ID: 384277
Sample Name: factura.exe
Cookbook: default.jbs
Time: 20:43:47
Date: 08/04/2021
Version: 31.0.0 Emerald

Table of Contents

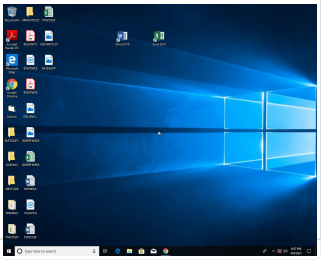
Analysis Report factura.exe

Overview

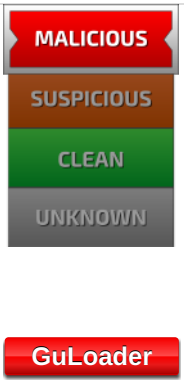
General Information

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

Most interesting Screenshot:



Detection



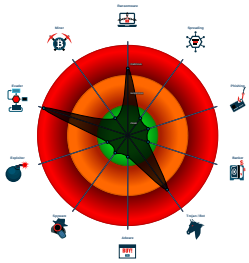
GuLoader

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

Signatures

- Multi AV Scanner detection for subm…
- Potential malicious icon found
- Yara detected GuLoader
- Contains functionality to detect hard…
- Contains functionality to hide a threa…
- Detected RDTSC dummy instruction…
- Found evasive API chain (may stop…
- Found potential dummy code loops (…
- Hides threads from debuggers
- Tries to detect Any.run
- Tries to detect sandboxes and other…
- Tries to detect virtualization through…

Classification



Startup

- **System is w10x64**
- factura.exe (PID: 7088 cmdline: 'C:\Users\user\Desktop\factura.exe' MD5: 5950CBE94B3B5DEDBF7B75FA1B95AC84)
  - RegAsm.exe (PID: 5420 cmdline: 'C:\Users\user\Desktop\factura.exe' MD5: 529695608EAFBED00ACA9E61EF333A7C)
  - RegAsm.exe (PID: 5388 cmdline: 'C:\Users\user\Desktop\factura.exe' MD5: 529695608EAFBED00ACA9E61EF333A7C)
    - conhost.exe (PID: 5392 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

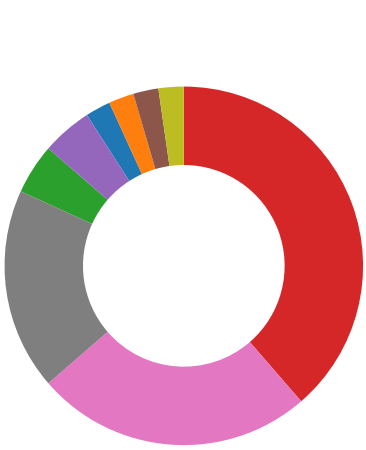
Memory Dumps

Source	Rule	Description	Author	Strings
0000000F.00000002.1031687205.0000000000C00000.00000040.00000001.sdmp	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	
Process Memory Space: RegAsm.exe PID: 5388	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	

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

Data Obfuscation:

Yara detected GuLoader

Malware Analysis System Evasion:

Contains functionality to detect hardware virtualization (CPUID execution measurement)

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

Found evasive API chain (may stop execution after reading information in the PEB, e.g. number of processors)

Tries to detect Any.run

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

Contains functionality to hide a thread from the debugger

Found potential dummy code loops (likely to delay analysis)

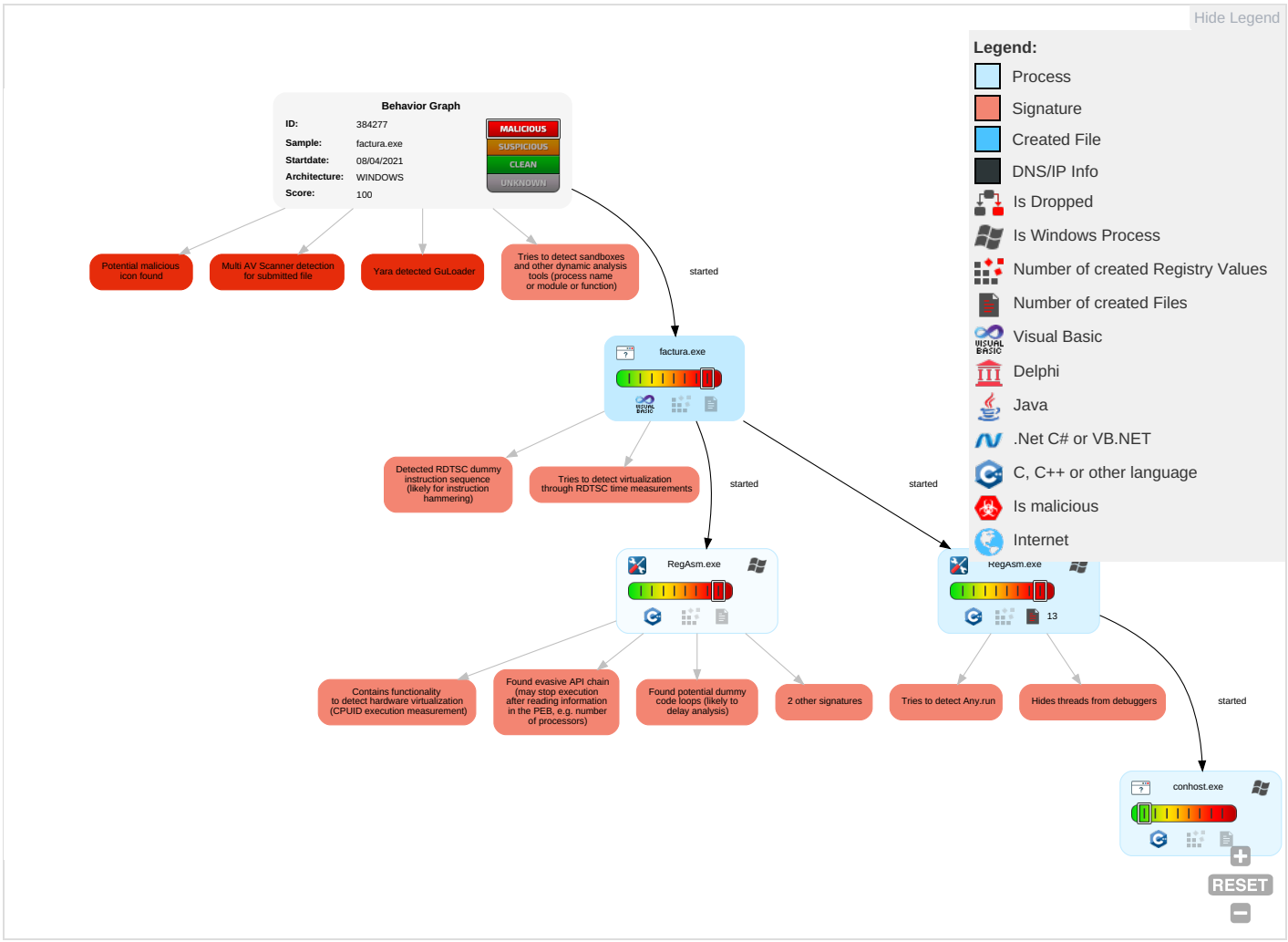
Hides threads from debuggers

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remot Servic Effects
Valid Accounts	Native API 1	DLL Side-Loading 1	Process Injection 2	Virtualization/Sandbox Evasion 3 2 1	OS Credential Dumping	Security Software Discovery 8 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Remot Track D Withou Authori
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	Remot Wipe D Withou Authori

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remot Servic Effects
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	Obtain Device Cloud Backup
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	System Information Discovery 3 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	49%	Virustotal		Browse
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

Source	Detection	Scanner	Label	Link
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://pki.g	0%	Avira URL Cloud	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://pki.goog/gsr2/GTS1O1.crt0	RegAsm.exe, 0000000F.00000002.1031930913.00000000010CC000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.pki.goog/gsr2/gsr2.crl0?	RegAsm.exe, 0000000F.00000002.1031930913.00000000010CC000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://pki.goog/repository/0	RegAsm.exe, 0000000F.00000002.1031930913.00000000010CC000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://pki.g	RegAsm.exe, 0000000F.00000002.1031916338.00000000010B0000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.pki.goog/GTS1O1core.crl0	RegAsm.exe, 0000000F.00000002.1031930913.00000000010CC000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

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:	20:43:47
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 43s
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
Run name:	Run with higher sleep bypass
Number of analysed new started processes analysed:	18
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.rans.troj.evad.winEXE@4/0@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 95.3% (good quality ratio 66.7%) • Quality average: 41.5% • Quality standard deviation: 34.2%
HCA Information:	• Successful, ratio: 69% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Sleeps bigger than 120000ms are automatically reduced to 1000ms • Found application associated with file extension: .exe
Warnings:	Show All • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 13.88.21.125, 40.88.32.150, 20.82.209.183, 23.10.249.26, 23.10.249.43, 104.42.151.234, 104.43.193.48, 52.155.217.156, 205.185.216.10, 205.185.216.42, 20.54.26.129, 20.82.210.154, 172.217.168.14 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.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, 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, consumerrp-displaycatalog-aks2eap.md.mp.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.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.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (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

General

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
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 00007F99E4BE87C5h
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 00007F99E4BE8768h
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

Instruction
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
xchg eax, ebx
push ebx
push eax
fcmovu st(0), st(6)
jp 00007F99E4BE8787h
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 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

Name	Virtual Address	Virtual Size	Is in Section
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
.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

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

Network Behavior

UDP Packets

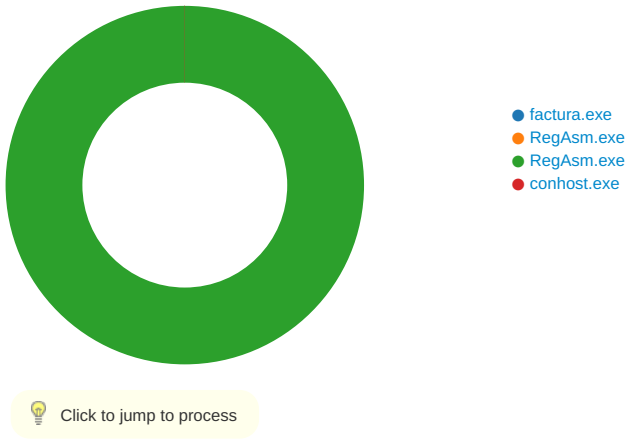
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 20:44:25.018028021 CEST	58028	53	192.168.2.4	8.8.8.8
Apr 8, 2021 20:44:25.033273935 CEST	53	58028	8.8.8.8	192.168.2.4
Apr 8, 2021 20:44:26.235450983 CEST	53097	53	192.168.2.4	8.8.8.8
Apr 8, 2021 20:44:26.249053001 CEST	53	53097	8.8.8.8	192.168.2.4
Apr 8, 2021 20:44:27.647319078 CEST	49257	53	192.168.2.4	8.8.8.8
Apr 8, 2021 20:44:27.659986973 CEST	53	49257	8.8.8.8	192.168.2.4
Apr 8, 2021 20:44:28.400440931 CEST	62389	53	192.168.2.4	8.8.8.8
Apr 8, 2021 20:44:28.413872957 CEST	53	62389	8.8.8.8	192.168.2.4
Apr 8, 2021 20:44:29.390337944 CEST	49910	53	192.168.2.4	8.8.8.8
Apr 8, 2021 20:44:29.403570890 CEST	53	49910	8.8.8.8	192.168.2.4
Apr 8, 2021 20:44:30.673795938 CEST	55854	53	192.168.2.4	8.8.8.8
Apr 8, 2021 20:44:30.687885046 CEST	53	55854	8.8.8.8	192.168.2.4
Apr 8, 2021 20:44:55.153501987 CEST	64549	53	192.168.2.4	8.8.8.8
Apr 8, 2021 20:44:55.170157909 CEST	53	64549	8.8.8.8	192.168.2.4
Apr 8, 2021 20:45:01.328985929 CEST	63153	53	192.168.2.4	8.8.8.8
Apr 8, 2021 20:45:01.348550081 CEST	53	63153	8.8.8.8	192.168.2.4
Apr 8, 2021 20:45:03.537647963 CEST	52991	53	192.168.2.4	8.8.8.8
Apr 8, 2021 20:45:03.550663948 CEST	53	52991	8.8.8.8	192.168.2.4
Apr 8, 2021 20:45:06.732263088 CEST	53700	53	192.168.2.4	8.8.8.8
Apr 8, 2021 20:45:06.745244026 CEST	53	53700	8.8.8.8	192.168.2.4
Apr 8, 2021 20:45:07.484611988 CEST	51726	53	192.168.2.4	8.8.8.8
Apr 8, 2021 20:45:07.500202894 CEST	53	51726	8.8.8.8	192.168.2.4
Apr 8, 2021 20:45:08.270230055 CEST	56794	53	192.168.2.4	8.8.8.8
Apr 8, 2021 20:45:08.283471107 CEST	53	56794	8.8.8.8	192.168.2.4
Apr 8, 2021 20:45:09.470990896 CEST	56534	53	192.168.2.4	8.8.8.8
Apr 8, 2021 20:45:09.483995914 CEST	53	56534	8.8.8.8	192.168.2.4
Apr 8, 2021 20:45:10.602649927 CEST	56627	53	192.168.2.4	8.8.8.8
Apr 8, 2021 20:45:10.615151882 CEST	53	56627	8.8.8.8	192.168.2.4
Apr 8, 2021 20:45:11.359272003 CEST	56621	53	192.168.2.4	8.8.8.8
Apr 8, 2021 20:45:11.371999025 CEST	53	56621	8.8.8.8	192.168.2.4
Apr 8, 2021 20:45:14.906299114 CEST	63116	53	192.168.2.4	8.8.8.8
Apr 8, 2021 20:45:14.919040918 CEST	53	63116	8.8.8.8	192.168.2.4
Apr 8, 2021 20:45:17.433084011 CEST	64078	53	192.168.2.4	8.8.8.8
Apr 8, 2021 20:45:17.545129061 CEST	53	64078	8.8.8.8	192.168.2.4
Apr 8, 2021 20:45:18.292279005 CEST	64801	53	192.168.2.4	8.8.8.8
Apr 8, 2021 20:45:18.384068012 CEST	53	64801	8.8.8.8	192.168.2.4
Apr 8, 2021 20:45:18.545285940 CEST	61721	53	192.168.2.4	8.8.8.8
Apr 8, 2021 20:45:18.560043097 CEST	53	61721	8.8.8.8	192.168.2.4
Apr 8, 2021 20:45:18.794848919 CEST	51255	53	192.168.2.4	8.8.8.8
Apr 8, 2021 20:45:18.807977915 CEST	53	51255	8.8.8.8	192.168.2.4
Apr 8, 2021 20:45:19.152693987 CEST	61522	53	192.168.2.4	8.8.8.8
Apr 8, 2021 20:45:19.168514967 CEST	53	61522	8.8.8.8	192.168.2.4
Apr 8, 2021 20:45:19.253931046 CEST	52337	53	192.168.2.4	8.8.8.8
Apr 8, 2021 20:45:19.266459942 CEST	53	52337	8.8.8.8	192.168.2.4
Apr 8, 2021 20:45:19.693877935 CEST	55046	53	192.168.2.4	8.8.8.8
Apr 8, 2021 20:45:19.706681013 CEST	53	55046	8.8.8.8	192.168.2.4
Apr 8, 2021 20:45:20.001358032 CEST	49612	53	192.168.2.4	8.8.8.8
Apr 8, 2021 20:45:20.014388084 CEST	53	49612	8.8.8.8	192.168.2.4
Apr 8, 2021 20:45:20.123475075 CEST	49285	53	192.168.2.4	8.8.8.8
Apr 8, 2021 20:45:20.139849901 CEST	53	49285	8.8.8.8	192.168.2.4
Apr 8, 2021 20:45:20.176346064 CEST	50601	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 20:45:20.190529108 CEST	53	50601	8.8.8.8	192.168.2.4
Apr 8, 2021 20:45:20.374970913 CEST	60875	53	192.168.2.4	8.8.8.8
Apr 8, 2021 20:45:20.407475948 CEST	53	60875	8.8.8.8	192.168.2.4
Apr 8, 2021 20:45:20.519582033 CEST	56448	53	192.168.2.4	8.8.8.8
Apr 8, 2021 20:45:20.611478090 CEST	53	56448	8.8.8.8	192.168.2.4
Apr 8, 2021 20:45:20.647066116 CEST	59172	53	192.168.2.4	8.8.8.8
Apr 8, 2021 20:45:20.661165953 CEST	53	59172	8.8.8.8	192.168.2.4
Apr 8, 2021 20:45:21.215986967 CEST	62420	53	192.168.2.4	8.8.8.8
Apr 8, 2021 20:45:21.229494095 CEST	53	62420	8.8.8.8	192.168.2.4
Apr 8, 2021 20:45:22.265459061 CEST	60579	53	192.168.2.4	8.8.8.8
Apr 8, 2021 20:45:22.280459881 CEST	53	60579	8.8.8.8	192.168.2.4
Apr 8, 2021 20:45:22.594882011 CEST	50183	53	192.168.2.4	8.8.8.8
Apr 8, 2021 20:45:22.648865938 CEST	53	50183	8.8.8.8	192.168.2.4
Apr 8, 2021 20:45:34.037904024 CEST	61531	53	192.168.2.4	8.8.8.8
Apr 8, 2021 20:45:34.058129072 CEST	53	61531	8.8.8.8	192.168.2.4
Apr 8, 2021 20:46:05.813369036 CEST	49228	53	192.168.2.4	8.8.8.8
Apr 8, 2021 20:46:05.828219891 CEST	53	49228	8.8.8.8	192.168.2.4
Apr 8, 2021 20:46:09.114721060 CEST	59794	53	192.168.2.4	8.8.8.8
Apr 8, 2021 20:46:09.143913984 CEST	53	59794	8.8.8.8	192.168.2.4
Apr 8, 2021 20:46:34.451797009 CEST	55916	53	192.168.2.4	8.8.8.8
Apr 8, 2021 20:46:34.480366945 CEST	53	55916	8.8.8.8	192.168.2.4

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: factura.exe PID: 7088 Parent PID: 5892

General

Start time:	20:44:30
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: 5420 Parent PID: 7088

General

Start time:	20:46:23
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:	0x310000
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: 5388 Parent PID: 7088

General

Start time:	20:46:24
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:	0x800000
File size:	53248 bytes
MD5 hash:	529695608EAFBED00ACA9E61EF333A7C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader, Description: Yara detected GuLoader, Source: 0000000F.00000002.1031687205.0000000000C00000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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	C01E8B	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	C01E8B	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	C01E8B	InternetOpenUrlA
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	C01E8B	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	C01E8B	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	C01E8B	InternetOpenUrlA

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 5392 Parent PID: 5388

General

Start time:	20:46:24
Start date:	08/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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