ID: 829698
Sample Name:
DefendUpdate.exe
Cookbook: default.jbs
Time: 00:20:11
Date: 19/03/2023
Version: 37.0.0 Beryl

Table of Contents

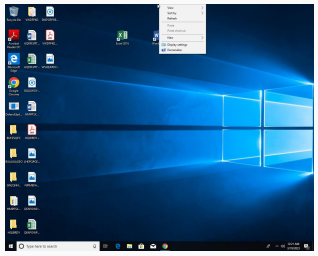
Windows Analysis Report

DefendUpdate.exe

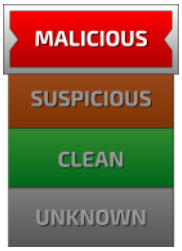
Overview

General Information

Sample Name:	DefendUpdate.exe
Analysis ID:	829698
MD5:	d9c8a47ef46ec..
SHA1:	d8abd4904ce2…
SHA256:	ae3e61c6db3e…
Tags:	exe
Infos:	



Detection

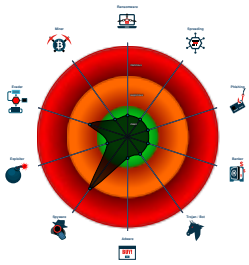


Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Tries to harvest and steal browser in…
- Sample execution stops while proce…
- Queries the volume information (nam…
- Program does not show much activi…
- Creates a process in suspended mo…
- PE file contains sections with non-s…

Classification



Process Tree

- **System is w10x64**
- DefendUpdate.exe (PID: 6016 cmdline: C:\Users\user\Desktop\DefendUpdate.exe MD5: D9C8A47EF46EC852F3EDDAD0EA93A799)
  - cmd.exe (PID: 1536 cmdline: C:\Windows\system32\cmd.exe /C choice /C Y /N /D Y /T 0 &Del C:\Users\user\Desktop\DefendUpdate.exe MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - conhost.exe (PID: 676 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - choice.exe (PID: 6136 cmdline: choice /C Y /N /D Y /T 0 MD5: EA29BC6BCB1EFCE9C9946C3602F3E754)
- **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

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

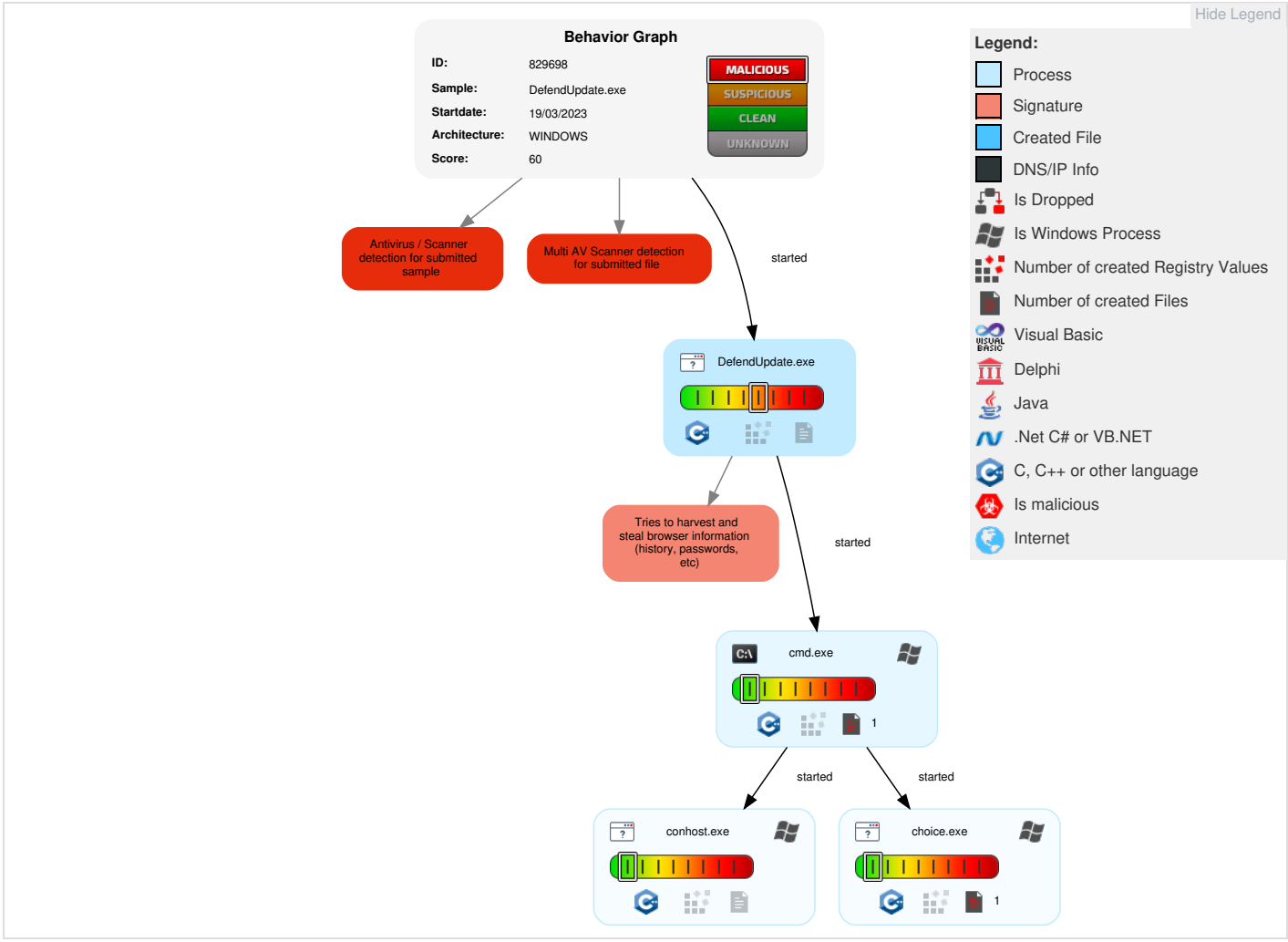
Stealing of Sensitive Information

Tries to harvest and steal browser information (history, passwords, etc)

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 1 Process Injection	1 Software Packing	1 OS Credential Dumping	1 Security Software Discovery	Remote Services	1 Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	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 1 Process Injection	LSASS Memory	1 File and Directory 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 Obfuscated Files or Information	Security Account Manager	1 1 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

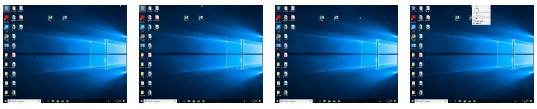
Behavior Graph



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
DefendUpdate.exe	28%	ReversingLabs	Win64.Trojan.Generic	
DefendUpdate.exe	30%	Virustotal		Browse
DefendUpdate.exe	100%	Avira	HEUR/AGEN.1250720	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://go-rod.github.io/#/compatibility?id=os:	0%	URL Reputation	safe	
http://https://go-rod.github.io/#/compatibility?id=osfunction(e)	0%	URL Reputation	safe	
http://https://registry.npmmirror.com/-/binary/chromium-browser-snapshots/%s/%d/%stls:	0%	URL Reputation	safe	
http://https://youtube.comif-unmodified-sinceillegal	0%	URL Reputation	safe	
http://https://www.youtube.comindex	0%	URL Reputation	safe	
http://www.bohemiancoding.com/sketch	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://go-rod.github.io/#/compatibility?id=os:	DefendUpdate.exe, 00000000.00000002.2505 06545.00000000010D1000.00000040.00000001 .01000000.00000003.sdmp	false	• URL Reputation: safe	unknown
http://https://go-rod.github.io/#/compatibility? id=osfunction(e)	DefendUpdate.exe, 00000000.00000002.2505 06545.00000000010D1000.00000040.00000001 .01000000.00000003.sdmp	false	• URL Reputation: safe	unknown
http:// https://studio.youtube.com/youtubei/v1/security/get_web_reauth_url?alt=json&key=tls:	DefendUpdate.exe, 00000000.00000002.2505 06545.00000000010D1000.00000040.00000001 .01000000.00000003.sdmp	false		high
http://https://registry.npmmirror.com/- /binary/chromium-browser-snapshots/%s/%d/%stls:	DefendUpdate.exe, 00000000.00000002.2505 06545.00000000010D1000.00000040.00000001 .01000000.00000003.sdmp	false	• URL Reputation: safe	unknown
http://https://studio.youtube.com/reauth	DefendUpdate.exe, 00000000.00000002.2505 06545.00000000010D1000.00000040.00000001 .01000000.00000003.sdmp	false		high
http://https://youtube.comif-unmodified-sinceillegal	DefendUpdate.exe, 00000000.00000002.2505 06545.00000000010D1000.00000040.00000001 .01000000.00000003.sdmp	false	• URL Reputation: safe	unknown
http://https://www.youtube.comindex	DefendUpdate.exe, 00000000.00000002.2505 06545.00000000010D1000.00000040.00000001 .01000000.00000003.sdmp	false	• URL Reputation: safe	unknown
http://www.bohemiancoding.com/sketch	DefendUpdate.exe, 00000000.00000002.2505 06545.00000000010D1000.00000040.00000001 .01000000.00000003.sdmp	false	• URL Reputation: safe	unknown
http:// https://www.youtube.com/getAccountSwitcherEndpoint mallocgc	DefendUpdate.exe, 00000000.00000002.2505 06545.00000000010D1000.00000040.00000001 .01000000.00000003.sdmp	false		high
http://https://youtube.com/inconsistent	DefendUpdate.exe, 00000000.00000002.2505 06545.00000000010D1000.00000040.00000001 .01000000.00000003.sdmp	false		high
http://https://golang.org/pkg/time/#ParseDuration)	DefendUpdate.exe, 00000000.00000002.2505 06545.00000000010D1000.00000040.00000001 .01000000.00000003.sdmp	false		high
http://https://studio.youtube.com/youtubei/v1/ars/grst? alt=json&key=net/http:	DefendUpdate.exe, 00000000.00000002.2505 06545.00000000010D1000.00000040.00000001 .01000000.00000003.sdmp	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	829698
Start date and time:	2023-03-19 00:20:11 +01:00
Joe Sandbox Product:	CloudBasic

Overall analysis duration:	0h 2m 39s
Hypervisor based Inspection enabled:	false
Report type:	light
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:	4
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:	DefendUpdate.exe
Detection:	MAL
Classification:	mal60.spyw.winEXE@6/0@0/0
EGA Information:	Failed
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 • Stop behavior analysis, all processes terminated

Warnings

- Excluded domains from analysis (whitelisted): fs.microsoft.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) x86-64 (stripped to external PDB), for MS Windows
Entropy (8bit):	7.999924637565079
TrID:	• UPX compressed Win32 Executable (30571/9) 65.62% • Win64 Executable (generic) (12005/4) 25.77% • Generic Win/DOS Executable (2004/3) 4.30% • DOS Executable Generic (2002/1) 4.30% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.02%
File name:	DefendUpdate.exe
File size:	4510208
MD5:	d9c8a47ef46ec852f3eddad0ea93a799
SHA1:	d8abd4904ce2a225226278556511473c1d0ea406
SHA256:	ae3e61c6db3e5886a7265c46658833259e5342e0f233fd980e9b4243d16f3336
SHA512:	fc8e15d901ee0050d09222c6dd8009151ca8e3683a6dd121190cde62f7583e8562213d5147abc266e5491ae244823d39c1f3e3a8f497b4ff8d7476a89ee9be27
SSDEEP:	98304:P6FJfC8HbiXNMLpU2MSJ8LIKZl9ll6QXengLduSkE:NauOU2xlsekenwdRkE
TLSH:	A32633750289C829F97377F4A27F0E70530E3A0E95BF7371898B66755890EF86CA6072
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d...vp.d....."..D.....@.....@.....`... .....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x125d040
Entrypoint Section:	UPX1
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, LARGE_ADDRESS_AWARE, DEBUG_STRIPPED
DLL Characteristics:	HIGH_ENTROPY_VA, DYNAMIC_BASE, NX_COMPAT, TERMINAL_SERVER_AWARE
Time Stamp:	0x64157076 [Sat Mar 18 08:04:06 2023 UTC]
TLS Callbacks:	0x125dbed
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	1
File Version Major:	6
File Version Minor:	1
Subsystem Version Major:	6
Subsystem Version Minor:	1
Import Hash:	9aebf3da4677af9275c461261e5abde3

Entrypoint Preview

Instruction
push ebx
push esi
push edi
push ebp
dec eax
lea esi, dword ptr [FFBB3FDAh]
dec eax
lea edi, dword ptr [esi-00A10025h]
dec eax
lea eax, dword ptr [edi+00E2EC5Ch]
push dword ptr [eax]
mov dword ptr [eax], 81304EFEh
push eax
push edi
mov eax, 00E5B5C4h
push eax
dec eax
mov ecx, esp
dec eax
mov edx, edi
dec eax
mov edi, esi
mov esi, 0044C017h
push ebp
dec eax
mov ebp, esp
inc esp
mov ecx, dword ptr [ecx]
dec ecx
mov eax, edx
dec eax
mov edx, esi
dec eax
lea esi, dword ptr [edi+02h]
push esi
mov al, byte ptr [edi]
dec edx
mov cl, al
and al, 07h
shr cl, 00000003h
dec eax
mov ebx, FFFFFD00h
dec eax
shl ebx, cl
mov cl, al
dec eax
lea ebx, dword ptr [esp+ebx*2-00000E78h]
dec eax
and ebx, FFFFFFC0h
push 00000000h
dec eax
cmp esp, ebx
jne 00007F841CCE855Bh
push ebx
dec eax
lea edi, dword ptr [ebx+08h]
mov cl, byte ptr [esi-01h]
dec edx
mov byte ptr [edi+02h], al

Instruction
mov al, cl
shr cl, 00000004h
mov byte ptr [edi+01h], cl
and al, 0Fh
mov byte ptr [edi], al
dec eax
lea ecx, dword ptr [edi-04h]
push eax
inc ecx
push edi
dec eax
lea eax, dword ptr [edi+04h]
inc ebp
xor edi, edi
inc ecx
push esi
inc ecx
mov esi, 00000001h
inc ecx
push ebp
inc ebp
xor ebp, ebp
inc ecx
push esp
push ebp
push ebx
dec eax
mov dword ptr [esp-10h], ecx
dec eax
mov dword ptr [esp-28h], eax
mov eax, 00000001h
dec eax
mov dword ptr [esp-08h], esi
dec esp
mov dword ptr [esp-18h], eax
mov ebx, eax
inc esp

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0xe30000	0x159	UPX1
IMAGE_DIRECTORY_ENTRY_IMPORT	0xe5e000	0xd0	UPX2
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0xdb9000	0x5e20	UPX1
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xe5e0d0	0x14	UPX2
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0xe5dc18	0x28	UPX1
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x0	0x0	
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
UPX0	0x1000	0xa10000	0x0	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
UPX1	0xa11000	0x44d000	0x44ce00	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
UPX2	0xe5e000	0x1000	0x200	False	0.28125	data	2.097972113314606	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE

Imports

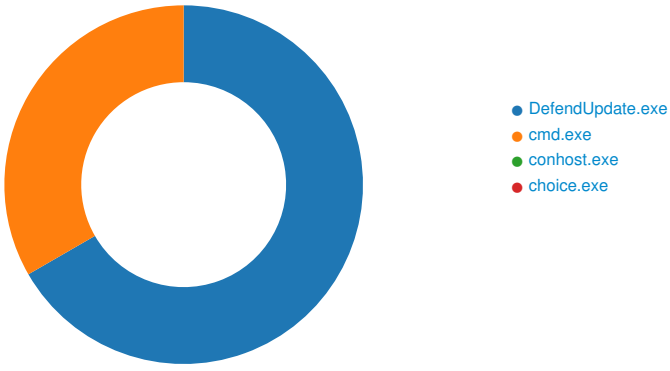
DLL	Import
KERNEL32.DLL	LoadLibraryA, ExitProcess, GetProcAddress, VirtualProtect
msvcrt.dll	exit

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: DefendUpdate.exe PID: **6016**, Parent PID: **3452**

General

Target ID:	0
Start time:	00:21:04
Start date:	19/03/2023
Path:	C:\Users\user\Desktop\DefendUpdate.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\DefendUpdate.exe

Imagebase:	0x10d0000
File size:	4510208 bytes
MD5 hash:	D9C8A47EF46EC852F3EDDAD0EA93A799
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Analysis Process: cmd.exe PID: **1536**, Parent PID: **6016**

General

Target ID:	1
Start time:	00:21:05
Start date:	19/03/2023
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\cmd.exe /C choice /C Y /N /D Y /T 0 &Del C:\Users\user\Desktop\DefendUpdate.exe
Imagebase:	0x7ff707bb0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
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

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\DefendUpdate.exe	cannot delete	1	7FF707BC90F0	DeleteFileW
C:\Users\user\Desktop\DefendUpdate.exe	cannot delete	1	7FF707BC90F0	DeleteFileW

Analysis Process: conhost.exe PID: **676**, Parent PID: **1536**

General

Target ID:	2
Start time:	00:21:05
Start date:	19/03/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
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: choice.exe PID: **6136**, Parent PID: **1536**

General

Target ID:	3

Start time:	00:21:06
Start date:	19/03/2023
Path:	C:\Windows\System32\choice.exe
Wow64 process (32bit):	false
Commandline:	choice /C Y /N /D Y /T 0
Imagebase:	0x7ff66f650000
File size:	33280 bytes
MD5 hash:	EA29BC6BCB1EFCE9C9946C3602F3E754
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Disassembly

No disassembly