ID: 384277
Sample Name: factura.exe
Cookbook: default.jbs
Time: 20:35:18
Date: 08/04/2021
Version: 31.0.0 Emerald

Table of Contents

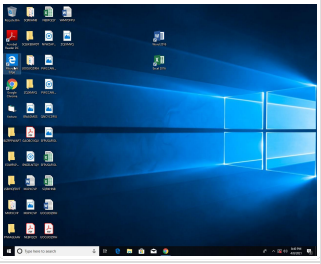
Analysis Report factura.exe

Overview

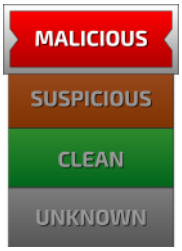
General Information

Sample Name:	factura.exe
Analysis ID:	384277
MD5:	5950cbe94b3b5d..
SHA1:	797bb1231483bb..
SHA256:	73f2aa87dad0670.
Infos:	

Most interesting Screenshot:



Detection

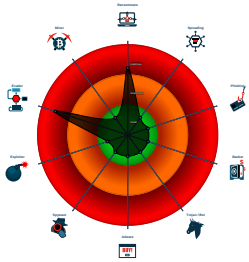


Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Potential malicious icon found
- Detected RDTSC dummy instruction…
- Found potential dummy code loops (…
- Hides threads from debuggers
- Tries to detect Any.run
- Tries to detect virtualization through…
- Abnormal high CPU Usage
- Checks if the current process is bein…
- Detected potential crypto function
- May sleep (evasive loops) to hinder …
- PE file contains strange resources
- Program does not show much activi…

Classification



Startup

- **System is w10x64**
- factura.exe (PID: 5932 cmdline: 'C:\Users\user\Desktop\factura.exe' MD5: 5950CBE94B3B5DEDBF7B75FA1B95AC84)
  - RegAsm.exe (PID: 4404 cmdline: 'C:\Users\user\Desktop\factura.exe' MD5: 529695608EAFBED00ACA9E61EF333A7C)
  - RegAsm.exe (PID: 5344 cmdline: 'C:\Users\user\Desktop\factura.exe' MD5: 529695608EAFBED00ACA9E61EF333A7C)
    - conhost.exe (PID: 68 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

No configs have been found

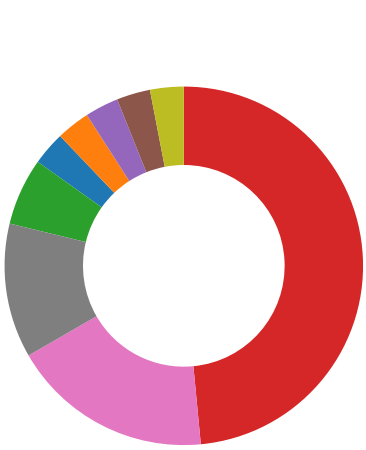
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

System Summary:

Potential malicious icon found

Malware Analysis System Evasion:

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

Tries to detect Any.run

Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

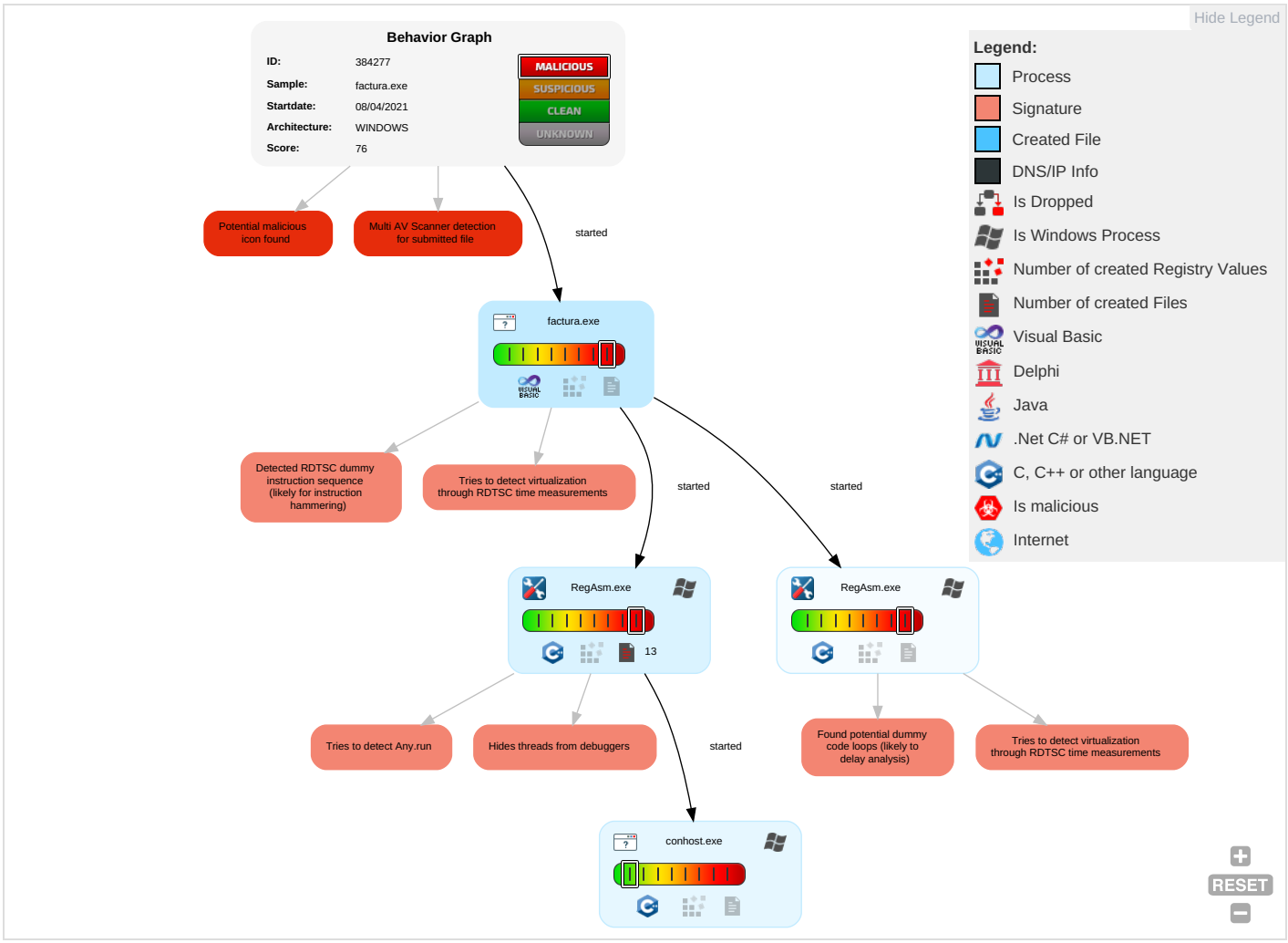
Found potential dummy code loops (likely to delay analysis)

Hides threads from debuggers

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Re Se Ef
Valid Accounts	Windows Management Instrumentation	DLL Side-Loading 1	Process Injection 2	Virtualization/Sandbox Evasion 3 2 1	OS Credential Dumping	Security Software Discovery 5 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Re Tr W Au
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Process Injection 2	LSASS Memory	Virtualization/Sandbox Evasion 3 2 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 to Redirect Phone Calls/SMS	Re W W Au
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	DLL Side-Loading 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Ol De Cl Ba
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	System Information Discovery 2 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	

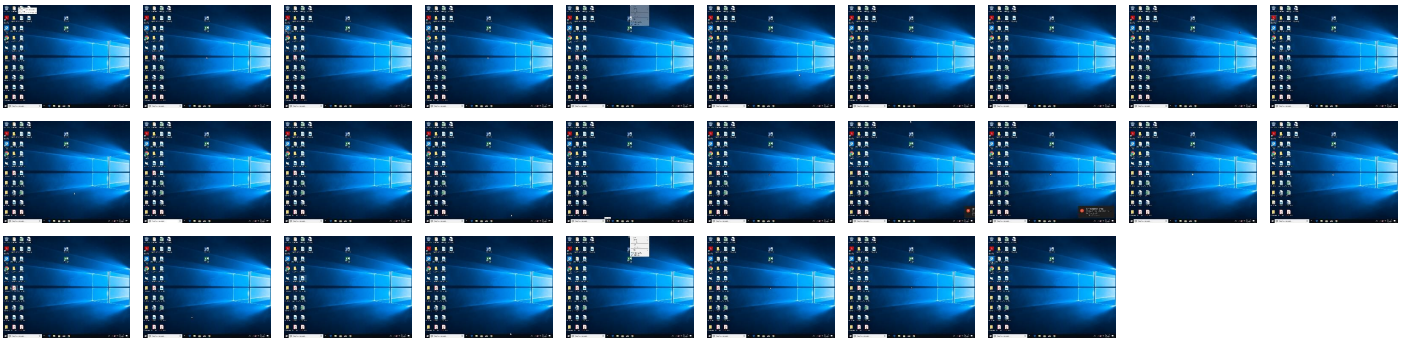
Behavior Graph



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
factura.exe	30%	Metadefender		Browse
factura.exe	46%	ReversingLabs	Win32.Trojan.GuLoader	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	384277
Start date:	08.04.2021
Start time:	20:35:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 36s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	factura.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	31
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:	mal76.rans.evad.winEXE@4/0@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 95.3% (good quality ratio 66.4%) • Quality average: 41.3% • Quality standard deviation: 34.2%
HCA Information:	• Successful, ratio: 58% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe • Override analysis time to 240s for sample files taking high CPU consumption

Warnings:	Show All • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 104.42.151.234, 13.64.90.137, 23.54.113.53, 40.88.32.150, 168.61.161.212, 104.43.139.144, 95.100.54.203, 205.185.216.10, 205.185.216.42, 20.50.102.62, 23.10.249.26, 23.10.249.43, 52.155.217.156, 20.54.26.129, 172.217.168.14 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, arc.trafficmanager.net, drive.google.com, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, consumerrp-displaycatalog-aks2eap.md.mp.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, cds.d2s7q6s2.hwcdn.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/384277/sample/factura.exe

Simulations

Behavior and APIs

Time	Type	Description
20:38:30	API Interceptor	350x Sleep call for process: RegAsm.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.437166061311082
TrID:	• Win32 Executable (generic) a (10002005/4) 99.15% • Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	factura.exe
File size:	57344
MD5:	5950cbe94b3b5dedbf7b75fa1b95ac84
SHA1:	797bb1231483bb11279f6e63fbb5d675bda58f2a
SHA256:	73f2aa87dad06704e8bbd41fb7449a987dc089160a12ba5e13d7d7f6f4196a4f
SHA512:	6e1f38b5f3d257a2d7926213a4ec6947882b6f38bbac8f42e9d0b3a92762494eeec21920e9ef6cf8440e7298aa2fe1eb73c51ce1c8ec1bc4abae14b2d32b1811
SSDEEP:	768:1hk5+yYZnkRUpyncqBRccge9kk1nA36yY1SoqOiiy:1a5+yk/AnbBTbkmA33RoqOe
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#...B...B...B..L^...B...`...B...d...B..Rich.B.....PE..L....-I`.....0.....@.....

File Icon

Icon Hash:	20047c7c70f0e004

Static PE Info

General

Entrypoint:	0x40169c
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui

General

Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x606C2D85 [Tue Apr 6 09:44:37 2021 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:	b983fc96c0bd34be8388eeea33042759

Entrypoint Preview

Instruction
push 0040192Ch
call 00007FE76CA428C5h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
xor byte ptr [eax], al
add byte ptr [eax], al
inc eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [esi], bl
mov word ptr [edi], cs
mov eax, 4C003ABAh
lahf
js 00007FE76CA42868h
push es
stosd
or dh, byte ptr [ecx]
add dword ptr [eax], 00000000h
add byte ptr [ecx], al
add byte ptr [eax], al
add byte ptr [ecx+00h], al
xchg byte ptr [eax-7Eh], dl
add dword ptr [ebx+4Bh], edx
inc ebp
dec ebp
inc ecx
inc esi
dec edi
push edx
dec ebp
inc ebp
push edx
add byte ptr [ecx+ebp+00000312h], al
add byte ptr [eax], al
dec esp
xor dword ptr [eax], eax
add eax, 02836AD0h
fmul qword ptr [ecx-66h]
dec edi
cdq
mov seg?, word ptr [esi]
call far B4BBh : 29F2388Ch
mov al, E7h
in al, 5Eh
dec esp
cdq

Instruction
xchg eax, ebx
push ebx
push eax
fcmovu st(0), st(6)
jp 00007FE76CA42887h
cmp cl, byte ptr [edi-53h]
xor ebx, dword ptr [ecx-48EE309Ah]
or al, 00h
stosb
add byte ptr [eax-2Dh], ah
xchg eax, ebx
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 dword ptr [eax], eax
add byte ptr [ebx+00h], cl
add byte ptr [eax], al
add byte ptr [ecx], cl
add byte ptr [ecx+ebp*2+73h], al
insd
imul ebp, dword ptr [esi+69h], 0D006E6Fh
add dword ptr [edx], ecx
add byte ptr [eax+61h], dh
imul esi, dword ptr [edx+70h], 00000069h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xada4	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xe000	0x9f0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x228	0x20	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x1ac	.text
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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xa3b8	0xb000	False	0.535866477273	data	6.30476552767	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0xc000	0x11b4	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0xe000	0x9f0	0x1000	False	0.181884765625	data	2.17356537605	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xe8c0	0x130	data		
RT_ICON	0xe5d8	0x2e8	data		
RT_ICON	0xe4b0	0x128	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0xe480	0x30	data		
RT_VERSION	0xe150	0x330	data	English	United States

Imports

DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaVarMove, __vbaHresultCheck, __vbaAryMove, __vbaFreeVar, __vbaStrVarMove, __vbaFreeVarList, __vbaEnd, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaHresultCheckObj, _adj_fdiv_m32, __vbaAryDestruct, __vbaOnError, __vbaObjSet, _adj_fdiv_m16i, __vbaObjSetAddref, _adj_fdivr_m16i, __vbaVarTstLt, __vbaFpR8, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, __vbaStrCmp, __vbaObjVar, _adj_fpatan, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, _adj_fprem, _adj_fdivr_m64, __vbaVarErrI4, __vbaI2Str, __vbaFPException, __vbaStrVarVal, __vbaDateVar, _CIlog, __vbaErrorOverflow, __vbaFileOpen, __vbaVar2Vec, __vbaNew2, __vbaInStr, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaI4Str, __vbaFreeStrList, _adj_fdivr_m32, _adj_fdiv_r, __vbaVarTstNe, __vbaVarAdd, __vbaLateMemCall, __vbaInStrB, __vbaVarDup, __vbaFpI4, __vbaLateMemCallLd, _CIatan, __vbaStrMove, __vbaCastObj, _allmul, _CItan, _CIexp, __vbaFreeStr, __vbaFreeObj

Version Infos

Description	Data
Translation	0x0409 0x04b0
LegalCopyright	Collutions
InternalName	kvalifikationen
FileVersion	1.00
CompanyName	Collutions
LegalTrademarks	Collutions
Comments	Collutions
ProductName	Collutions
ProductVersion	1.00
FileDescription	Creepy Collutions
OriginalFilename	kvalifikationen.exe

Possible Origin

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

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 20:35:58.124605894 CEST	57820	53	192.168.2.7	8.8.8.8
Apr 8, 2021 20:35:58.138807058 CEST	53	57820	8.8.8.8	192.168.2.7
Apr 8, 2021 20:35:59.861176014 CEST	50848	53	192.168.2.7	8.8.8.8
Apr 8, 2021 20:35:59.874805927 CEST	53	50848	8.8.8.8	192.168.2.7
Apr 8, 2021 20:36:00.442557096 CEST	61242	53	192.168.2.7	8.8.8.8

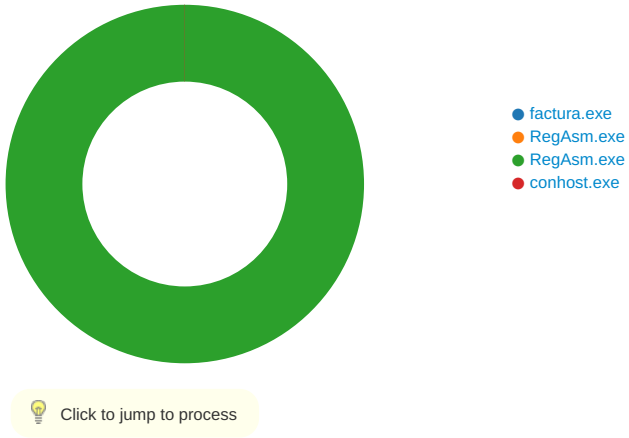
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 20:36:00.462649107 CEST	53	61242	8.8.8.8	192.168.2.7
Apr 8, 2021 20:36:01.041596889 CEST	58562	53	192.168.2.7	8.8.8.8
Apr 8, 2021 20:36:01.054368973 CEST	53	58562	8.8.8.8	192.168.2.7
Apr 8, 2021 20:36:02.216945887 CEST	56590	53	192.168.2.7	8.8.8.8
Apr 8, 2021 20:36:02.229949951 CEST	53	56590	8.8.8.8	192.168.2.7
Apr 8, 2021 20:36:03.330651999 CEST	60501	53	192.168.2.7	8.8.8.8
Apr 8, 2021 20:36:03.343095064 CEST	53	60501	8.8.8.8	192.168.2.7
Apr 8, 2021 20:36:04.365504026 CEST	53775	53	192.168.2.7	8.8.8.8
Apr 8, 2021 20:36:04.379268885 CEST	53	53775	8.8.8.8	192.168.2.7
Apr 8, 2021 20:36:05.174426079 CEST	51837	53	192.168.2.7	8.8.8.8
Apr 8, 2021 20:36:05.187256098 CEST	53	51837	8.8.8.8	192.168.2.7
Apr 8, 2021 20:36:06.344958067 CEST	55411	53	192.168.2.7	8.8.8.8
Apr 8, 2021 20:36:06.358233929 CEST	53	55411	8.8.8.8	192.168.2.7
Apr 8, 2021 20:36:07.345694065 CEST	63668	53	192.168.2.7	8.8.8.8
Apr 8, 2021 20:36:07.357342005 CEST	53	63668	8.8.8.8	192.168.2.7
Apr 8, 2021 20:36:09.270503998 CEST	54640	53	192.168.2.7	8.8.8.8
Apr 8, 2021 20:36:09.283051968 CEST	53	54640	8.8.8.8	192.168.2.7
Apr 8, 2021 20:36:10.129003048 CEST	58739	53	192.168.2.7	8.8.8.8
Apr 8, 2021 20:36:10.143260956 CEST	53	58739	8.8.8.8	192.168.2.7
Apr 8, 2021 20:36:11.852381945 CEST	60338	53	192.168.2.7	8.8.8.8
Apr 8, 2021 20:36:11.865338087 CEST	53	60338	8.8.8.8	192.168.2.7
Apr 8, 2021 20:36:12.845262051 CEST	58717	53	192.168.2.7	8.8.8.8
Apr 8, 2021 20:36:12.857690096 CEST	53	58717	8.8.8.8	192.168.2.7
Apr 8, 2021 20:36:13.845660925 CEST	59762	53	192.168.2.7	8.8.8.8
Apr 8, 2021 20:36:13.860131979 CEST	53	59762	8.8.8.8	192.168.2.7
Apr 8, 2021 20:36:14.864547968 CEST	54329	53	192.168.2.7	8.8.8.8
Apr 8, 2021 20:36:14.878345966 CEST	53	54329	8.8.8.8	192.168.2.7
Apr 8, 2021 20:36:18.225589991 CEST	58052	53	192.168.2.7	8.8.8.8
Apr 8, 2021 20:36:18.238105059 CEST	53	58052	8.8.8.8	192.168.2.7
Apr 8, 2021 20:36:19.297374010 CEST	54008	53	192.168.2.7	8.8.8.8
Apr 8, 2021 20:36:19.309941053 CEST	53	54008	8.8.8.8	192.168.2.7
Apr 8, 2021 20:36:20.350488901 CEST	59451	53	192.168.2.7	8.8.8.8
Apr 8, 2021 20:36:20.362494946 CEST	53	59451	8.8.8.8	192.168.2.7
Apr 8, 2021 20:36:24.112349033 CEST	52914	53	192.168.2.7	8.8.8.8
Apr 8, 2021 20:36:24.124360085 CEST	53	52914	8.8.8.8	192.168.2.7
Apr 8, 2021 20:36:24.996092081 CEST	64569	53	192.168.2.7	8.8.8.8
Apr 8, 2021 20:36:25.024862051 CEST	53	64569	8.8.8.8	192.168.2.7
Apr 8, 2021 20:36:26.457660913 CEST	52816	53	192.168.2.7	8.8.8.8
Apr 8, 2021 20:36:26.477552891 CEST	53	52816	8.8.8.8	192.168.2.7
Apr 8, 2021 20:36:26.722604036 CEST	50781	53	192.168.2.7	8.8.8.8
Apr 8, 2021 20:36:26.735862017 CEST	53	50781	8.8.8.8	192.168.2.7
Apr 8, 2021 20:36:52.940856934 CEST	54230	53	192.168.2.7	8.8.8.8
Apr 8, 2021 20:36:52.954406023 CEST	53	54230	8.8.8.8	192.168.2.7
Apr 8, 2021 20:36:53.004709959 CEST	54911	53	192.168.2.7	8.8.8.8
Apr 8, 2021 20:36:53.018409014 CEST	53	54911	8.8.8.8	192.168.2.7
Apr 8, 2021 20:36:59.098500967 CEST	49958	53	192.168.2.7	8.8.8.8
Apr 8, 2021 20:36:59.111011982 CEST	53	49958	8.8.8.8	192.168.2.7
Apr 8, 2021 20:37:14.608776093 CEST	50860	53	192.168.2.7	8.8.8.8
Apr 8, 2021 20:37:14.624608994 CEST	53	50860	8.8.8.8	192.168.2.7
Apr 8, 2021 20:37:24.458585978 CEST	50452	53	192.168.2.7	8.8.8.8
Apr 8, 2021 20:37:24.472449064 CEST	53	50452	8.8.8.8	192.168.2.7
Apr 8, 2021 20:37:54.713227034 CEST	59730	53	192.168.2.7	8.8.8.8
Apr 8, 2021 20:37:54.726056099 CEST	53	59730	8.8.8.8	192.168.2.7
Apr 8, 2021 20:38:19.167885065 CEST	59310	53	192.168.2.7	8.8.8.8
Apr 8, 2021 20:38:19.181062937 CEST	53	59310	8.8.8.8	192.168.2.7
Apr 8, 2021 20:38:19.822521925 CEST	51919	53	192.168.2.7	8.8.8.8
Apr 8, 2021 20:38:19.837526083 CEST	53	51919	8.8.8.8	192.168.2.7
Apr 8, 2021 20:38:20.359267950 CEST	64296	53	192.168.2.7	8.8.8.8
Apr 8, 2021 20:38:20.472702026 CEST	53	64296	8.8.8.8	192.168.2.7
Apr 8, 2021 20:38:21.086715937 CEST	56680	53	192.168.2.7	8.8.8.8
Apr 8, 2021 20:38:21.101727009 CEST	53	56680	8.8.8.8	192.168.2.7
Apr 8, 2021 20:38:21.528199911 CEST	58820	53	192.168.2.7	8.8.8.8
Apr 8, 2021 20:38:21.541776896 CEST	53	58820	8.8.8.8	192.168.2.7
Apr 8, 2021 20:38:21.716824055 CEST	60983	53	192.168.2.7	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 20:38:21.744277954 CEST	53	60983	8.8.8.8	192.168.2.7
Apr 8, 2021 20:38:22.060075045 CEST	49247	53	192.168.2.7	8.8.8.8
Apr 8, 2021 20:38:22.073153973 CEST	53	49247	8.8.8.8	192.168.2.7
Apr 8, 2021 20:38:22.459789038 CEST	52286	53	192.168.2.7	8.8.8.8
Apr 8, 2021 20:38:22.473186970 CEST	53	52286	8.8.8.8	192.168.2.7
Apr 8, 2021 20:38:23.178003073 CEST	56064	53	192.168.2.7	8.8.8.8
Apr 8, 2021 20:38:23.191903114 CEST	53	56064	8.8.8.8	192.168.2.7
Apr 8, 2021 20:38:24.355834961 CEST	63744	53	192.168.2.7	8.8.8.8
Apr 8, 2021 20:38:24.371221066 CEST	53	63744	8.8.8.8	192.168.2.7
Apr 8, 2021 20:38:24.683099031 CEST	61457	53	192.168.2.7	8.8.8.8
Apr 8, 2021 20:38:24.695868015 CEST	53	61457	8.8.8.8	192.168.2.7
Apr 8, 2021 20:38:30.105998993 CEST	58367	53	192.168.2.7	8.8.8.8
Apr 8, 2021 20:38:30.132018089 CEST	53	58367	8.8.8.8	192.168.2.7

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: factura.exe PID: 5932 Parent PID: 5772

General

Start time:	20:36:05
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\factura.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\factura.exe'
Imagebase:	0x400000
File size:	57344 bytes
MD5 hash:	5950CBE94B3B5DEDBF7B75FA1B95AC84
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic

Reputation:	low

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: RegAsm.exe PID: 4404 Parent PID: 5932

General

Start time:	20:38:18
Start date:	08/04/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\Desktop\factura.exe'
Imagebase:	0x130000
File size:	53248 bytes
MD5 hash:	529695608EAFBED00ACA9E61EF333A7C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RegAsm.exe PID: 5344 Parent PID: 5932

General

Start time:	20:38:18
Start date:	08/04/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\factura.exe'
Imagebase:	0x8a0000
File size:	53248 bytes
MD5 hash:	529695608EAFBED00ACA9E61EF333A7C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	D01E8B	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	D01E8B	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	D01E8B	InternetOpenUrlA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	D01E8B	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	D01E8B	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	D01E8B	InternetOpenUrlA

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 68 Parent PID: 5344

General

Start time:	20:38:19
Start date:	08/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis