ID: 715067
Sample Name: empudh9lY5
Cookbook: default.jbs
Time: 15:49:52
Date: 03/10/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents 2
Windows Analysis Report empudh9lY5 3
Overview 3
General Information 3
Detection 3
Signatures 3
Classification 3
Process Tree 3
Malware Configuration 3
Yara Signatures 3
Memory Dumps 3
Sigma Signatures 4
Snort Signatures 5
Joe Sandbox Signatures 5
AV Detection 5
System Summary 5
Mitre Att&ck Matrix 5
Behavior Graph 5
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 8
Contacted Domains 8
World Map of Contacted IPs 8
Public IPs 8
General Information 8
Warnings 9
Simulations 9
Behavior and APIs 9
Joe Sandbox View / Context 9
IPs 9
Domains 9
ASNs 9
JA3 Fingerprints 9
Dropped Files 9
Created / dropped Files 9
Static File Info 9
General 10
File Icon 10
Static PE Info 10
General 10
Entrypoint Preview 10
Data Directories 11
Sections 12
Resources 12
Imports 14
Exports 15
Possible Origin 16
Network Behavior 16
Network Port Distribution 16
TCP Packets 16
UDP Packets 17
DNS Queries 17
DNS Answers 17
Statistics 17
System Behavior 17
Analysis Process: empudh9lY5.exePID: 2560, Parent PID: 3452 17
General 17
File Activities 18
Disassembly 18

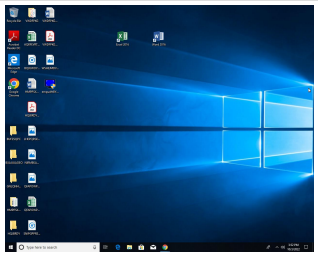
Windows Analysis Report

empudh9lY5

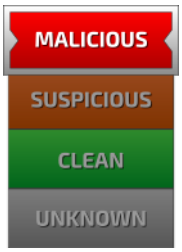
Overview

General Information

Sample Name:	empudh9lY5 (renamed file extension from none to exe)
Analysis ID:	715067
MD5:	8f43b86f351db10.
SHA1:	ad9b43ecbae064..
SHA256:	9830e0d007c073..
Infos:	



Detection

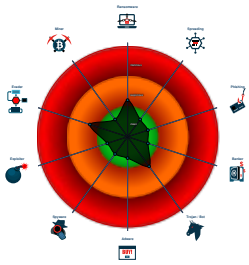


Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Malicious sample detected (through…
- Multi AV Scanner detection for subm…
- Uses 32bit PE files
- Yara signature match
- Found large amount of non-executed…
- PE file contains strange resources
- Contains functionality to read the PE…
- Uses code obfuscation techniques (…
- Detected TCP or UDP traffic on non…
- Detected potential crypto function
- Found potential string decryption / a…

Classification



Process Tree

- **System is w10x64**
- empudh9lY5.exe (PID: 2560 cmdline: C:\Users\user\Desktop\empudh9lY5.exe MD5: 8F43B86F351DB105A727E67E39459D78)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
00000000.00000002.516789881.0000000000570000.00000040.00001000.00020000.00000000.sdmp	CoreImpact_sysdll_exe	Detects a malware sysdll.exe from the Rocket Kitten APT	Florian Roth	• 0x1e799:$x6: /info.dat • 0x1e6bf:$z2: Encountered error sending error message to client • 0x1e68b:$z3: Encountered error building error message to client • 0x1e4b3:$z4: Attempting to unlock uninitialized lock! • 0x1e273:$z5: connect_back_tcp_channel#do_connect:: Error resolving connect back hostname • 0x1e343:$z6: select_event_get(): fd not found • 0x1e6f3:$z7: Encountered error sending syscall response to client • 0x20d8b:$z8: GetProcAddress() error • 0x1e498:$z9: Error entering thread lock • 0x1e4dc:$z10: Error exiting thread lock • 0x1e2bf:$z11: connect_back_tcp_channel_init:: socket() failed • 0x1e73e:$z12: event_add() failed for ev. • 0x1e728:$z13: Uh, oh, exit() failed • 0x1e73e:$z14: event_add() failed for ev. • 0x1e759:$z15: event_add() failed. • 0x1e77e:$z16: needroot • 0x1e78e:$z17: ./plugins/
00000000.00000002.516789881.0000000000570000.00000040.00001000.00020000.00000000.sdmp	WoolenGoldfish_Generic_3	Detects a operation Woolen-Goldfish sample - http://goo.gl/NpJpVZ	Florian Roth	• 0x1e273:$x3: connect_back_tcp_channel#do_connect:: Error resolving connect back hostname • 0x48fb:$s0: kernel32.dll GetProcAddressLoadLibraryAws2_32.dll • 0x1e4b3:$s2: Attempting to unlock uninitialized lock! • 0x20910:$s4: unable to load kernel32.dll • 0x1e6f3:$s7: Encountered error sending syscall response to client • 0x1e799:$s9: /info.dat • 0x1e498:$s10: Error entering thread lock • 0x1e4dc:$s11: Error exiting thread lock • 0x1e2bf:$s12: connect_back_tcp_channel_init:: socket() failed
Process Memory Space: empudh9lY5.exe PID: 2560	CoreImpact_sysdll_exe	Detects a malware sysdll.exe from the Rocket Kitten APT	Florian Roth	• 0x8395:$x6: /info.dat • 0x87ba:$x6: /info.dat • 0x82ce:$z2: Encountered error sending error message to client • 0x829b:$z3: Encountered error building error message to client • 0x80e7:$z4: Attempting to unlock uninitialized lock! • 0x7eb9:$z5: connect_back_tcp_channel#do_connect:: Error resolving connect back hostname • 0x7f85:$z6: select_event_get(): fd not found • 0x8300:$z7: Encountered error sending syscall response to client • 0x8ed9:$z8: GetProcAddress() error • 0x80cc:$z9: Error entering thread lock • 0x8110:$z10: Error exiting thread lock • 0x7f05:$z11: connect_back_tcp_channel_init:: socket() failed • 0x834b:$z12: event_add() failed for ev. • 0x8335:$z13: Uh, oh, exit() failed • 0x834b:$z14: event_add() failed for ev. • 0x8366:$z15: event_add() failed. • 0x837a:$z16: needroot • 0x838a:$z17: ./plugins/
Process Memory Space: empudh9lY5.exe PID: 2560	WoolenGoldfish_Generic_3	Detects a operation Woolen-Goldfish sample - http://goo.gl/NpJpVZ	Florian Roth	• 0x7eb9:$x3: connect_back_tcp_channel#do_connect:: Error resolving connect back hostname • 0x7c4c:$s0: kernel32.dll GetProcAddressLoadLibraryAws2_32.dll • 0x80e7:$s2: Attempting to unlock uninitialized lock! • 0x8a82:$s4: unable to load kernel32.dll • 0x8300:$s7: Encountered error sending syscall response to client • 0x8395:$s9: /info.dat • 0x87ba:$s9: /info.dat • 0x80cc:$s10: Error entering thread lock • 0x8110:$s11: Error exiting thread lock • 0x7f05:$s12: connect_back_tcp_channel_init:: socket() failed

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

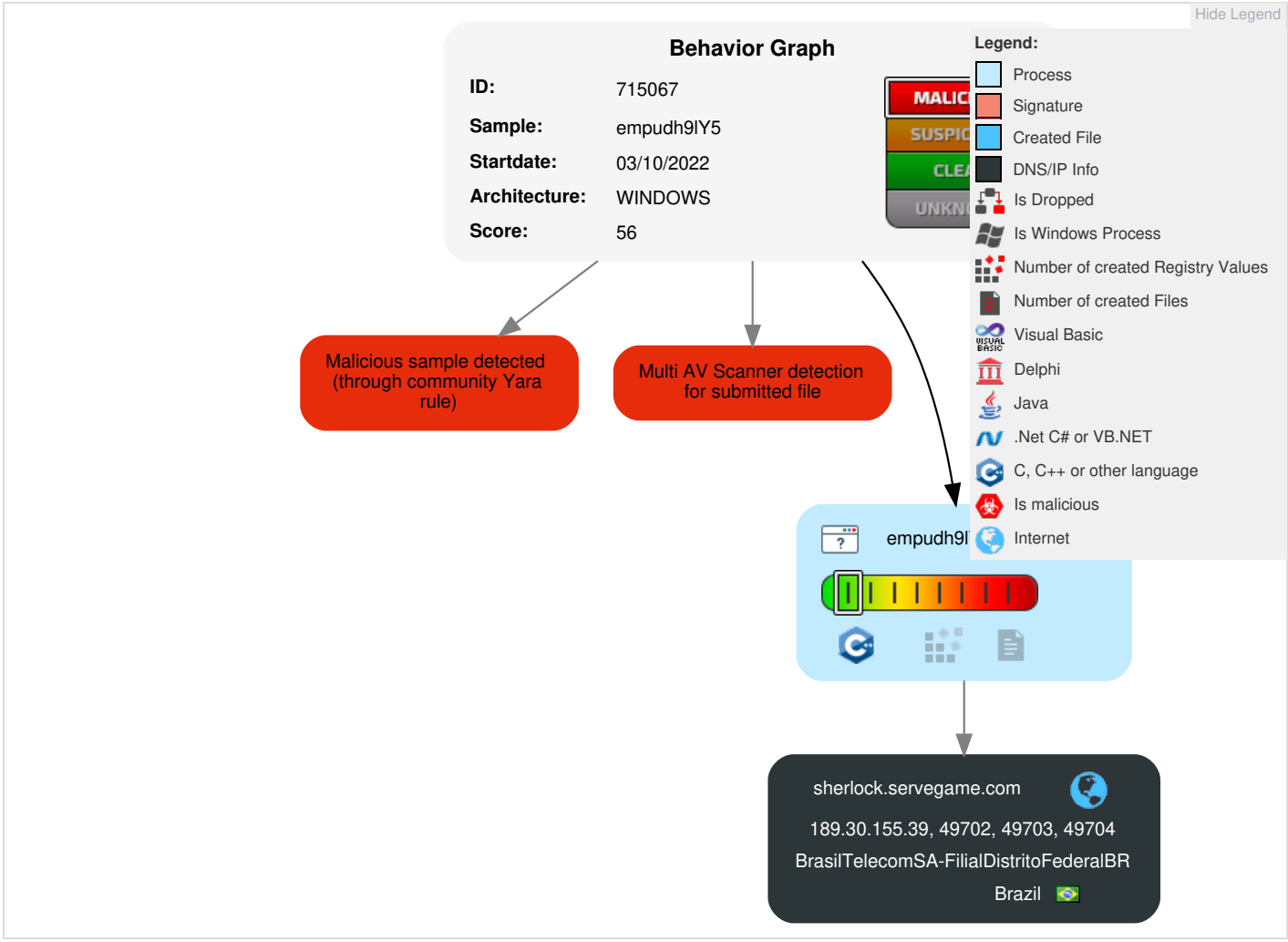
System Summary

Malicious sample detected (through community Yara rule)

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	Path Interception	1 Software Packing	OS Credential Dumping	1 System Information 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 Deobfuscate/Decode Files or Information	LSASS Memory	1 Remote System Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	3 Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud

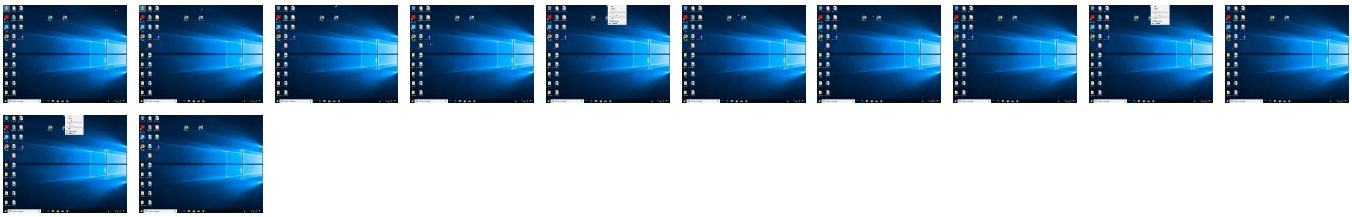
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
empudh9lY5.exe	22%	ReversingLabs	Win32.Trojan.Gholee	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

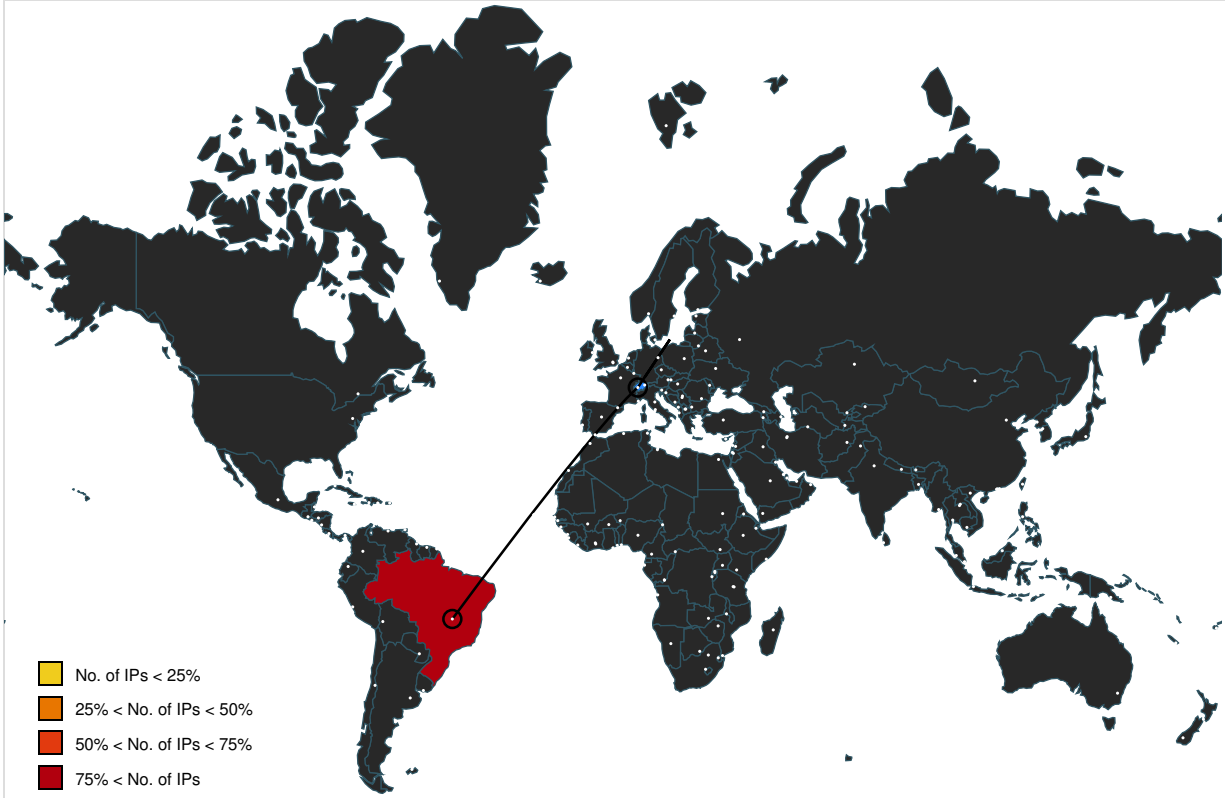
No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
sherlock.servegame.com	189.30.155.39	true	false		unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
189.30.155.39	sherlock.servegame.com	Brazil		8167	BrasilTelecomSA-FilialDistritoFederalBR	false

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	715067
Start date and time:	2022-10-03 15:49:52 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 26s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	empudh9lY5 (renamed file extension from none to 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:	MAL
Classification:	mal56.winEXE@1/0@3/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, ocsp.digicert.com, ctldl.windowsupdate.com
- Not all processes where analyzed, report is missing behavior information
- VT rate limit hit for: empudh9lY5.exe

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 (stripped to external PDB), for MS Windows
Entropy (8bit):	6.2099397885668255
TrID:	• Win32 Executable (generic) a (10002005/4) 98.87% • InstallShield setup (43055/19) 0.43% • Win32 EXE PECompact compressed (generic) (41571/9) 0.41% • Windows Screen Saver (13104/52) 0.13% • DOS Executable Borland C++ (13009/5) 0.13%
File name:	empudh9lY5.exe
File size:	1283072
MD5:	8f43b86f351db105a727e67e39459d78
SHA1:	ad9b43ecbae064ddca1908c40999974bc28466ba
SHA256:	9830e0d007c07364bf97b2a3e0496b7a7f5811e7e71fcdd9dada104d29d1982c
SHA512:	e8d59fceaa01d7ef3b5ced15f15d75a0bdd0bd3cc828a741798798e4527f4d58051a2b3c5a028f347c42a49f760d918bd9f1d46f7ab8adccf5837db024982011
SSDEEP:	24576:pmUgVoR4T0gR1U2vfVD8sA15qkJ1K3mbDQca9L32GY:pGoqT0ujvTO6L3
TLSH:	27555AA27694C132C0620674DD6BCAF964357E24DF30A5877BE03F4F3EB5B807926296
File Content Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7.....

File Icon

Icon Hash:	6117164569166de9

Static PE Info

General

Entrypoint:	0x40138c
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, DEBUG_STRIPPED
DLL Characteristics:	
Time Stamp:	0x4B3D3B00 [Fri Jan 1 00:00:00 2010 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	cafc89e1b0a9b2c5b10389d6d19936ce

Entrypoint Preview

Instruction
jmp 00007F2114C4EAC2h
bound di, dword ptr [edx]
inc ebx
sub ebp, dword ptr [ebx]
dec eax
dec edi
dec edi
dec ebx
nop
jmp 00007F2115114B4Dh
mov eax, dword ptr [004C608Bh]
shl eax, 02h
mov dword ptr [004C608Fh], eax

Instruction
push edx
push 00000000h
call 00007F2114D12010h
mov edx, eax
call 00007F2114D0326Fh
pop edx
call 00007F2114D03191h
call 00007F2114D032A4h
push 00000000h
call 00007F2114D044D9h
pop ecx
push 004C6034h
push 00000000h
call 00007F2114D11FEAh
mov dword ptr [004C6093h], eax
push 00000000h
jmp 00007F2114D0D99Ch
jmp 00007F2114D0450Bh
xor eax, eax
mov al, byte ptr [004C607Dh]
ret
mov eax, dword ptr [004C6093h]
ret
pushad
mov ebx, BCB05000h
push ebx
push 00000BADh
ret
mov ecx, 000000E4h
or ecx, ecx
je 00007F2114C4EAFFh
cmp dword ptr [004C608Bh], 00000000h
jnc 00007F2114C4EABCh
mov eax, 000000FEh
call 00007F2114C4EA8Ch
mov ecx, 000000E4h
push ecx
push 00000008h
call 00007F2114D11FA7h
push eax
call 00007F2114D11FF5h
or eax, eax
jne 00007F2114C4EABCh
mov eax, 000000FDh
call 00007F2114C4EA6Bh
push eax
push eax
push dword ptr [004C608Bh]
call 00007F2114D0DB66h
push dword ptr [004C608Bh]

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0xfc000	0x482	.edata
IMAGE_DIRECTORY_ENTRY_IMPORT	0xf9000	0x24e5	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xfd000	0x489e3	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0xf8000	0x18	.rdata
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
.text	0x1000	0xc5000	0xc4200	False	0.5265893881453155	data	6.9280540298858515	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0xc6000	0x31000	0x29200	False	0.3381637063069909	data	5.3675051401997385	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.tls	0xf7000	0x1000	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rdata	0xf8000	0x1000	0x200	False	0.05078125	data	0.2108262677871819	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.idata	0xf9000	0x3000	0x2600	False	0.3246299342105263	data	5.165811799711141	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.edata	0xfc000	0x1000	0x600	False	0.3919270833333333	data	4.649758707069864	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0xfd000	0x489e3	0x48a00	False	0.07789304539586919	data	3.41590450767586	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x146000	0xc000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_BITMAP	0xfe558	0x5c	Device independent bitmap graphic, 9 x 11 x 1, image size 44		
RT_BITMAP	0xfe5b4	0x64	Device independent bitmap graphic, 11 x 13 x 1, image size 52		
RT_BITMAP	0xfe618	0x6c	Device independent bitmap graphic, 13 x 15 x 1, image size 60		
RT_BITMAP	0xfe684	0x74	Device independent bitmap graphic, 15 x 17 x 1, image size 68		
RT_BITMAP	0xfe6f8	0x7c	Device independent bitmap graphic, 15 x 19 x 1, image size 76		
RT_BITMAP	0xfe774	0x84	Device independent bitmap graphic, 17 x 21 x 1, image size 84		
RT_BITMAP	0xfe7f8	0x8c	Device independent bitmap graphic, 19 x 23 x 1, image size 92		
RT_BITMAP	0xfe884	0x94	Device independent bitmap graphic, 21 x 25 x 1, image size 100		
RT_BITMAP	0xfe918	0x9c	Device independent bitmap graphic, 21 x 27 x 1, image size 108		
RT_BITMAP	0xfe9b4	0xb0	Device independent bitmap graphic, 14 x 9 x 4, image size 72		
RT_BITMAP	0xfea64	0xec	Device independent bitmap graphic, 18 x 11 x 4, image size 132		
RT_BITMAP	0xfeb50	0x104	Device independent bitmap graphic, 22 x 13 x 4, image size 156		

Name	RVA	Size	Type	Language	Country
RT_BITMAP	0xfec54	0x158	Device independent bitmap graphic, 26 x 15 x 4, image size 240		
RT_BITMAP	0xfedac	0x178	Device independent bitmap graphic, 26 x 17 x 4, image size 272		
RT_BITMAP	0xfef24	0x198	Device independent bitmap graphic, 30 x 19 x 4, image size 304		
RT_BITMAP	0xff0bc	0x20c	Device independent bitmap graphic, 34 x 21 x 4, image size 420		
RT_BITMAP	0xff2c8	0x234	Device independent bitmap graphic, 38 x 23 x 4, image size 460		
RT_BITMAP	0xff4fc	0x25c	Device independent bitmap graphic, 38 x 25 x 4, image size 500		
RT_BITMAP	0xff758	0x5c	Device independent bitmap graphic, 9 x 11 x 1, image size 44		
RT_BITMAP	0xff7b4	0x64	Device independent bitmap graphic, 11 x 13 x 1, image size 52		
RT_BITMAP	0xff818	0x6c	Device independent bitmap graphic, 13 x 15 x 1, image size 60		
RT_BITMAP	0xff884	0x74	Device independent bitmap graphic, 15 x 17 x 1, image size 68		
RT_BITMAP	0xff8f8	0x7c	Device independent bitmap graphic, 15 x 19 x 1, image size 76		
RT_BITMAP	0xff974	0x84	Device independent bitmap graphic, 17 x 21 x 1, image size 84		
RT_BITMAP	0xff9f8	0x8c	Device independent bitmap graphic, 19 x 23 x 1, image size 92		
RT_BITMAP	0xffa84	0x94	Device independent bitmap graphic, 21 x 25 x 1, image size 100		
RT_BITMAP	0xffb18	0x9c	Device independent bitmap graphic, 21 x 27 x 1, image size 108		
RT_BITMAP	0xffbb4	0xb0	Device independent bitmap graphic, 14 x 9 x 4, image size 72		
RT_BITMAP	0xffc64	0xec	Device independent bitmap graphic, 18 x 11 x 4, image size 132		
RT_BITMAP	0xffd50	0x104	Device independent bitmap graphic, 22 x 13 x 4, image size 156		
RT_BITMAP	0xffe54	0x158	Device independent bitmap graphic, 26 x 15 x 4, image size 240		
RT_BITMAP	0xfffac	0x178	Device independent bitmap graphic, 26 x 17 x 4, image size 272		
RT_BITMAP	0x100124	0x198	Device independent bitmap graphic, 30 x 19 x 4, image size 304		
RT_BITMAP	0x1002bc	0x20c	Device independent bitmap graphic, 34 x 21 x 4, image size 420		
RT_BITMAP	0x1004c8	0x234	Device independent bitmap graphic, 38 x 23 x 4, image size 460		
RT_BITMAP	0x1006fc	0x25c	Device independent bitmap graphic, 38 x 25 x 4, image size 500		
RT_ICON	0x100958	0x882	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_ICON	0x1011dc	0x94a8	Device independent bitmap graphic, 96 x 192 x 32, image size 0	English	United States
RT_ICON	0x10a684	0x7258	Device independent bitmap graphic, 84 x 168 x 32, image size 0	English	United States
RT_ICON	0x1118dc	0x67e8	Device independent bitmap graphic, 80 x 160 x 32, image size 0	English	United States
RT_ICON	0x1180c4	0x5488	Device independent bitmap graphic, 72 x 144 x 32, image size 0	English	United States
RT_ICON	0x11d54c	0x4228	Device independent bitmap graphic, 64 x 128 x 32, image size 0	English	United States
RT_ICON	0x121774	0x3a48	Device independent bitmap graphic, 60 x 120 x 32, image size 0	English	United States
RT_ICON	0x1251bc	0x32e8	Device independent bitmap graphic, 56 x 112 x 32, image size 0	English	United States
RT_ICON	0x1284a4	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	English	United States
RT_ICON	0x12aa4c	0x1a68	Device independent bitmap graphic, 40 x 80 x 32, image size 0	English	United States
RT_ICON	0x12c4b4	0x1588	Device independent bitmap graphic, 36 x 72 x 32, image size 0	English	United States

Name	RVA	Size	Type	Language	Country
RT_ICON	0x12da3c	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	English	United States
RT_ICON	0x12eae4	0xcd8	Device independent bitmap graphic, 28 x 56 x 32, image size 0	English	United States
RT_ICON	0x12f7bc	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0	English	United States
RT_ICON	0x130144	0x6b8	Device independent bitmap graphic, 20 x 40 x 32, image size 0	English	United States
RT_ICON	0x1307fc	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	English	United States
RT_DIALOG	0x130c64	0x76	data		
RT_STRING	0x130cdc	0x35c	data		
RT_STRING	0x131038	0xdc	data		
RT_STRING	0x131114	0x10c	data		
RT_STRING	0x131220	0x33c	data		
RT_STRING	0x13155c	0x3dc	data		
RT_STRING	0x131938	0xf0	data		
RT_STRING	0x131a28	0xd8	data		
RT_STRING	0x131b00	0x274	data		
RT_STRING	0x131d74	0x3d8	data		
RT_STRING	0x13214c	0x374	data		
RT_STRING	0x1324c0	0x2dc	data		
RT_STRING	0x13279c	0x390	data		
RT_STRING	0x132b2c	0x454	data		
RT_RCDATA	0x132f80	0x10	data		
RT_RCDATA	0x132f90	0x734	Delphi compiled form 'TAddCEADataForm'		
RT_RCDATA	0x1336c4	0x3ca	Delphi compiled form 'TAddDIDDataForm'		
RT_RCDATA	0x133a90	0x15c7	Delphi compiled form 'TAudioFormatForm'		
RT_RCDATA	0x135058	0x78f	Delphi compiled form 'TAudioFormatListForm'		
RT_RCDATA	0x1357e8	0xb12	Delphi compiled form 'TColorimetryForm'		
RT_RCDATA	0x1362fc	0xff	Delphi compiled form 'TCommonForm'		
RT_RCDATA	0x1363fc	0x1aa2	Delphi compiled form 'TDetailedResolutionForm'		
RT_RCDATA	0x137ea0	0x7e4	Delphi compiled form 'TDIDDetailedResolutionListForm'		
RT_RCDATA	0x138684	0x2216	Delphi compiled form 'TDisplayForm'		
RT_RCDATA	0x13a89c	0x1c20	Delphi compiled form 'TExtensionBlockForm'		
RT_RCDATA	0x13c4bc	0x45f	Delphi compiled form 'TFreeSyncRangeForm'		
RT_RCDATA	0x13c91c	0x16d1	Delphi compiled form 'THDMI2SupportForm'		
RT_RCDATA	0x13dff0	0x4f3	Delphi compiled form 'THDMIResolutionForm'		
RT_RCDATA	0x13e4e4	0x18dd	Delphi compiled form 'THDMISupportForm'		
RT_RCDATA	0x13fdc4	0x830	Delphi compiled form 'THDRStaticMetadataForm'		
RT_RCDATA	0x1405f4	0xf41	Delphi compiled form 'TPropertiesForm'		
RT_RCDATA	0x141538	0xee8	Delphi compiled form 'TSpeakerSetupForm'		
RT_RCDATA	0x142420	0x581	Delphi compiled form 'TStandardResolutionForm'		
RT_RCDATA	0x1429a4	0x13af	Delphi compiled form 'TTiledDisplayTopologyForm'		
RT_RCDATA	0x143d54	0x556	Delphi compiled form 'TTVResolutionForm'		
RT_RCDATA	0x1442ac	0x7d2	Delphi compiled form 'TTVResolutionListForm'		
RT_RCDATA	0x144a80	0xaba	Delphi compiled form 'TVideoCapabilityForm'		
RT_GROUP_ICON	0x14553c	0xe6	GLS_BINARY_LSB_FIRST	English	United States
RT_MANIFEST	0x145624	0x3bf	ASCII text, with CRLF line terminators		

Imports

DLL	Import
SETUPAPI.DLL	SetupDiDestroyDeviceInfoList, SetupDiEnumDeviceInfo, SetupDiGetClassDevsA
ADVAPI32.DLL	RegCloseKey, RegCreateKeyExA, RegDeleteKeyA, RegDeleteValueA, RegEnumKeyExA, RegFlushKey, RegOpenKeyExA, RegQueryValueExA, RegSetValueExA

DLL	Import
KERNEL32.DLL	CloseHandle, CompareStringA, CreateEventA, CreateFileA, CreateThread, DeleteCriticalSection, DeleteFileA, EnterCriticalSection, EnumCalendarInfoA, ExitProcess, FindClose, FindFirstFileA, FindResourceA, FormatMessageA, FreeLibrary, FreeResource, GetACP, GetCPInfo, GetCommandLineA, GetCurrentProcessId, GetCurrentThreadId, GetDateFormatA, GetDiskFreeSpaceA, GetEnvironmentStrings, GetFileAttributesA, GetFileType, GetFullPathNameA, GetLastError, GetLocalTime, GetLocaleInfoA, GetModuleFileNameA, GetModuleHandleA, GetOEMCP, GetProcAddress, GetProcessHeap, GetStartupInfoA, GetStdHandle, GetStringTypeA, GetStringTypeW, GetSystemDefaultLangID, GetThreadLocale, GetTickCount, GetUserDefaultLCID, GetVersion, GetVersionExA, GlobalAddAtomA, GlobalDeleteAtom, GlobalFindAtomA, HeapAlloc, HeapFree, InitializeCriticalSection, InterlockedDecrement, InterlockedExchange, InterlockedIncrement, IsValidLocale, LCMapStringA, LeaveCriticalSection, LoadLibraryA, LoadLibraryExA, LoadResource, LockResource, MulDiv, MultiByteToWideChar, RaiseException, ReadFile, ResetEvent, RtlUnwind, SetConsoleCtrlHandler, SetEndOfFile, SetErrorMode, SetEvent, SetFilePointer, SetHandleCount, SetLastError, SetThreadLocale, SizeofResource, Sleep, TlsAlloc, TlsFree, TlsGetValue, TlsSetValue, UnhandledExceptionFilter, VirtualAlloc, VirtualFree, VirtualQuery, WaitForSingleObject, WideCharToMultiByte, WriteFile, lstrcpyA, lstrcpynA, lstrlenA
VERSION.DLL	GetFileVersionInfoA, GetFileVersionInfoSizeA, VerQueryValueA
COMCTL32.DLL	ImageList_Add, ImageList_BeginDrag, ImageList_Destroy, ImageList_DragEnter, ImageList_DragLeave, ImageList_DragMove, ImageList_DragShowNolock, ImageList_Draw, ImageList_DrawEx, ImageList_EndDrag, ImageList_GetBkColor, ImageList_GetDragImage, ImageList_GetIconSize, ImageList_GetImageCount, ImageList_Read, ImageList_Remove, ImageList_Replace, ImageList_SetBkColor, ImageList_SetIconSize, ImageList_Write, _TrackMouseEvent, ImageList_Create
COMDLG32.DLL	GetOpenFileNameA, GetSaveFileNameA
GDI32.DLL	BitBlt, CreateBitmap, CreateBrushIndirect, CreateCompatibleBitmap, CreateCompatibleDC, CreateDIBSection, CreateDIBitmap, CreateFontIndirectA, CreateHalftonePalette, CreatePalette, CreatePenIndirect, CreateSolidBrush, DeleteDC, DeleteObject, Ellipse, ExcludeClipRect, ExtTextOutA, GetBitmapBits, GetBrushOrgEx, GetClipBox, GetCurrentPositionEx, GetDCOrgEx, GetDIBColorTable, GetDIBits, GetDeviceCaps, GetObjectA, GetPaletteEntries, GetPixel, GetRgnBox, GetStockObject, GetSystemPaletteEntries, GetTextExtentPoint32A, GetTextMetricsA, GetWindowOrgEx, IntersectClipRect, LineTo, MaskBlt, MoveToEx, PatBlt, RealizePalette, RectVisible, Rectangle, RestoreDC, RoundRect, SaveDC, SelectClipRgn, SelectObject, SelectPalette, SetBkColor, SetBkMode, SetBrushOrgEx, SetDIBColorTable, SetPixel, SetROP2, SetStretchBltMode, SetTextColor, SetViewportOrgEx, SetWindowOrgEx, StretchBlt, UnrealizeObject
USER32.DLL	ActivateKeyboardLayout, AdjustWindowRectEx, BeginPaint, CallNextHookEx, CallWindowProcA, CharLowerA, CharNextA, CharToOemA, CheckDlgButton, CheckMenuItem, ClientToScreen, CreateIcon, CreateMenu, CreatePopupMenu, CreateWindowExA, DefFrameProcA, DefMDIChildProcA, DefWindowProcA, DeleteMenu, DestroyCursor, DestroyIcon, DestroyMenu, DestroyWindow, DispatchMessageA, DispatchMessageW, DrawEdge, DrawFocusRect, DrawFrameControl, DrawIcon, DrawIconEx, DrawMenuBar, DrawTextA, EnableMenuItem, EnableScrollBar, EnableWindow, EndPaint, EnumChildWindows, EnumThreadWindows, EnumWindows, EqualRect, FillRect, FindWindowA, FrameRect, GetActiveWindow, GetCapture, GetClassInfoA, GetClassLongA, GetClientRect, GetCursor, GetCursorPos, GetDC, GetDCEx, GetDesktopWindow, GetFocus, GetForegroundWindow, GetIconInfo, GetKeyNameTextA, GetKeyState, GetKeyboardLayout, GetKeyboardLayoutList, GetKeyboardLayoutNameA, GetKeyboardState, GetKeyboardType, GetLastActivePopup, GetMenu, GetMenuItemCount, GetMenuItemID, GetMenuItemInfoA, GetMenuState, GetMenuStringA, GetMessagePos, GetParent, GetPropA, GetScrollInfo, GetScrollPos, GetScrollRange, GetSubMenu, GetSysColor, GetSysColorBrush, GetSystemMenu, GetTopWindow, GetWindow, GetWindowDC, GetWindowLongA, GetWindowLongW, GetWindowPlacement, GetWindowRect, GetWindowTextA, GetWindowThreadProcessId, InflateRect, InsertMenuA, InsertMenuItemA, IntersectRect, InvalidateRect, IsChild, IsDialogMessageA, IsDialogMessageW, IsDlgButtonChecked, IsIconic, IsRectEmpty, IsWindow, IsWindowEnabled, IsWindowUnicode, IsWindowVisible, IsZoomed, KillTimer, LoadBitmapA, LoadCursorA, LoadIconA, LoadKeyboardLayoutA, LoadStringA, MapVirtualKeyA, MapWindowPoints, MessageBoxA, OemToCharA, OffsetRect, PeekMessageA, PeekMessageW, PostMessageA, PostQuitMessage, PtInRect, RedrawWindow, RegisterClassA, RegisterClipboardFormatA, RegisterWindowMessageA, ReleaseCapture, ReleaseDC, RemoveMenu, RemovePropA, ScreenToClient, ScrollWindow, SendMessageA, SendMessageW, SetActiveWindow, SetCapture, SetClassLongA, SetCursor, SetFocus, SetForegroundWindow, SetMenu, SetMenuItemInfoA, SetParent, SetPropA, SetRect, SetScrollInfo, SetScrollPos, SetScrollRange, SetTimer, SetWindowLongA, SetWindowLongW, SetWindowPlacement, SetWindowPos, SetWindowTextA, SetWindowsHookExA, ShowOwnedPopups, ShowScrollBar, ShowWindow, SystemParametersInfoA, TrackPopupMenu, TranslateMDISysAccel, TranslateMessage, UnhookWindowsHookEx, UnregisterClassA, UpdateWindow, WaitMessage, WindowFromPoint, wsprintfA, GetSystemMetrics
OLEAUT32.DLL	SafeArrayCreate, SafeArrayGetLBound, SafeArrayGetUBound, SafeArrayPtrOfIndex, SysAllocStringLen, SysFreeString, SysReAllocStringLen, VariantChangeType, VariantClear, VariantCopy, VariantInit

Exports

Name	Ordinal	Address
@xp28Vistaaltfixunit@TVistaAltFix	3	0x466b0c
@Vistaaltfixunit@Finalization$qqrv	8	0x466cb0
@Vistaaltfixunit@Register$qqrv	4	0x466b38
@Vistaaltfixunit@TVistaAltFix@	2	0x466ac8
@Vistaaltfixunit@TVistaAltFix@$bctr$qqrp18Classes@TComponent	5	0x466ba4
@Vistaaltfixunit@TVistaAltFix@$bdtr$qqrv	6	0x466c1c
@Vistaaltfixunit@TVistaAltFix@VistaWithTheme$qqrv	7	0x466c6c
@Vistaaltfixunit@initialization$qqrv	9	0x466ce0
_AddCEADataForm	11	0x4ef1a0
_AddDIDDataForm	12	0x4ef1a4
_AudioFormatForm	13	0x4ef1a8
_AudioFormatListForm	14	0x4ef1ac

Name	Ordinal	Address
_ColorimetryForm	15	0x4ef1b0
_CommonForm	16	0x4ef1b4
_DIDDetailedResolutionListForm	18	0x4ef20c
_DetailedResolutionForm	17	0x4ef208
_DisplayForm	19	0x4ef214
_ExtensionBlockForm	20	0x4ef254
_FreeSyncRangeForm	21	0x4f2714
_HDMI2SupportForm	24	0x4f2720
_HDMIResolutionForm	22	0x4f2718
_HDMISupportForm	23	0x4f271c
_HDRStaticMetadataForm	25	0x4f2724
_PropertiesForm	26	0x4f2728
_SpeakerSetupForm	27	0x4f272c
_StandardResolutionForm	28	0x4f2730
_TVResolutionForm	30	0x4f2738
_TVResolutionListForm	31	0x4f273c
_TiledDisplayTopologyForm	29	0x4f2734
_VideoCapabilityForm	32	0x4f2740
__GetExceptDLLinfo	1	0x4013e5
___CPPdebugHook	10	0x4c6098

Possible Origin

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

Network Behavior

Network Port Distribution

Total Packets: 12

- 53 (DNS)
- 8080 undefined

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 15:51:33.522084951 CEST	49702	8080	192.168.2.3	189.30.155.39
Oct 3, 2022 15:51:33.783726931 CEST	8080	49702	189.30.155.39	192.168.2.3
Oct 3, 2022 15:51:34.319655895 CEST	49702	8080	192.168.2.3	189.30.155.39
Oct 3, 2022 15:51:34.578561068 CEST	8080	49702	189.30.155.39	192.168.2.3
Oct 3, 2022 15:51:35.210315943 CEST	49702	8080	192.168.2.3	189.30.155.39

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 15:51:35.469022989 CEST	8080	49702	189.30.155.39	192.168.2.3
Oct 3, 2022 15:52:05.559123993 CEST	49703	8080	192.168.2.3	189.30.155.39
Oct 3, 2022 15:52:05.794964075 CEST	8080	49703	189.30.155.39	192.168.2.3
Oct 3, 2022 15:52:06.306580067 CEST	49703	8080	192.168.2.3	189.30.155.39
Oct 3, 2022 15:52:06.542495012 CEST	8080	49703	189.30.155.39	192.168.2.3
Oct 3, 2022 15:52:07.056663990 CEST	49703	8080	192.168.2.3	189.30.155.39
Oct 3, 2022 15:52:07.292512894 CEST	8080	49703	189.30.155.39	192.168.2.3
Oct 3, 2022 15:52:37.412137985 CEST	49704	8080	192.168.2.3	189.30.155.39
Oct 3, 2022 15:52:37.656075001 CEST	8080	49704	189.30.155.39	192.168.2.3
Oct 3, 2022 15:52:38.168632984 CEST	49704	8080	192.168.2.3	189.30.155.39
Oct 3, 2022 15:52:38.412554026 CEST	8080	49704	189.30.155.39	192.168.2.3
Oct 3, 2022 15:52:38.918927908 CEST	49704	8080	192.168.2.3	189.30.155.39
Oct 3, 2022 15:52:39.163156033 CEST	8080	49704	189.30.155.39	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 15:51:33.484947920 CEST	57840	53	192.168.2.3	8.8.8.8
Oct 3, 2022 15:51:33.507029057 CEST	53	57840	8.8.8.8	192.168.2.3
Oct 3, 2022 15:52:05.536159992 CEST	57990	53	192.168.2.3	8.8.8.8
Oct 3, 2022 15:52:05.556083918 CEST	53	57990	8.8.8.8	192.168.2.3
Oct 3, 2022 15:52:37.390862942 CEST	52387	53	192.168.2.3	8.8.8.8
Oct 3, 2022 15:52:37.410737038 CEST	53	52387	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Oct 3, 2022 15:51:33.484947920 CEST	192.168.2.3	8.8.8.8	0x7839	Standard query (0)	sherlock.servegame.com	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:52:05.536159992 CEST	192.168.2.3	8.8.8.8	0x74c3	Standard query (0)	sherlock.servegame.com	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:52:37.390862942 CEST	192.168.2.3	8.8.8.8	0x5f5e	Standard query (0)	sherlock.servegame.com	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Oct 3, 2022 15:51:33.507029057 CEST	8.8.8.8	192.168.2.3	0x7839	No error (0)	sherlock.servegame.com		189.30.155.39	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:52:05.556083918 CEST	8.8.8.8	192.168.2.3	0x74c3	No error (0)	sherlock.servegame.com		189.30.155.39	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:52:37.410737038 CEST	8.8.8.8	192.168.2.3	0x5f5e	No error (0)	sherlock.servegame.com		189.30.155.39	A (IP address)	IN (0x0001)	false

Statistics

No statistics

System Behavior

Analysis Process: empudh9lY5.exe PID: 2560, Parent PID: 3452

General

Target ID:	0

Start time:	15:50:47
Start date:	03/10/2022
Path:	C:\Users\user\Desktop\empudh9lY5.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\empudh9lY5.exe
Imagebase:	0x400000
File size:	1283072 bytes
MD5 hash:	8F43B86F351DB105A727E67E39459D78
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: CoreImpact_sysdll_exe, Description: Detects a malware sysdll.exe from the Rocket Kitten APT, Source: 00000000.00000002.516789881.0000000000570000.00000040.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: WoolenGoldfish_Generic_3, Description: Detects a operation Woolen-Goldfish sample - http://goo.gl/NpJpVZ, Source: 00000000.00000002.516789881.0000000000570000.00000040.00001000.00020000.00000000.sdmp, Author: Florian Roth
Reputation:	low

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly