ID: 753421
Sample Name: conhost.exe
Cookbook: default.jbs
Time: 19:48:36
Date: 24/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Copyright Joe Security LLC 2022

Disassembly 20

Copyright Joe Security LLC 2022

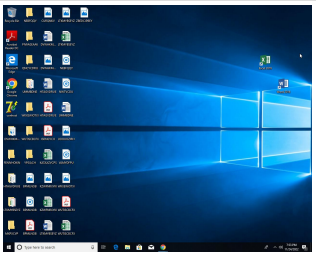
Windows Analysis Report

conhost.exe

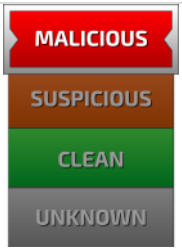
Overview

General Information

Sample Name:	conhost.exe
Analysis ID:	753421
MD5:	8c9dca7a1d21e4..
SHA1:	39cdfb61bf1a94d..
SHA256:	7cb6264b793849..
Infos:	



Detection



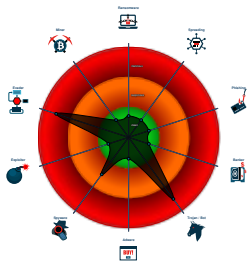
CryptOne, SystemBC

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

Signatures

- Multi AV Scanner detection for subm…
- Icon mismatch, binary includes an i…
- Malicious sample detected (through…
- Detected unpacking (overwrites its o…
- Yara detected CryptOne packer
- Yara detected SystemBC
- Detected unpacking (changes PE se…
- Found evasive API chain (may stop…
- Machine Learning detection for sam…
- C2 URLs / IPs found in malware con…
- Uses 32bit PE files
- Found decision node followed by no…

Classification



Process Tree

- **System is w10x64**
- conhost.exe (PID: 3648 cmdline: C:\Users\user\Desktop\conhost.exe MD5: 8C9DCA7A1D21E402C885D50AF18737D1)
- conhost.exe (PID: 3924 cmdline: C:\Users\user\Desktop\conhost.exe start MD5: 8C9DCA7A1D21E402C885D50AF18737D1)
- **cleanup**

Malware Configuration

Threatname: SystemBC


```
{
  "HOST1": "207.148.1.174",
  "HOST2": "146.70.53.169",
  "PORT1": "443",
  "TOR": ""
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.326977694.0000000000400000.00000040.00000001.01000000.00000003.sdmp	EXT_MAL_SystemBC_Mar22_1	Detects unpacked SystemBC module as used by Emotet in March 2022	Thomas Barabosch, Deutsche Telekom Security	• 0x516d:$sx1: -WindowStyle Hidden -ep bypass -file • 0x5000:$sx2: BEGINDATA • 0x51a9:$sx3: GET %s HTTP/1.0 • 0x51c4:$s5: User-Agent: • 0x5115:$s8: ALLUSERSPROFILE
00000001.00000002.326977694.0000000000400000.00000040.00000001.01000000.00000003.sdmp	JoeSecurity_SystemBC	Yara detected SystemBC	Joe Security	

Copyright Joe Security LLC 2022

Source	Rule	Description	Author	Strings
00000001.00000002.326977694.0000000000400000.00000040.00000001.01000000.00000003.sdmp	MALWARE_Win_EXEPWSH_DLAgent	Detects SystemBC	ditekSHen	• 0x5162:$pwsh: powershell • 0x51a9:$s1: GET %s HTTP/1 • 0x51c4:$s2: User-Agent: • 0x516d:$s3: -WindowStyle Hidden -ep bypass -file " • 0x519e:$s4: LdrLoadDll • 0x5000:$v1: BEGINDATA • 0x500a:$v2: HOST1: • 0x503c:$v2: HOST2: • 0x506e:$v3: PORT1: • 0x507a:$v4: TOR: • 0x5108:$v5: Fwow64 • 0x510f:$v6: start
00000001.00000002.327790803.0000000002B50000.00000040.00001000.00020000.00000000.sdmp	EXT_MAL_SystemBC_Mar22_1	Detects unpacked SystemBC module as used by Emotet in March 2022	Thomas Barabosch, Deutsche Telekom Security	• 0x32e1:$sx1: -WindowStyle Hidden -ep bypass -file • 0x3174:$sx2: BEGINDATA • 0x331d:$sx3: GET %s HTTP/1.0 • 0x3338:$s5: User-Agent: • 0x3289:$s8: ALLUSERSPROFILE
00000001.00000002.327790803.0000000002B50000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_SystemBC	Yara detected SystemBC	Joe Security	
Click to see the 7 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.conhost.exe.2b50174.2.raw.unpack	EXT_MAL_SystemBC_Mar22_1	Detects unpacked SystemBC module as used by Emotet in March 2022	Thomas Barabosch, Deutsche Telekom Security	• 0x316d:$sx1: -WindowStyle Hidden -ep bypass -file • 0x3000:$sx2: BEGINDATA • 0x31a9:$sx3: GET %s HTTP/1.0 • 0x31c4:$s5: User-Agent: • 0x3115:$s8: ALLUSERSPROFILE
1.2.conhost.exe.2b50174.2.raw.unpack	JoeSecurity_SystemBC	Yara detected SystemBC	Joe Security	
1.2.conhost.exe.2b50174.2.raw.unpack	MALWARE_Win_EXEPWSH_DLAgent	Detects SystemBC	ditekSHen	• 0x3162:$pwsh: powershell • 0x31a9:$s1: GET %s HTTP/1 • 0x31c4:$s2: User-Agent: • 0x316d:$s3: -WindowStyle Hidden -ep bypass -file " • 0x319e:$s4: LdrLoadDll • 0x3000:$v1: BEGINDATA • 0x300a:$v2: HOST1: • 0x303c:$v2: HOST2: • 0x306e:$v3: PORT1: • 0x307a:$v4: TOR: • 0x3108:$v5: Fwow64 • 0x310f:$v6: start
1.2.conhost.exe.400000.0.unpack	EXT_MAL_SystemBC_Mar22_1	Detects unpacked SystemBC module as used by Emotet in March 2022	Thomas Barabosch, Deutsche Telekom Security	• 0x316d:$sx1: -WindowStyle Hidden -ep bypass -file • 0x3000:$sx2: BEGINDATA • 0x31a9:$sx3: GET %s HTTP/1.0 • 0x31c4:$s5: User-Agent: • 0x3115:$s8: ALLUSERSPROFILE
1.2.conhost.exe.400000.0.unpack	JoeSecurity_SystemBC	Yara detected SystemBC	Joe Security	
Click to see the 7 entries				

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

Machine Learning detection for sample

Compliance

Detected unpacking (overwrites its own PE header)

Networking

C2 URLs / IPs found in malware configuration

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

Detected unpacking (overwrites its own PE header)

Detected unpacking (changes PE section rights)

Hooking and other Techniques for Hiding and Protection

Icon mismatch, binary includes an icon from a different legit application in order to fool users

Malware Analysis System Evasion

Found evasive API chain (may stop execution after checking mutex)

Stealing of Sensitive Information

Yara detected CryptOne packer

Yara detected SystemBC

Remote Access Functionality

Yara detected CryptOne packer

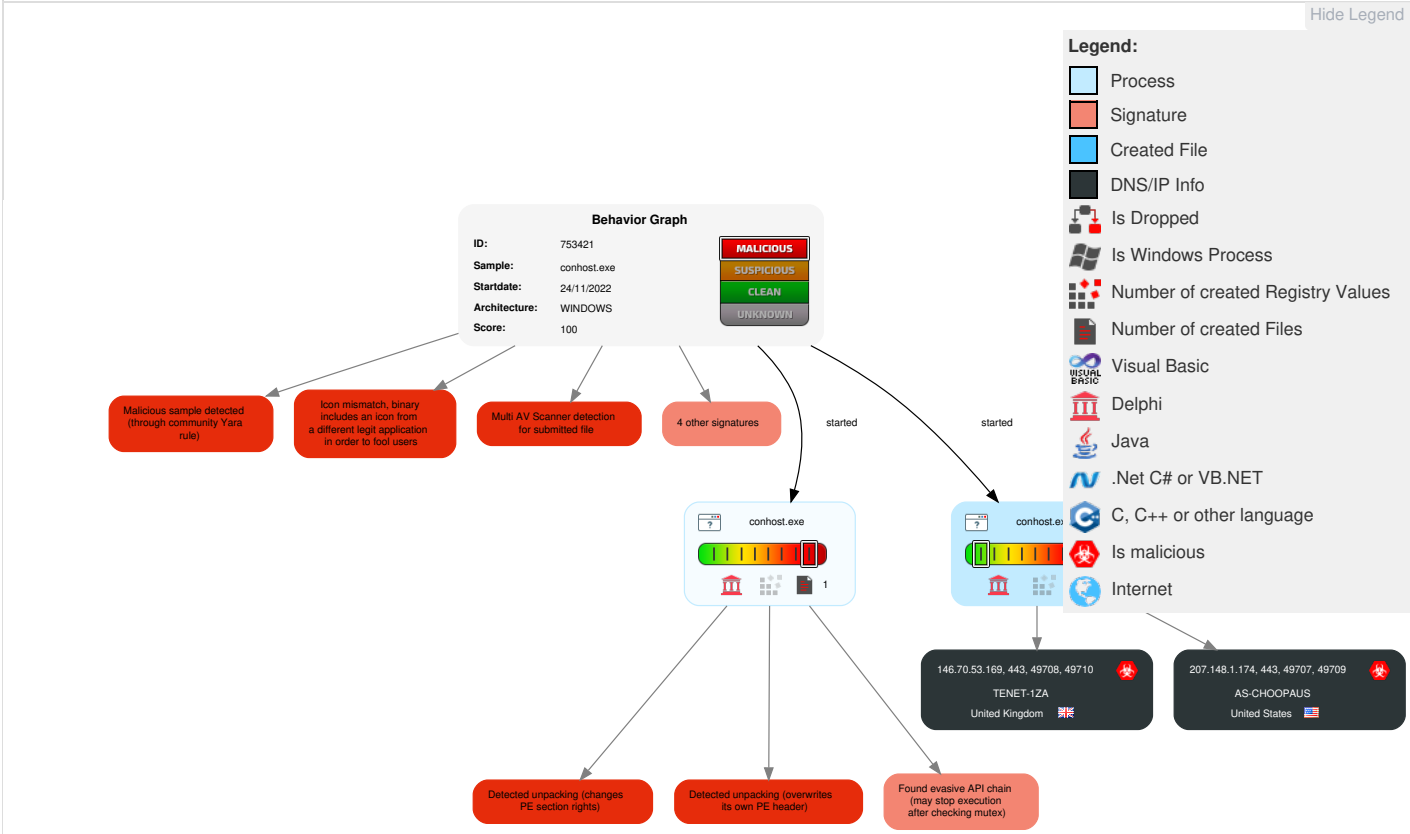
Yara detected SystemBC

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	1 Scheduled Task/Job	1 Scheduled Task/Job	1 Process Injection	1 1 Masquerading	OS Credential Dumping	1 System Time Discovery	Remote Services	1 Screen Capture	Exfiltration Over Other Network Medium	2 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 3 Native API	1 DLL Side-Loading	1 Scheduled Task/Job	1 Disable or Modify Tools	LSASS Memory	1 Security Software Discovery	Remote Desktop Protocol	1 Clipboard Data	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	1 DLL Side-Loading	1 1 Virtualization/Sandbox Evasion	Security Account Manager	1 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 1 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Obfuscated Files or Information	LSA Secrets	1 Account Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 1 Software Packing	Cached Domain Credentials	1 System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 DLL Side-Loading	DCSync	2 3 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

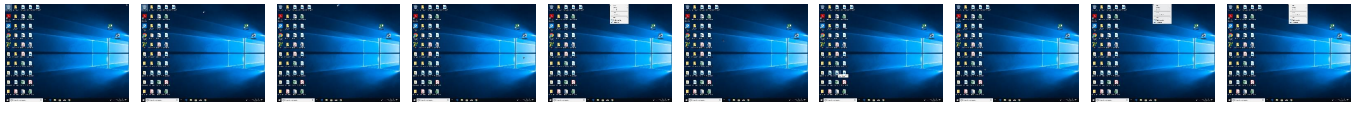
Behavior Graph

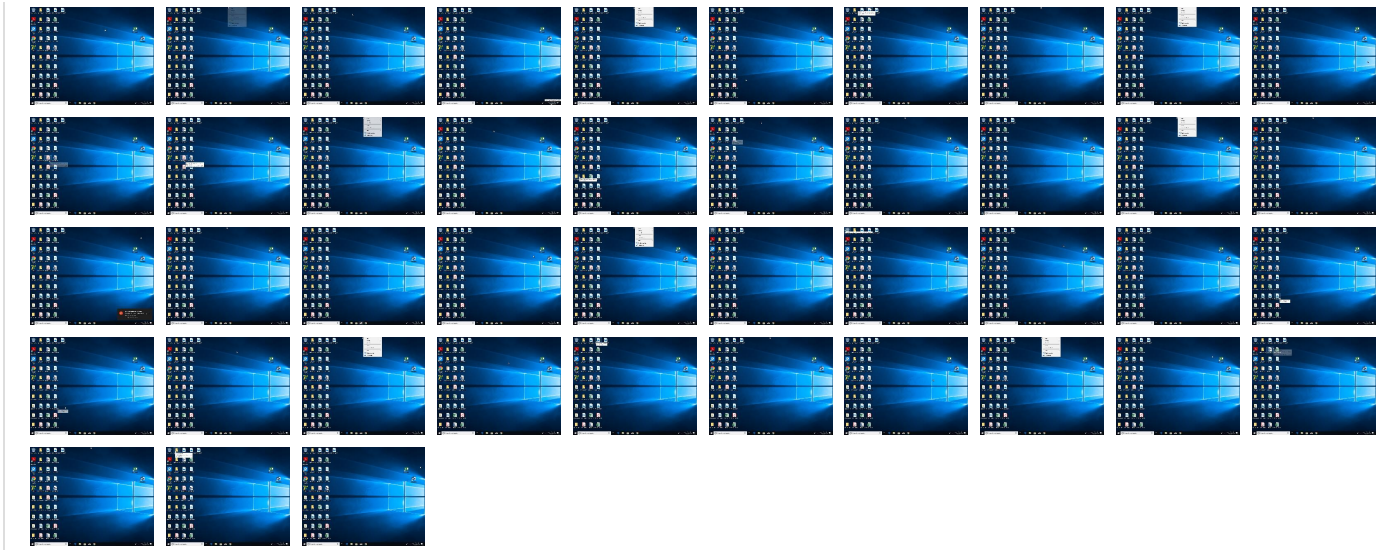


Screenshots

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
conhost.exe	22%	ReversingLabs	Win32.Trojan.Jaik	

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link
conhost.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.conhost.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1207314		Download File
1.2.conhost.exe.2990000.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.2.conhost.exe.2b50174.2.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.2.conhost.exe.2b60000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
146.70.53.169	0%	Avira URL Cloud	safe	
207.148.1.174	0%	Avira URL Cloud	safe	

Domains and IPs

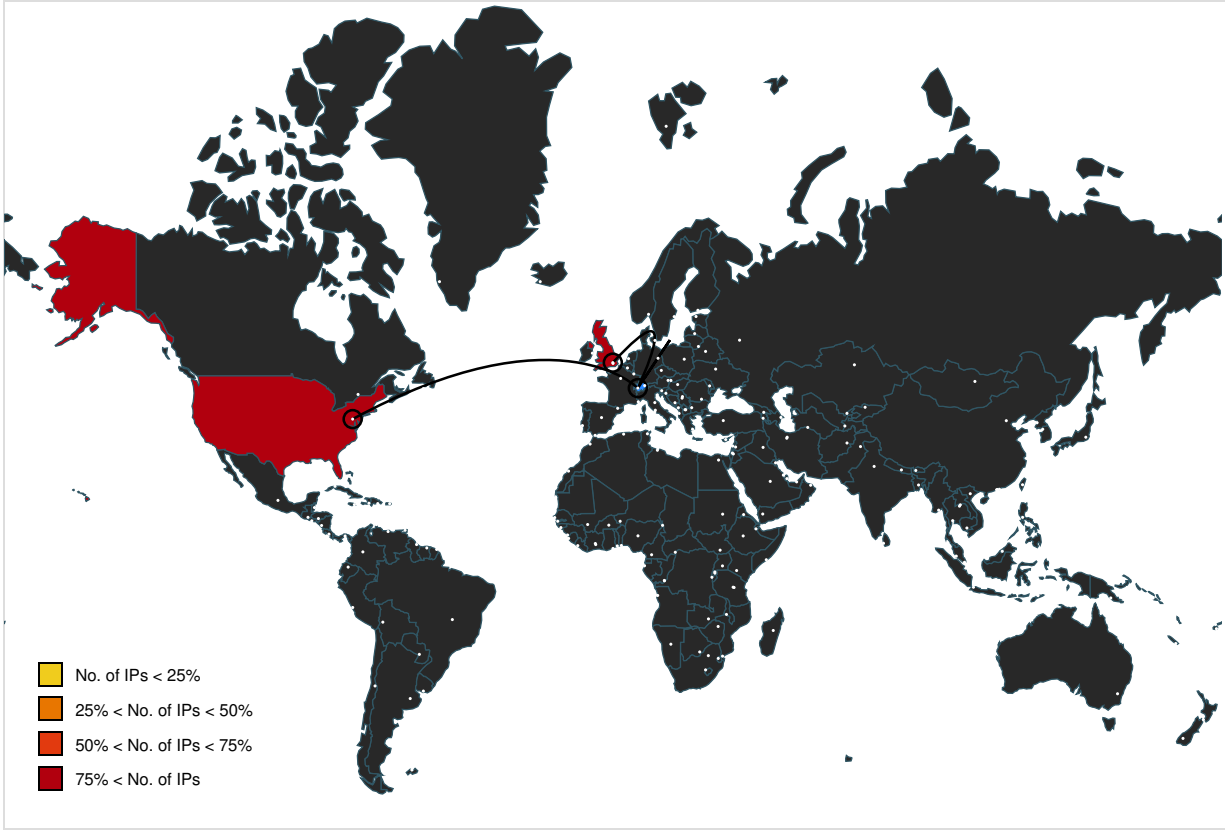
Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
207.148.1.174	true	• Avira URL Cloud: safe	unknown
146.70.53.169	true	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
207.148.1.174	unknown	United States		20473	AS-CHOOPAUS	true
146.70.53.169	unknown	United Kingdom		2018	TENET-1ZA	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	753421
Start date and time:	2022-11-24 19:48:36 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 39s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	conhost.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:	mal100.troj.evad.winEXE@2/1@0/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 3% (good quality ratio 2.9%) • Quality average: 78.6% • Quality standard deviation: 23.2%

Copyright Joe Security LLC 2022

HCA Information:	• Successful, ratio: 89% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Override analysis time to 240s for sample files taking high CPU consumption

Warnings

- Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information.
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): client.wns.windows.com
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing network information.
- Report size getting too big, too many NtDeviceIoControlFile calls found.
- VT rate limit hit for: conhost.exe

Simulations

Behavior and APIs

Time	Type	Description
19:49:44	API Interceptor	2x Sleep call for process: conhost.exe modified
19:49:45	Task Scheduler	Run new task: wow64 path: C:\Users\user\Desktop\conhost.exe s>start

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Windows\Tasks\wow64.job

Process:	C:\Users\user\Desktop\conhost.exe
File Type:	data
Category:	dropped
Size (bytes):	272
Entropy (8bit):	3.543933576684731
Encrypted:	false
SSDEEP:	6:P98jO/80e//5ZsFWr6AtoADCzcF/v5t/uy0lc3/a:ayS/EF4T+zcFaVua
MD5:	65B27BF9361F0023AC53DD93C125103A

SHA1:	2F81B65A3E7CDE6C03358BDFA460D64E456C8580
SHA-256:	B28AF9BA07C95BBCB7366E36C257D97D21AF06DB29123DBA1C2AA91B57AE8FDF
SHA-512:	23D0E6EBE279F920BD3ABC1449E6E81A5B1B78ADB4084A8D800D9E0E7D29BEA13B502559C5A802CFA6EA5508FEB60E4058259895584BFF7232F48E07797BEBB7
Malicious:	false
Reputation:	low
Preview:	....ba.yxF.A..dv%...F.....<... .....\....."....$.C.:.\.U.s.e.r.s.\.a.l.f.o.n.s.\.D.e.s.k.t.o.p.\.c.o.n.h.o.s.t...e.x.e.....s.t.a.r.t.....D.E.S.K.T.O.P.-.7.1.6.T.7.7.1.\.a.l.f.o.n.s.....0.....J.....3. .....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.129904154417161
TrID:	• Win32 Executable (generic) a (10002005/4) 91.23% • Win32 Executable Borland Delphi 7 (665061/41) 6.07% • Win32 Executable Borland Delphi 6 (262906/60) 2.40% • Win32 Executable Delphi generic (14689/80) 0.13% • Windows Screen Saver (13104/52) 0.12%
File name:	conhost.exe
File size:	1298944
MD5:	8c9dca7a1d21e402c885d50af18737d1
SHA1:	39cdfb61bf1a94d064a5ac5648ab552ca20be539
SHA256:	7cb6264b793849e31f23a7eb4f18f59a71fd3e44760be9d6052bbcdc2dfdf15c
SHA512:	2c2dda6e2a7323a587e932903943ce12db9bedb1b42ec0683e293d1d8883b57667652767ba8af8f79953d4a4719fd67eaee8ed277a887248e69b90d3729c1113
SSDEEP:	24576:iZcicBG2rYbrozA48eI193G7V3IVi4oIIXEJo7SFY8V7ygQay3VzcA8:ZiAEHxAJ4VWIB798V7FKVzc
TLSH:	6255BE22AEA208F6C0B6167D4CFB53D79827BD4129E4A5CE3BE41B884F356113B351B7
File Content Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7.....

File Icon

Icon Hash:	b99988fcd4f66e0f

Static PE Info

General

Entrypoint:	0x485e84
Entrypoint Section:	CODE
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, BYTES_REVERSED_LO, 32BIT_MACHINE, BYTES_REVERSED_HI
DLL Characteristics:	
Time Stamp:	0x2A425E19 [Fri Jun 19 22:22:17 1992 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:	3e0b4375409ad38c7e70ca98362a4d30

Entrypoint Preview

Instruction
push ebp

Instruction
mov ebp, esp
add esp, FFFFFFF0h
mov eax, 00485BF4h
call 00007F5CA85BA5DDh
xor eax, eax
push ebp
push 00485EF8h
push dword ptr fs:[eax]
mov dword ptr fs:[eax], esp
mov eax, dword ptr [00487A3Ch]
mov eax, dword ptr [eax]
call 00007F5CA86101D3h
mov ecx, dword ptr [00487C04h]
mov eax, dword ptr [00487A3Ch]
mov eax, dword ptr [eax]
mov edx, dword ptr [00485734h]
call 00007F5CA86101D3h
mov ecx, dword ptr [0048789Ch]
mov eax, dword ptr [00487A3Ch]
mov eax, dword ptr [eax]
mov edx, dword ptr [004603DCh]
call 00007F5CA86101BBh
mov eax, dword ptr [00487A3Ch]
mov eax, dword ptr [eax]
call 00007F5CA861022Fh
xor eax, eax
pop edx
pop ecx
pop ecx
mov dword ptr fs:[eax], edx
push 00485EFFh
ret
jmp 00007F5CA85B80E4h
jmp 00007F5CA863A68Ah
call 00007F5CA85B85E9h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Copyright Joe Security LLC 2022

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x89000	0x23ba	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x98000	0xa9a00	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x8e000	0x9e3c	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x8d000	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
CODE	0x1000	0x84f04	0x85000	False	0.5101547814849624	data	6.4987829224600135	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
DATA	0x86000	0x1c9c	0x1e00	False	0.4485677083333333	data	4.560359362872963	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
BSS	0x88000	0xe25	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.idata	0x89000	0x23ba	0x2400	False	0.3677300347222222	data	5.028417057566957	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.tls	0x8c000	0x10	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rdata	0x8d000	0x18	0x200	False	0.048828125	data	0.2005819074398449	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.reloc	0x8e000	0x9e3c	0xa000	False	0.5245849609375	data	6.5985698340803	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.rsrc	0x98000	0xa9a00	0xa9a00	False	0.7924693142041267	data	7.384724458379548	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_CURSOR	0x98dd4	0x134	data		
RT_CURSOR	0x98f08	0x134	data		
RT_CURSOR	0x9903c	0x134	data		
RT_CURSOR	0x99170	0x134	data		
RT_CURSOR	0x992a4	0x134	data		
RT_CURSOR	0x993d8	0x134	data		
RT_CURSOR	0x9950c	0x134	Targa image data - RGB 64 x 65536 x 1 +32 "\001"		
RT_CURSOR	0x99640	0x134	Targa image data - Map 64 x 65536 x 1 +32 "\001"		
RT_BITMAP	0x99774	0x1d0	Device independent bitmap graphic, 36 x 18 x 4, image size 360		
RT_BITMAP	0x99944	0x1e4	Device independent bitmap graphic, 36 x 19 x 4, image size 380		
RT_BITMAP	0x99b28	0x1d0	Device independent bitmap graphic, 36 x 18 x 4, image size 360		
RT_BITMAP	0x99cf8	0x1d0	Device independent bitmap graphic, 36 x 18 x 4, image size 360		
RT_BITMAP	0x99ec8	0x1d0	Device independent bitmap graphic, 36 x 18 x 4, image size 360		
RT_BITMAP	0x9a098	0x1d0	Device independent bitmap graphic, 36 x 18 x 4, image size 360		
RT_BITMAP	0x9a268	0x1d0	Device independent bitmap graphic, 36 x 18 x 4, image size 360		
RT_BITMAP	0x9a438	0x1d0	Device independent bitmap graphic, 36 x 18 x 4, image size 360		
RT_BITMAP	0x9a608	0x1d0	Device independent bitmap graphic, 36 x 18 x 4, image size 360		
RT_BITMAP	0x9a7d8	0x1d0	Device independent bitmap graphic, 36 x 18 x 4, image size 360		
RT_BITMAP	0x9a9a8	0xe8	Device independent bitmap graphic, 16 x 16 x 4, image size 128		
RT_ICON	0x9aa90	0x2e8	Device independent bitmap graphic, 32 x 64 x 4, image size 512	English	United States
RT_DIALOG	0x9ad78	0x52	data		
RT_STRING	0x9adcc	0x120	data		
RT_STRING	0x9aeec	0x108	data		
RT_STRING	0x9aff4	0x24c	data		
RT_STRING	0x9b240	0x4a4	data		
RT_STRING	0x9b6e4	0x378	data		
RT_STRING	0x9ba5c	0x3b8	data		
RT_STRING	0x9be14	0x308	data		
RT_STRING	0x9c11c	0x1cc	data		
RT_STRING	0x9c2e8	0x188	data		
RT_STRING	0x9c470	0x1b0	data		
RT_STRING	0x9c620	0x294	data		
RT_STRING	0x9c8b4	0xe0	data		
RT_STRING	0x9c994	0x194	data		
RT_STRING	0x9cb28	0x268	data		
RT_STRING	0x9cd90	0x3f8	data		
RT_STRING	0x9d188	0x384	data		
RT_STRING	0x9d50c	0x440	data		
RT_STRING	0x9d94c	0x160	data		
RT_STRING	0x9daac	0xec	data		
RT_STRING	0x9db98	0x20c	data		
RT_STRING	0x9dda4	0x3f4	data		
RT_STRING	0x9e198	0x340	data		
RT_STRING	0x9e4d8	0x2c4	data		
RT_RCDATA	0x9e79c	0x10	data		
RT_RCDATA	0x9e7ac	0x350	data		
RT_RCDATA	0x9eafc	0x13c	Delphi compiled form 'Tertw'		
RT_RCDATA	0x9ec38	0x1c1	Delphi compiled form 'TFastLineSeriesEditor'		
RT_RCDATA	0x9edfc	0x19d	Delphi compiled form 'TForm2'		
RT_RCDATA	0x9ef9c	0x58c	Delphi compiled form 'TPenDialog'		

Copyright Joe Security LLC 2022

Name	RVA	Size	Type	Language	Country
RT_RCDATA	0x9f528	0x19e	Delphi compiled form 'Ttjw458t724'		
RT_RCDATA	0x9f6c8	0xa2170	Applesoft BASIC program data, first line number 10	Chinese	Singapore
RT_GROUP_CURSOR	0x141838	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x14184c	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x141860	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x141874	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x141888	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x14189c	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x1418b0	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x1418c4	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_ICON	0x1418d8	0x14	data	English	United States

Imports

DLL	Import
kernel32.dll	DeleteCriticalSection, LeaveCriticalSection, EnterCriticalSection, InitializeCriticalSection, VirtualFree, VirtualAlloc, LocalFree, LocalAlloc, GetTickCount, QueryPerformanceCounter, GetVersion, GetCurrentThreadId, InterlockedDecrement, InterlockedIncrement, VirtualQuery, WideCharToMultiByte, MultiByteToWideChar, lstrlenA, lstrcpynA, LoadLibraryExA, GetThreadLocale, GetStartupInfoA, GetProcAddress, GetModuleHandleA, GetModuleFileNameA, GetLocaleInfoA, GetCommandLineA, FreeLibrary, FindFirstFileA, FindClose, ExitProcess, WriteFile, UnhandledExceptionFilter, RtlUnwind, RaiseException, GetStdHandle
user32.dll	GetKeyboardType, LoadStringA, MessageBoxA, CharNextA
advapi32.dll	RegQueryValueExA, RegOpenKeyExA, RegCloseKey
oleaut32.dll	SysFreeString, SysReAllocStringLen, SysAllocStringLen
kernel32.dll	TlsSetValue, TlsGetValue, LocalAlloc, GetModuleHandleA
advapi32.dll	RegQueryValueExA, RegOpenKeyExA, RegCloseKey
kernel32.dll	lstrcpyA, WriteFile, WaitForSingleObject, VirtualQuery, VirtualAlloc, Sleep, SizeofResource, SetThreadLocale, SetFilePointer, SetEvent, SetErrorMode, SetEndOfFile, ResetEvent, ReadFile, MulDiv, LockResource, LoadResource, LoadLibraryA, LeaveCriticalSection, InitializeCriticalSection, GlobalUnlock, GlobalReAlloc, GlobalHandle, GlobalLock, GlobalFree, GlobalFindAtomA, GlobalDeleteAtom, GlobalAlloc, GlobalAddAtomA, GetVersionExA, GetVersion, GetTickCount, GetThreadLocale, GetTempPathA, GetSystemInfo, GetStringTypeExA, GetStdHandle, GetProcAddress, GetModuleHandleA, GetModuleFileNameA, GetLocaleInfoA, GetLocalTime, GetLastError, GetFullPathNameA, GetFileSize, GetDiskFreeSpaceA, GetDateFormatA, GetCurrentThreadId, GetCurrentProcessId, GetCPInfo, GetACP, FreeResource, InterlockedExchange, FreeLibrary, FormatMessageA, FindResourceA, EnumCalendarInfoA, EnterCriticalSection, DeleteCriticalSection, CreateThread, CreateFileA, CreateEventA, CompareStringA, CloseHandle
version.dll	VerQueryValueA, GetFileVersionInfoSizeA, GetFileVersionInfoA
gdi32.dll	UpdateColors, UnrealizeObject, TextOutA, StretchBlt, SetWindowOrgEx, SetWinMetaFileBits, SetViewportOrgEx, SetTextColor, SetTextAlign, SetStretchBltMode, SetROP2, SetPixel, SetEnhMetaFileBits, SetDIBColorTable, SetBrushOrgEx, SetBkMode, SetBkColor, SelectPalette, SelectObject, SelectClipRgn, SaveDC, RoundRect, RestoreDC, Rectangle, RectVisible, RealizePalette, Polyline, Polygon, PlayEnhMetaFile, Pie, PathToRegion, PatBlt, MoveToEx, MaskBlt, LineTo, LPtoDP, IntersectClipRect, GetWindowOrgEx, GetWinMetaFileBits, GetTextMetricsA, GetTextExtentPoint32A, GetTextAlign, GetSystemPaletteEntries, GetStockObject, GetPixel, GetPaletteEntries, GetObjectA, GetEnhMetaFilePaletteEntries, GetEnhMetaFileHeader, GetEnhMetaFileBits, GetDeviceCaps, GetDIBits, GetDIBColorTable, GetDCOrgEx, GetCurrentPositionEx, GetClipBox, GetBrushOrgEx, GetBkMode, GetBkColor, GetBitmapBits, ExtSelectClipRgn, ExtCreatePen, ExcludeClipRect, Ellipse, DeleteObject, DeleteEnhMetaFile, DeleteDC, CreateSolidBrush, CreateRectRgn, CreatePolygonRgn, CreatePenIndirect, CreatePalette, CreateHalftonePalette, CreateFontIndirectA, CreateDIBitmap, CreateDIBSection, CreateCompatibleDC, CreateCompatibleBitmap, CreateBrushIndirect, CreateBitmap, CopyEnhMetaFileA, BitBlt, Arc

DLL	Import
user32.dll	CreateWindowExA, WindowFromPoint, WinHelpA, WaitMessage, UpdateWindow, UnregisterClassA, UnhookWindowsHookEx, TranslateMessage, TranslateMDISysAccel, TrackPopupMenu, SystemParametersInfoA, ShowWindow, ShowScrollBar, ShowOwnedPopups, ShowCursor, SetWindowsHookExA, SetWindowTextA, SetWindowPos, SetWindowPlacement, SetWindowLongA, SetTimer, SetScrollRange, SetScrollPos, SetScrollInfo, SetRect, SetPropA, SetParent, SetMenuItemInfoA, SetMenu, SetKeyboardState, SetForegroundWindow, SetFocus, SetCursor, SetClipboardData, SetClassLongA, SetCapture, SetActiveWindow, SendMessageA, ScrollWindow, ScreenToClient, RemovePropA, RemoveMenu, ReleaseDC, ReleaseCapture, RegisterWindowMessageA, RegisterClipboardFormatA, RegisterClassA, RedrawWindow, PtInRect, PostQuitMessage, PostMessageA, PeekMessageA, OpenClipboard, OffsetRect, OemToCharA, MessageBoxA, MessageBeep, MapWindowPoints, MapVirtualKeyA, LoadStringA, LoadKeyboardLayoutA, LoadIconA, LoadCursorA, LoadBitmapA, KillTimer, IsZoomed, IsWindowVisible, IsWindowEnabled, IsWindow, IsRectEmpty, IsIconic, IsDialogMessageA, IsChild, IsCharAlphaNumericA, IsCharAlphaA, InvalidateRect, IntersectRect, InsertMenuItemA, InsertMenuA, InflateRect, GetWindowThreadProcessId, GetWindowTextA, GetWindowRect, GetWindowPlacement, GetWindowLongA, GetWindowDC, GetTopWindow, GetSystemMetrics, GetSystemMenu, GetSysColorBrush, GetSysColor, GetSubMenu, GetScrollRange, GetScrollPos, GetScrollInfo, GetPropA, GetParent, GetWindow, GetMenuStringA, GetMenuState, GetMenuItemInfoA, GetMenuItemID, GetMenuItemCount, GetMenu, GetLastActivePopup, GetKeyboardState, GetKeyboardLayoutList, GetKeyboardLayout, GetKeyState, GetKeyNameTextA, GetIconInfo, GetForegroundWindow, GetFocus, GetDesktopWindow, GetDCEx, GetDC, GetCursorPos, GetCursor, GetClipboardData, GetClientRect, GetClassNameA, GetClassInfoA, GetCapture, GetActiveWindow, FrameRect, FindWindowA, FillRect, EqualRect, EnumWindows, EnumThreadWindows, EnumClipboardFormats, EndPaint, EndDeferWindowPos, EnableWindow, EnableScrollBar, EnableMenuItem, EmptyClipboard, DrawTextA, DrawMenuBar, DrawIconEx, DrawIcon, DrawFrameControl, DrawFocusRect, DrawEdge, DispatchMessageA, DestroyWindow, DestroyMenu, DestroyIcon, DestroyCursor, DeleteMenu, DeferWindowPos, DefWindowProcA, DefMDIChildProcA, DefFrameProcA, CreatePopupMenu, CreateMenu, CreateIcon, CloseClipboard, ClientToScreen, CheckMenuItem, CallWindowProcA, CallNextHookEx, BeginPaint, BeginDeferWindowPos, CharNextA, CharLowerBuffA, CharLowerA, CharUpperBuffA, CharToOemA, AdjustWindowRectEx, ActivateKeyboardLayout
kernel32.dll	Sleep
oleaut32.dll	SafeArrayPtrOfIndex, SafeArrayGetUBound, SafeArrayGetLBound, SafeArrayCreate, VariantChangeType, VariantCopy, VariantClear, VariantInit
comctl32.dll	ImageList_SetIconSize, ImageList_GetIconSize, ImageList_Write, ImageList_Read, ImageList_GetDragImage, ImageList_DragShowNolock, ImageList_SetDragCursorImage, ImageList_DragMove, ImageList_DragLeave, ImageList_DragEnter, ImageList_EndDrag, ImageList_BeginDrag, ImageList_Remove, ImageList_DrawEx, ImageList_Replace, ImageList_Draw, ImageList_GetBkColor, ImageList_SetBkColor, ImageList_ReplaceIcon, ImageList_Add, ImageList_GetImageCount, ImageList_Destroy, ImageList_Create, InitCommonControls
comdlg32.dll	ChooseColorA

Possible Origin

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

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 24, 2022 19:50:02.961976051 CET	49707	443	192.168.2.5	207.148.1.174
Nov 24, 2022 19:50:02.962052107 CET	443	49707	207.148.1.174	192.168.2.5
Nov 24, 2022 19:50:02.962168932 CET	49707	443	192.168.2.5	207.148.1.174
Nov 24, 2022 19:50:02.962764978 CET	49707	443	192.168.2.5	207.148.1.174
Nov 24, 2022 19:50:02.962804079 CET	443	49707	207.148.1.174	192.168.2.5
Nov 24, 2022 19:50:02.962963104 CET	443	49707	207.148.1.174	192.168.2.5
Nov 24, 2022 19:50:02.966327906 CET	49708	443	192.168.2.5	146.70.53.169
Nov 24, 2022 19:50:02.966392994 CET	443	49708	146.70.53.169	192.168.2.5
Nov 24, 2022 19:50:02.966487885 CET	49708	443	192.168.2.5	146.70.53.169
Nov 24, 2022 19:50:02.967125893 CET	49708	443	192.168.2.5	146.70.53.169
Nov 24, 2022 19:50:02.967170954 CET	443	49708	146.70.53.169	192.168.2.5
Nov 24, 2022 19:50:02.967272997 CET	443	49708	146.70.53.169	192.168.2.5
Nov 24, 2022 19:50:02.978005886 CET	49709	443	192.168.2.5	207.148.1.174
Nov 24, 2022 19:50:02.978058100 CET	443	49709	207.148.1.174	192.168.2.5

Copyright Joe Security LLC 2022

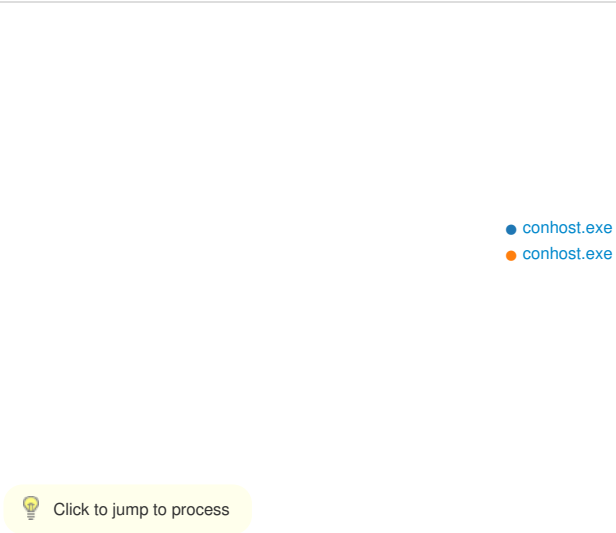
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 24, 2022 19:50:02.978164911 CET	49709	443	192.168.2.5	207.148.1.174
Nov 24, 2022 19:50:02.979168892 CET	49709	443	192.168.2.5	207.148.1.174
Nov 24, 2022 19:50:02.979211092 CET	443	49709	207.148.1.174	192.168.2.5
Nov 24, 2022 19:50:02.979314089 CET	443	49709	207.148.1.174	192.168.2.5
Nov 24, 2022 19:50:02.981857061 CET	49710	443	192.168.2.5	146.70.53.169
Nov 24, 2022 19:50:02.981947899 CET	443	49710	146.70.53.169	192.168.2.5
Nov 24, 2022 19:50:02.982079983 CET	49710	443	192.168.2.5	146.70.53.169
Nov 24, 2022 19:50:02.982795954 CET	49710	443	192.168.2.5	146.70.53.169
Nov 24, 2022 19:50:02.982824087 CET	443	49710	146.70.53.169	192.168.2.5
Nov 24, 2022 19:50:02.982914925 CET	443	49710	146.70.53.169	192.168.2.5
Nov 24, 2022 19:50:02.985480070 CET	49711	443	192.168.2.5	207.148.1.174
Nov 24, 2022 19:50:02.985522032 CET	443	49711	207.148.1.174	192.168.2.5
Nov 24, 2022 19:50:02.985615015 CET	49711	443	192.168.2.5	207.148.1.174
Nov 24, 2022 19:50:02.986449957 CET	49711	443	192.168.2.5	207.148.1.174
Nov 24, 2022 19:50:02.986473083 CET	443	49711	207.148.1.174	192.168.2.5
Nov 24, 2022 19:50:02.986538887 CET	443	49711	207.148.1.174	192.168.2.5
Nov 24, 2022 19:50:02.988950968 CET	49712	443	192.168.2.5	146.70.53.169
Nov 24, 2022 19:50:02.989012957 CET	443	49712	146.70.53.169	192.168.2.5
Nov 24, 2022 19:50:02.989126921 CET	49712	443	192.168.2.5	146.70.53.169
Nov 24, 2022 19:50:02.990008116 CET	49712	443	192.168.2.5	146.70.53.169
Nov 24, 2022 19:50:02.990039110 CET	443	49712	146.70.53.169	192.168.2.5
Nov 24, 2022 19:50:02.990103006 CET	443	49712	146.70.53.169	192.168.2.5
Nov 24, 2022 19:50:02.992351055 CET	49713	443	192.168.2.5	207.148.1.174
Nov 24, 2022 19:50:02.992383957 CET	443	49713	207.148.1.174	192.168.2.5
Nov 24, 2022 19:50:02.992503881 CET	49713	443	192.168.2.5	207.148.1.174
Nov 24, 2022 19:50:02.993408918 CET	49713	443	192.168.2.5	207.148.1.174
Nov 24, 2022 19:50:02.993511915 CET	443	49713	207.148.1.174	192.168.2.5
Nov 24, 2022 19:50:02.993587971 CET	443	49713	207.148.1.174	192.168.2.5
Nov 24, 2022 19:50:02.995920897 CET	49714	443	192.168.2.5	146.70.53.169
Nov 24, 2022 19:50:02.996090889 CET	443	49714	146.70.53.169	192.168.2.5
Nov 24, 2022 19:50:02.996212959 CET	49714	443	192.168.2.5	146.70.53.169
Nov 24, 2022 19:50:02.996932983 CET	49714	443	192.168.2.5	146.70.53.169
Nov 24, 2022 19:50:02.996980906 CET	443	49714	146.70.53.169	192.168.2.5
Nov 24, 2022 19:50:02.997037888 CET	443	49714	146.70.53.169	192.168.2.5
Nov 24, 2022 19:50:03.021893978 CET	49715	443	192.168.2.5	207.148.1.174
Nov 24, 2022 19:50:03.021946907 CET	443	49715	207.148.1.174	192.168.2.5
Nov 24, 2022 19:50:03.022036076 CET	49715	443	192.168.2.5	207.148.1.174
Nov 24, 2022 19:50:03.022720098 CET	49715	443	192.168.2.5	207.148.1.174
Nov 24, 2022 19:50:03.022743940 CET	443	49715	207.148.1.174	192.168.2.5
Nov 24, 2022 19:50:03.022811890 CET	443	49715	207.148.1.174	192.168.2.5
Nov 24, 2022 19:50:03.028750896 CET	49716	443	192.168.2.5	146.70.53.169
Nov 24, 2022 19:50:03.028884888 CET	443	49716	146.70.53.169	192.168.2.5
Nov 24, 2022 19:50:03.029043913 CET	49716	443	192.168.2.5	146.70.53.169
Nov 24, 2022 19:50:03.029613972 CET	49716	443	192.168.2.5	146.70.53.169
Nov 24, 2022 19:50:03.029663086 CET	443	49716	146.70.53.169	192.168.2.5
Nov 24, 2022 19:50:03.029936075 CET	443	49716	146.70.53.169	192.168.2.5
Nov 24, 2022 19:50:03.041013002 CET	49717	443	192.168.2.5	207.148.1.174
Nov 24, 2022 19:50:03.041071892 CET	443	49717	207.148.1.174	192.168.2.5
Nov 24, 2022 19:50:03.041174889 CET	49717	443	192.168.2.5	207.148.1.174
Nov 24, 2022 19:50:03.041975975 CET	49717	443	192.168.2.5	207.148.1.174
Nov 24, 2022 19:50:03.042011976 CET	443	49717	207.148.1.174	192.168.2.5
Nov 24, 2022 19:50:03.042103052 CET	443	49717	207.148.1.174	192.168.2.5
Nov 24, 2022 19:50:03.044338942 CET	49718	443	192.168.2.5	146.70.53.169
Nov 24, 2022 19:50:03.044399023 CET	443	49718	146.70.53.169	192.168.2.5
Nov 24, 2022 19:50:03.044487000 CET	49718	443	192.168.2.5	146.70.53.169
Nov 24, 2022 19:50:03.045294046 CET	49718	443	192.168.2.5	146.70.53.169
Nov 24, 2022 19:50:03.045329094 CET	443	49718	146.70.53.169	192.168.2.5
Nov 24, 2022 19:50:03.045397043 CET	443	49718	146.70.53.169	192.168.2.5
Nov 24, 2022 19:50:03.048052073 CET	49719	443	192.168.2.5	207.148.1.174

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 24, 2022 19:50:03.048099041 CET	443	49719	207.148.1.174	192.168.2.5
Nov 24, 2022 19:50:03.048167944 CET	49719	443	192.168.2.5	207.148.1.174
Nov 24, 2022 19:50:03.048870087 CET	49719	443	192.168.2.5	207.148.1.174
Nov 24, 2022 19:50:03.048897028 CET	443	49719	207.148.1.174	192.168.2.5
Nov 24, 2022 19:50:03.048978090 CET	443	49719	207.148.1.174	192.168.2.5
Nov 24, 2022 19:50:03.051232100 CET	49720	443	192.168.2.5	146.70.53.169
Nov 24, 2022 19:50:03.051275015 CET	443	49720	146.70.53.169	192.168.2.5
Nov 24, 2022 19:50:03.051358938 CET	49720	443	192.168.2.5	146.70.53.169
Nov 24, 2022 19:50:03.052207947 CET	49720	443	192.168.2.5	146.70.53.169
Nov 24, 2022 19:50:03.052238941 CET	443	49720	146.70.53.169	192.168.2.5
Nov 24, 2022 19:50:03.052314997 CET	443	49720	146.70.53.169	192.168.2.5
Nov 24, 2022 19:50:03.054652929 CET	49721	443	192.168.2.5	207.148.1.174
Nov 24, 2022 19:50:03.054692984 CET	443	49721	207.148.1.174	192.168.2.5
Nov 24, 2022 19:50:03.054763079 CET	49721	443	192.168.2.5	207.148.1.174
Nov 24, 2022 19:50:03.055377960 CET	49721	443	192.168.2.5	207.148.1.174
Nov 24, 2022 19:50:03.055403948 CET	443	49721	207.148.1.174	192.168.2.5
Nov 24, 2022 19:50:03.055486917 CET	443	49721	207.148.1.174	192.168.2.5
Nov 24, 2022 19:50:03.058118105 CET	49722	443	192.168.2.5	146.70.53.169
Nov 24, 2022 19:50:03.058168888 CET	443	49722	146.70.53.169	192.168.2.5
Nov 24, 2022 19:50:03.058238983 CET	49722	443	192.168.2.5	146.70.53.169
Nov 24, 2022 19:50:03.059057951 CET	49722	443	192.168.2.5	146.70.53.169
Nov 24, 2022 19:50:03.059101105 CET	443	49722	146.70.53.169	192.168.2.5
Nov 24, 2022 19:50:03.059151888 CET	443	49722	146.70.53.169	192.168.2.5
Nov 24, 2022 19:50:03.061359882 CET	49723	443	192.168.2.5	207.148.1.174
Nov 24, 2022 19:50:03.061400890 CET	443	49723	207.148.1.174	192.168.2.5
Nov 24, 2022 19:50:03.061475992 CET	49723	443	192.168.2.5	207.148.1.174
Nov 24, 2022 19:50:03.062216043 CET	49723	443	192.168.2.5	207.148.1.174

Statistics

Behavior



System Behavior

Analysis Process: conhost.exe PID: **3648**, Parent PID: **3324**

General

Target ID:	1

Start time:	19:49:24
Start date:	24/11/2022
Path:	C:\Users\user\Desktop\conhost.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\conhost.exe
Imagebase:	0x400000
File size:	1298944 bytes
MD5 hash:	8C9DCA7A1D21E402C885D50AF18737D1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: EXT_MAL_SystemBC_Mar22_1, Description: Detects unpacked SystemBC module as used by Emotet in March 2022, Source: 00000001.00000002.326977694.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: Thomas Barabosch, Deutsche Telekom Security • Rule: JoeSecurity_SystemBC, Description: Yara detected SystemBC, Source: 00000001.00000002.326977694.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: MALWARE_Win_EXEPWSH_DLAgent, Description: Detects SystemBC, Source: 00000001.00000002.326977694.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: ditekSHen • Rule: EXT_MAL_SystemBC_Mar22_1, Description: Detects unpacked SystemBC module as used by Emotet in March 2022, Source: 00000001.00000002.327790803.0000000002B50000.00000040.00001000.00020000.00000000.sdmp, Author: Thomas Barabosch, Deutsche Telekom Security • Rule: JoeSecurity_SystemBC, Description: Yara detected SystemBC, Source: 00000001.00000002.327790803.0000000002B50000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Crypt, Description: Yara detected CryptOne packer, Source: 00000001.00000002.327790803.0000000002B50000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: EXT_MAL_SystemBC_Mar22_1, Description: Detects unpacked SystemBC module as used by Emotet in March 2022, Source: 00000001.00000002.327897370.0000000002B60000.00000040.00001000.00020000.00000000.sdmp, Author: Thomas Barabosch, Deutsche Telekom Security • Rule: JoeSecurity_SystemBC, Description: Yara detected SystemBC, Source: 00000001.00000002.327897370.0000000002B60000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_EXEPWSH_DLAgent, Description: Detects SystemBC, Source: 00000001.00000002.327897370.0000000002B60000.00000040.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_Crypt, Description: Yara detected CryptOne packer, Source: 00000001.00000002.327382635.00000000028E0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **3924**, Parent PID: **1084**

General

Target ID:	8
Start time:	19:49:44
Start date:	24/11/2022
Path:	C:\Users\user\Desktop\conhost.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\conhost.exe start
Imagebase:	0x400000
File size:	1298944 bytes
MD5 hash:	8C9DCA7A1D21E402C885D50AF18737D1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Reputation:	low

Disassembly

No disassembly