parent PID: 5700

General

Start time:	08:08:59
Start date:	09/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: 6204 Parent PID: 1140

General

Start time:	08:09:00
Start date:	09/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c cd Matter m
Imagebase:	0x7ff797770000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 6240 Parent PID: 1556

General

Start time:	08:09:00
Start date:	09/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c cd Matter m
Imagebase:	0x150000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 6248 Parent PID: 6204

General

Start time:	08:09:00
Start date:	09/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: 6260 Parent PID: 6240

General

Start time:	08:09:00
Start date:	09/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: 6324 Parent PID: 2212

General

Start time:	08:09:02
Start date:	09/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\kS5hYPcgm8.dll,Mindlake
Imagebase:	0xbe0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: 6336 Parent PID: 6324

General

Start time:	08:09:03
Start date:	09/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c cd Island
Imagebase:	0x150000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 6348 Parent PID: 6336

General

Start time:	08:09:03
Start date:	09/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 6388 Parent PID: 2212

General

Start time:	08:09:05
Start date:	09/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\kS5hYPcgm8.dll,Porthigh
Imagebase:	0xbe0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 6396 Parent PID: 6324

General

Start time:	08:09:05

Start date:	09/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c cd Matter m
Imagebase:	0x150000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 6404 Parent PID: 6396

General

Start time:	08:09:06
Start date:	09/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 6416 Parent PID: 6388

General

Start time:	08:09:06
Start date:	09/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c cd Island
Imagebase:	0x150000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 6428 Parent PID: 6416

General

Start time:	08:09:07

Start date:	09/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 6488 Parent PID: 2212

General

Start time:	08:09:09
Start date:	09/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\kS5hYPcgm8.dll,Problemscale
Imagebase:	0xbe0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 6500 Parent PID: 6388

General

Start time:	08:09:10
Start date:	09/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c cd Matter m
Imagebase:	0x150000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 6512 Parent PID: 6500

General

Start time:	08:09:10
Start date:	09/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000

File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 6524 Parent PID: 6488

General

Start time:	08:09:10
Start date:	09/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c cd Island
Imagebase:	0x150000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 6720 Parent PID: 2212

General

Start time:	08:09:13
Start date:	09/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\kS5hYPcgm8.dll,WingGrass
Imagebase:	0xbe0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 6728 Parent PID: 6524

General

Start time:	08:09:13
Start date:	09/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 6888 Parent PID: 2212

General

Start time:	08:09:16
Start date:	09/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c cd Island
Imagebase:	0x150000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 6908 Parent PID: 6720

General

Start time:	08:09:17
Start date:	09/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c cd Island
Imagebase:	0x150000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 6924 Parent PID: 6908

General

Start time:	08:09:18
Start date:	09/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 6936 Parent PID: 6488

General

Start time:	08:09:20
Start date:	09/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c cd Matter m
Imagebase:	0x150000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 6944 Parent PID: 2212

General

Start time:	08:09:21
Start date:	09/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c cd Matter m
Imagebase:	0x150000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 7036 Parent PID: 6936

General

Start time:	08:09:26
Start date:	09/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 7060 Parent PID: 6720

General

Start time:	08:09:27
Start date:	09/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c cd Matter m
Imagebase:	0x150000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 7104 Parent PID: 7060

General

Start time:	08:09:28
Start date:	09/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis