ID: 387666
Sample Name:
faktura_ODfk0021.exe
Cookbook: default.jbs
Time: 14:02:16
Date: 15/04/2021
Version: 31.0.0 Emerald

Table of Contents

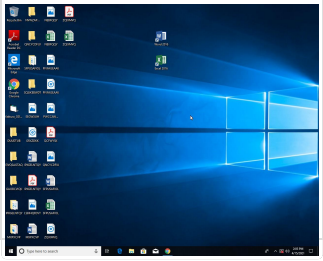
Analysis Report faktura_ODfk0021.exe

Overview

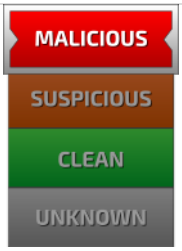
General Information

Sample Name:	faktura_ODfk0021.exe
Analysis ID:	387666
MD5:	b7b1644fce14205.
SHA1:	4cbfa9cf4b8dc27...
SHA256:	f760c40ea4cca84..
Infos:	

Most interesting Screenshot:



Detection



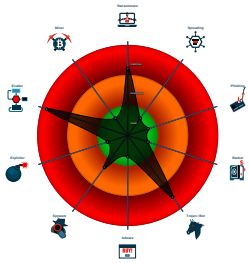
AgentTesla GuLoader

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

Signatures

- Found malware configuration
- Potential malicious icon found
- Yara detected AgentTesla
- Yara detected GuLoader
- C2 URLs / IPs found in malware con...
- Contains functionality to detect hard...
- Detected RDTSC dummy instruction...
- Hides threads from debuggers
- Queries sensitive BIOS Information ...
- Queries sensitive network adapter in...
- Tries to detect Any.run
- Tries to detect sandboxes and other...

Classification



Startup

- **System is w10x64**
- faktura_ODfk0021.exe (PID: 3784 cmdline: 'C:\Users\user\Desktop\faktura_ODfk0021.exe' MD5: B7B1644FCE14205ACECBE822DF95749A)
  - RegAsm.exe (PID: 6328 cmdline: 'C:\Users\user\Desktop\faktura_ODfk0021.exe' MD5: 6FD7592411112729BF6B1F2F6C34899F)
    - conhost.exe (PID: 6336 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: GuLoader


```
{
  "Payload URL": "https://drive.google.com/uc?export=download&id=1aKE_k9PJVE2kZn5sEN4ZiJNhonuPIbPw",
  "Injection Process": [
    "RegAsm.exe",
    "RegSvcs.exe",
    "MSBuild.exe"
  ]
}
```


Yara Overview

Memory Dumps

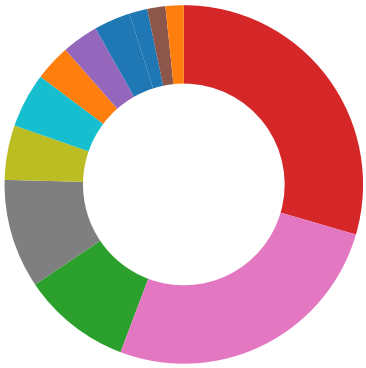
Source	Rule	Description	Author	Strings
00000003.00000002.499283716.000000001DA1 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000003.00000002.499283716.000000001DA1 1000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000003.00000002.491326318.0000000000C2 1000.00000040.00000001.sdmp	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	
Process Memory Space: RegAsm.exe PID: 6328	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
Process Memory Space: RegAsm.exe PID: 6328	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Click to see the 1 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Networking
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Networking:

C2 URLs / IPs found in malware configuration

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)

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

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:

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected AgentTesla

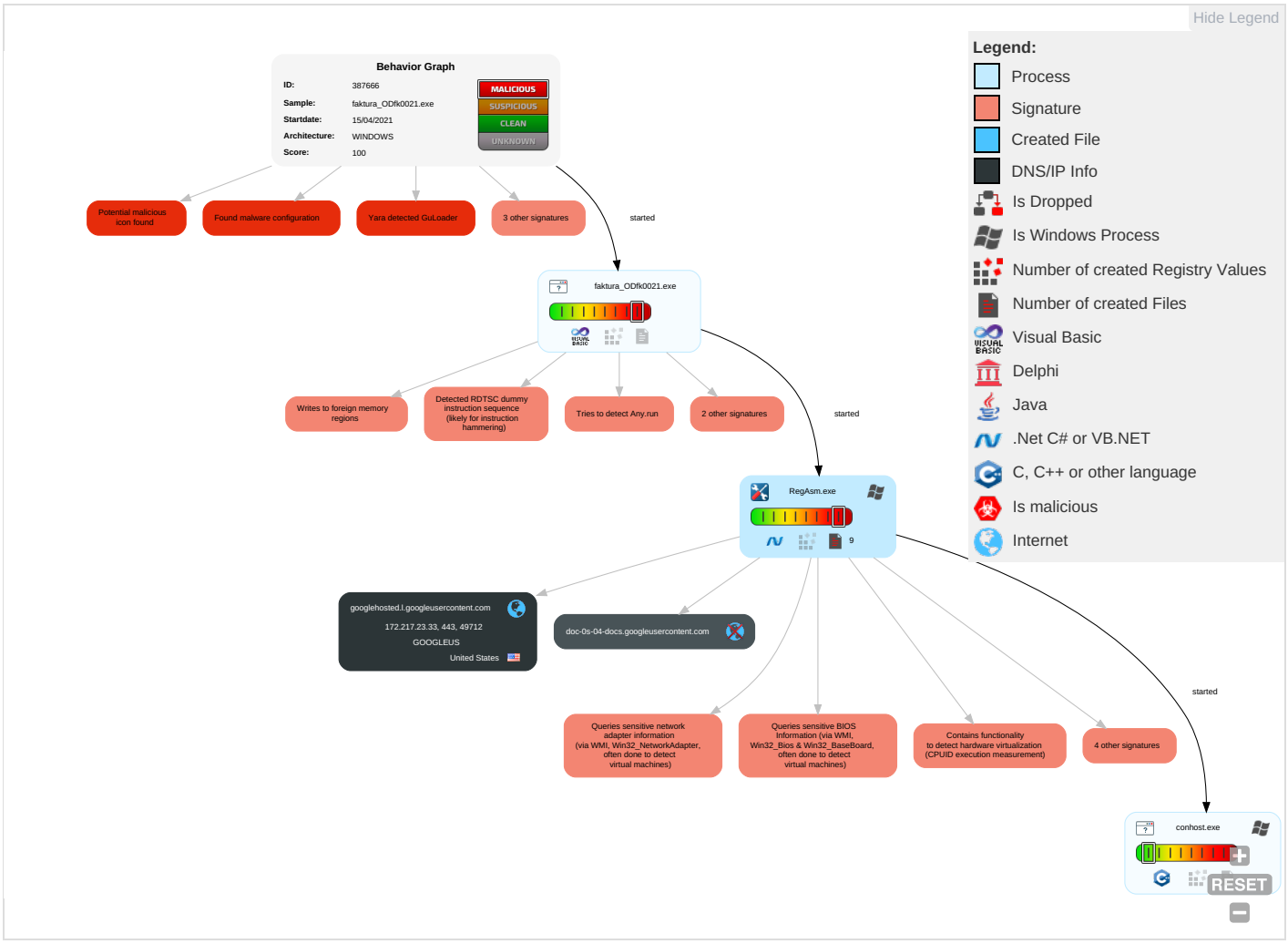
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	I
Valid Accounts	Windows Management Instrumentation 2 1 1	DLL Side-Loading 1	Process Injection 1 1 2	Disable or Modify Tools 1	OS Credential Dumping	Security Software Discovery 7 3 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Virtualization/Sandbox Evasion 3 4 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 1 2	Security Account Manager	Virtualization/Sandbox Evasion 3 4 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 1 2	
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	DLL Side-Loading 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Information Discovery 4 2 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	

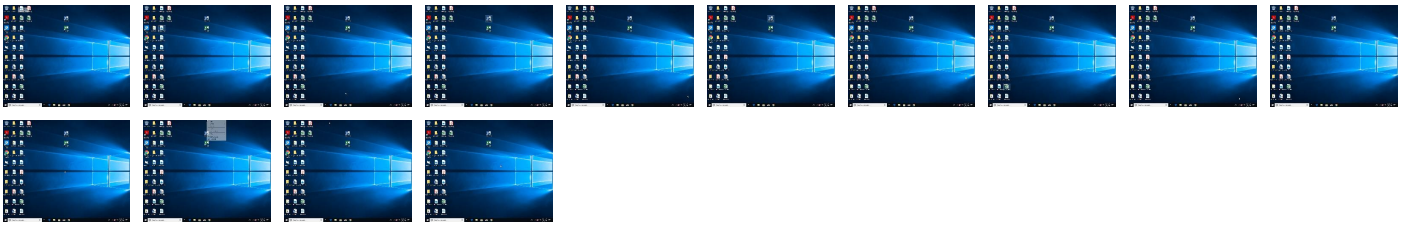
Behavior Graph



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
faktura_ODfk0021.exe	9%	ReversingLabs	Win32.Worm.Wbvb	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	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://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://zQsfOZ.com	0%	Avira URL Cloud	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://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	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

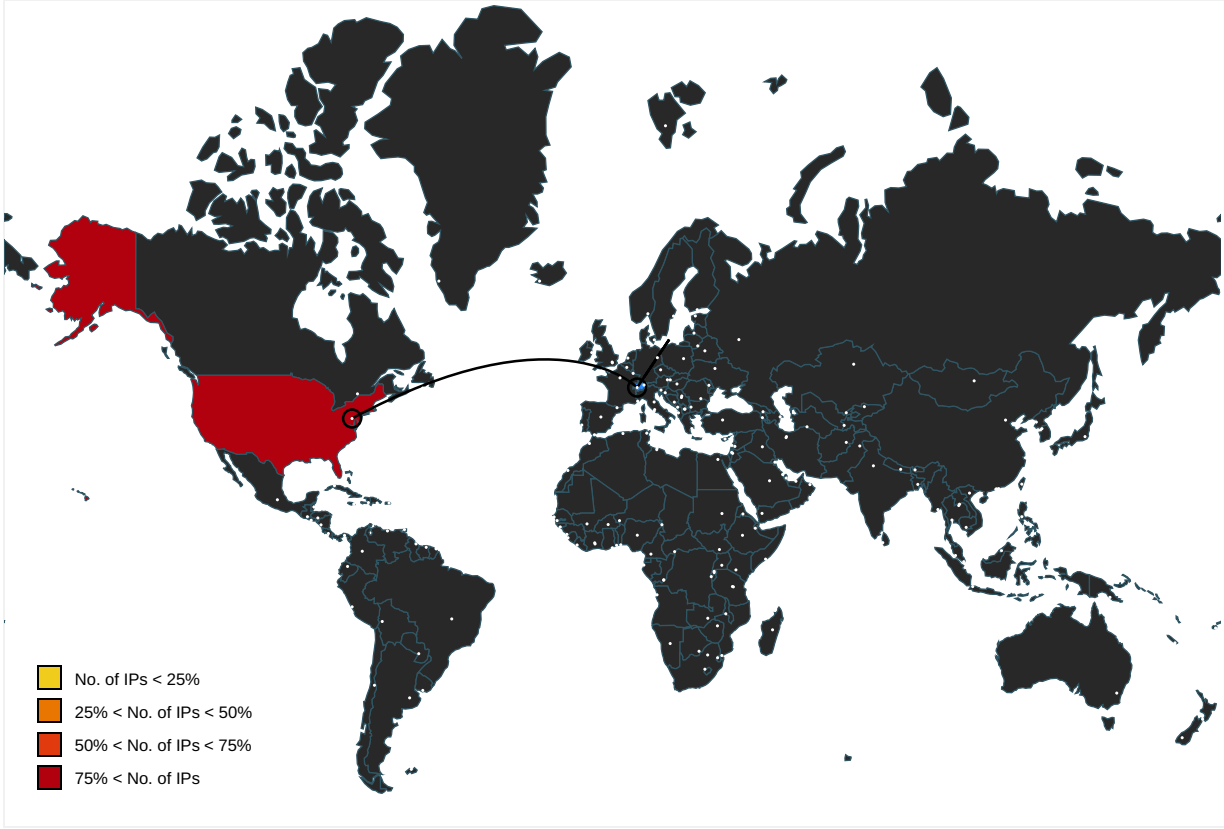
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
googlehosted.l.googleusercontent.com	172.217.23.33	true	false		high
doc-0s-04-docs.googleusercontent.com	unknown	unknown	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	RegAsm.exe, 00000003.00000002.499283716.000000001DA11000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://DynDns.comDynDNS	RegAsm.exe, 00000003.00000002.499283716.000000001DA11000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://pki.goog/gsr2/GTS1O1.crt0	RegAsm.exe, 00000003.00000002.491961756.0000000000FFA000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://doc-0s-04-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/uq2l008j	RegAsm.exe, 00000003.00000002.491961756.0000000000FFA000.00000004.00000020.sdmp	false		high
http://zQsfOZ.com	RegAsm.exe, 00000003.00000002.499283716.000000001DA11000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.pki.goog/gsr2/gsr2.crl0?	RegAsm.exe, 00000003.00000002.491961756.0000000000FFA000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://pki.goog/repository/0	RegAsm.exe, 00000003.00000002.491961756.0000000000FFA000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	RegAsm.exe, 00000003.00000002.499283716.000000001DA11000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.pki.goog/GTS1O1core.crl0	RegAsm.exe, 00000003.00000002.491961756.0000000000FFA000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.217.23.33	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	387666
Start date:	15.04.2021
Start time:	14:02:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 14s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	faktura_ODfk0021.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:	27
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@1/1
EGA Information:	Failed

HDC Information:	• Successful, ratio: 17% (good quality ratio 7.2%) • Quality average: 25.8% • Quality standard deviation: 32%
HCA Information:	• Successful, ratio: 94% • 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
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, SgrmBroker.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 131.253.33.200, 13.107.22.200, 20.82.210.154, 40.88.32.150, 92.122.145.220, 92.122.144.200, 13.64.90.137, 172.217.20.238, 52.255.188.83, 2.20.143.16, 2.20.142.210, 51.103.5.186, 104.43.193.48, 23.32.238.234, 23.32.238.177, 52.155.217.156, 20.54.26.129 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, 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, skypedataprdcoleus15.cloudapp.net, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.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, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, client.wns.windows.com, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, skypedataprdcolcus15.cloudapp.net, dual-a-0001.dc-msedge.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.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/387666/sample/faktura_ODfk0021.exe

Simulations

Behavior and APIs

Time	Type	Description
14:03:56	API Interceptor	543x Sleep call for process: RegAsm.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	documents-1865367136.xlsb	Get hash	malicious	Browse	• 172.217.23.33
	documents-1522654785.xlsb	Get hash	malicious	Browse	• 172.217.23.33
	documents-1988650417.xlsb	Get hash	malicious	Browse	• 172.217.23.33
	documents-852304211.xlsb	Get hash	malicious	Browse	• 172.217.23.33
	Tooligram_PRO.exe	Get hash	malicious	Browse	• 172.217.23.33
	documents-1884913828.xlsb	Get hash	malicious	Browse	• 172.217.23.33
	documents-1097636918.xlsb	Get hash	malicious	Browse	• 172.217.23.33
	documents-798055763.xlsb	Get hash	malicious	Browse	• 172.217.23.33
	documents-590513756.xlsb	Get hash	malicious	Browse	• 172.217.23.33
	#Ud83d#Udcde Bpost.be AudioMessage 59-20596.htm	Get hash	malicious	Browse	• 172.217.23.33
	VoicePlayback (01_47) for steph.miller tsbbank .html	Get hash	malicious	Browse	• 172.217.23.33
	Factura proforma, nuevo pedido.exe	Get hash	malicious	Browse	• 172.217.23.33
	documents-1321106901.xlsb	Get hash	malicious	Browse	• 172.217.23.33
	BR-424305.htm	Get hash	malicious	Browse	• 172.217.23.33
	0901e76c84536f06b_2500332020005403099_0901e76c4489e546f06b_250020214405500030995.WsF	Get hash	malicious	Browse	• 172.217.23.33
	mail_6512365134_7863_20210413.html	Get hash	malicious	Browse	• 172.217.23.33
	Cocha904.htm	Get hash	malicious	Browse	• 172.217.23.33
	documents-1136727851.xlsb	Get hash	malicious	Browse	• 172.217.23.33
	Lista comenzilor.exe	Get hash	malicious	Browse	• 172.217.23.33
	documents-2136656015.xlsb	Get hash	malicious	Browse	• 172.217.23.33

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):	5.82523235745994

General

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:	faktura_ODfk0021.exe
File size:	73728
MD5:	b7b1644fce14205acecbe822df95749a
SHA1:	4cbfa9cf4b8dc27bf2b2a2463761092d5c2402e7
SHA256:	f760c40ea4cca84e06c511f96c8d43525350e3f52c97c1baa30528d9c4fbcfec
SHA512:	8110f60d9c116b277a247b059099100afaf3ebf4fd9e685686c043b78119e2ebf3e5793128c6c607b992d231a92101956b4738a213e0ca6bf8f291d2e68a0a7e
SSDEEP:	1536:A35XClFvvI5WX5sdzUPgKYxVm18htRXPA:EXClBI5zi1utFPA
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.....w`.....0.....@.....

File Icon

Icon Hash:	20047c7c70f0e004

Static PE Info

General

Entrypoint:	0x4015b4
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:	0x6077DFAB [Thu Apr 15 06:39:39 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:	fff80e017e94a979a89868fcc864e987

Entrypoint Preview

Instruction
push 0040179Ch
call 00007F21FCF8FE35h
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 al, al
scasb

Instruction
push edx
xor cl, cl
mov edx, C1B4469Ah
cmp al, 4Eh
jne 00007F21FCF8FE80h
int1
mov ebx, 00000000h
add byte ptr [eax], al
add dword ptr [eax], eax
add byte ptr [eax], al
or cl, byte ptr [726F460Ah]
push ebx
push 00000075h
jnc 00007F21FCF8FEADh
jc 00007F21FCF8FEACh
jc 00007F21FCF8FE77h
add byte ptr [eax], ah
dec ecx
or ax, 00000000h
add byte ptr [eax], al
dec esp
xor dword ptr [eax], eax
add eax, 6D740047h
mov ebp, A34121E1h
jne 00007F21FCF8FE9Dh
into
mov ebp, B5608642h
wait
in al, FAh
insd
dec eax
inc edi
dec ebx
sbb dword ptr [edx], 24BD732Fh
loopne 00007F21FCF8FE50h
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
cmp eax, 52000001h
add byte ptr [eax], al
add byte ptr [eax], al
push cs
add byte ptr [ebx+45h], al

Instruction
dec esi
push esp
inc ebp
push edx
dec eax
inc ecx
dec esp
inc esi
inc edx
inc ecx
inc ebx
dec ebx
add byte ptr [42000B01h], cl

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xf864	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x12000	0x8e0	.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	0x15c	.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	0xee24	0xf000	False	0.473046875	data	6.47418964724	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x10000	0x12a8	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x12000	0x8e0	0x1000	False	0.16552734375	data	1.93654602979	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x127b0	0x130	data		
RT_ICON	0x124c8	0x2e8	data		
RT_ICON	0x123a0	0x128	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x12370	0x30	data		
RT_VERSION	0x12150	0x220	data	Chinese	Taiwan

Imports

DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaVarMove, __vbaFreeVar, __vbaStrVarMove, __vbaFreeVarList, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaSetSystemError, __vbaHresultCheckObj, _adj_fdiv_m32, __vbaAryDestruct, __vbaObjSet, _adj_fdiv_m16i, __vbaObjSetAddref, _adj_fdivr_m16i, __vbaVarTstLt, __vbaFpR8, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, __vbaGenerateBoundsError, __vbaStrCmp, __vbaAryConstruct2, __vbaObjVar, DllFunctionCall, _adj_fpatan, __vbaLateIdCallLd, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, __vbaStrToUnicode, _adj_fprem, _adj_fdivr_m64, __vbaFPException, __vbaStrVarVal, _CIlog, __vbaFileOpen, __vbaNew2, __vbaR8Str, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaI4Str, __vbaFreeStrList, _adj_fdivr_m32, _adj_fdiv_r, __vbaVarTstNe, __vbaI4Var, __vbaVarAdd, __vbaLateMemCall, __vbaStrToAnsi, __vbaVarDup, __vbaFpI4, _CIatan, __vbaStrMove, __vbaCastObj, _allmul, __vbaLateIdSt, _CItan, _CIexp, __vbaFreeObj, __vbaFreeStr

Version Infos

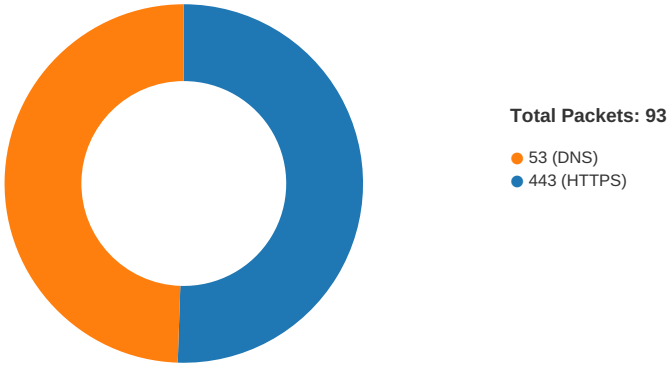
Description	Data
Translation	0x0404 0x04b0
InternalName	Cass7
FileVersion	1.00
CompanyName	ADP
ProductName	ADP
ProductVersion	1.00
FileDescription	ADP
OriginalFilename	Cass7.exe

Possible Origin

Language of compilation system	Country where language is spoken	Map
Chinese	Taiwan	

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 15, 2021 14:03:48.067195892 CEST	49712	443	192.168.2.7	172.217.23.33
Apr 15, 2021 14:03:48.110661030 CEST	443	49712	172.217.23.33	192.168.2.7
Apr 15, 2021 14:03:48.110769033 CEST	49712	443	192.168.2.7	172.217.23.33
Apr 15, 2021 14:03:48.111541986 CEST	49712	443	192.168.2.7	172.217.23.33
Apr 15, 2021 14:03:48.156805038 CEST	443	49712	172.217.23.33	192.168.2.7
Apr 15, 2021 14:03:48.170378923 CEST	443	49712	172.217.23.33	192.168.2.7
Apr 15, 2021 14:03:48.170437098 CEST	443	49712	172.217.23.33	192.168.2.7
Apr 15, 2021 14:03:48.170475006 CEST	443	49712	172.217.23.33	192.168.2.7
Apr 15, 2021 14:03:48.170511961 CEST	443	49712	172.217.23.33	192.168.2.7
Apr 15, 2021 14:03:48.170531034 CEST	49712	443	192.168.2.7	172.217.23.33
Apr 15, 2021 14:03:48.170556068 CEST	49712	443	192.168.2.7	172.217.23.33
Apr 15, 2021 14:03:48.170574903 CEST	49712	443	192.168.2.7	172.217.23.33
Apr 15, 2021 14:03:48.181966066 CEST	49712	443	192.168.2.7	172.217.23.33
Apr 15, 2021 14:03:48.225636959 CEST	443	49712	172.217.23.33	192.168.2.7
Apr 15, 2021 14:03:48.225717068 CEST	49712	443	192.168.2.7	172.217.23.33
Apr 15, 2021 14:03:48.227636099 CEST	49712	443	192.168.2.7	172.217.23.33
Apr 15, 2021 14:03:48.275768995 CEST	443	49712	172.217.23.33	192.168.2.7
Apr 15, 2021 14:03:48.827013969 CEST	443	49712	172.217.23.33	192.168.2.7
Apr 15, 2021 14:03:48.827038050 CEST	443	49712	172.217.23.33	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 15, 2021 14:03:48.827056885 CEST	443	49712	172.217.23.33	192.168.2.7
Apr 15, 2021 14:03:48.827074051 CEST	443	49712	172.217.23.33	192.168.2.7
Apr 15, 2021 14:03:48.827090025 CEST	443	49712	172.217.23.33	192.168.2.7
Apr 15, 2021 14:03:48.827107906 CEST	49712	443	192.168.2.7	172.217.23.33
Apr 15, 2021 14:03:48.827148914 CEST	49712	443	192.168.2.7	172.217.23.33
Apr 15, 2021 14:03:48.830087900 CEST	443	49712	172.217.23.33	192.168.2.7
Apr 15, 2021 14:03:48.830108881 CEST	443	49712	172.217.23.33	192.168.2.7
Apr 15, 2021 14:03:48.830226898 CEST	49712	443	192.168.2.7	172.217.23.33
Apr 15, 2021 14:03:48.830244064 CEST	49712	443	192.168.2.7	172.217.23.33
Apr 15, 2021 14:03:48.833547115 CEST	443	49712	172.217.23.33	192.168.2.7
Apr 15, 2021 14:03:48.833617926 CEST	49712	443	192.168.2.7	172.217.23.33
Apr 15, 2021 14:03:48.833900928 CEST	443	49712	172.217.23.33	192.168.2.7
Apr 15, 2021 14:03:48.833956957 CEST	49712	443	192.168.2.7	172.217.23.33
Apr 15, 2021 14:03:48.836338997 CEST	443	49712	172.217.23.33	192.168.2.7
Apr 15, 2021 14:03:48.836359978 CEST	443	49712	172.217.23.33	192.168.2.7
Apr 15, 2021 14:03:48.836402893 CEST	49712	443	192.168.2.7	172.217.23.33
Apr 15, 2021 14:03:48.836492062 CEST	49712	443	192.168.2.7	172.217.23.33
Apr 15, 2021 14:03:48.839488029 CEST	443	49712	172.217.23.33	192.168.2.7
Apr 15, 2021 14:03:48.839509964 CEST	443	49712	172.217.23.33	192.168.2.7
Apr 15, 2021 14:03:48.839556932 CEST	49712	443	192.168.2.7	172.217.23.33
Apr 15, 2021 14:03:48.839572906 CEST	49712	443	192.168.2.7	172.217.23.33
Apr 15, 2021 14:03:48.842108965 CEST	443	49712	172.217.23.33	192.168.2.7
Apr 15, 2021 14:03:48.842129946 CEST	443	49712	172.217.23.33	192.168.2.7
Apr 15, 2021 14:03:48.842190981 CEST	49712	443	192.168.2.7	172.217.23.33
Apr 15, 2021 14:03:48.870493889 CEST	443	49712	172.217.23.33	192.168.2.7
Apr 15, 2021 14:03:48.870529890 CEST	443	49712	172.217.23.33	192.168.2.7
Apr 15, 2021 14:03:48.870584011 CEST	49712	443	192.168.2.7	172.217.23.33
Apr 15, 2021 14:03:48.870604038 CEST	49712	443	192.168.2.7	172.217.23.33
Apr 15, 2021 14:03:48.872016907 CEST	443	49712	172.217.23.33	192.168.2.7
Apr 15, 2021 14:03:48.872037888 CEST	443	49712	172.217.23.33	192.168.2.7
Apr 15, 2021 14:03:48.872087955 CEST	49712	443	192.168.2.7	172.217.23.33
Apr 15, 2021 14:03:48.872103930 CEST	49712	443	192.168.2.7	172.217.23.33
Apr 15, 2021 14:03:48.875106096 CEST	443	49712	172.217.23.33	192.168.2.7
Apr 15, 2021 14:03:48.875178099 CEST	49712	443	192.168.2.7	172.217.23.33
Apr 15, 2021 14:03:48.875179052 CEST	443	49712	172.217.23.33	192.168.2.7
Apr 15, 2021 14:03:48.875221968 CEST	49712	443	192.168.2.7	172.217.23.33
Apr 15, 2021 14:03:48.878283024 CEST	443	49712	172.217.23.33	192.168.2.7
Apr 15, 2021 14:03:48.878315926 CEST	443	49712	172.217.23.33	192.168.2.7
Apr 15, 2021 14:03:48.878360033 CEST	49712	443	192.168.2.7	172.217.23.33
Apr 15, 2021 14:03:48.878376961 CEST	49712	443	192.168.2.7	172.217.23.33
Apr 15, 2021 14:03:48.881469011 CEST	443	49712	172.217.23.33	192.168.2.7
Apr 15, 2021 14:03:48.881489992 CEST	443	49712	172.217.23.33	192.168.2.7
Apr 15, 2021 14:03:48.881541967 CEST	49712	443	192.168.2.7	172.217.23.33
Apr 15, 2021 14:03:48.881562948 CEST	49712	443	192.168.2.7	172.217.23.33
Apr 15, 2021 14:03:48.884577036 CEST	443	49712	172.217.23.33	192.168.2.7
Apr 15, 2021 14:03:48.884596109 CEST	443	49712	172.217.23.33	192.168.2.7
Apr 15, 2021 14:03:48.884650946 CEST	49712	443	192.168.2.7	172.217.23.33
Apr 15, 2021 14:03:48.884666920 CEST	49712	443	192.168.2.7	172.217.23.33
Apr 15, 2021 14:03:48.887749910 CEST	443	49712	172.217.23.33	192.168.2.7
Apr 15, 2021 14:03:48.887769938 CEST	443	49712	172.217.23.33	192.168.2.7
Apr 15, 2021 14:03:48.887830973 CEST	49712	443	192.168.2.7	172.217.23.33
Apr 15, 2021 14:03:48.887850046 CEST	49712	443	192.168.2.7	172.217.23.33
Apr 15, 2021 14:03:48.891469955 CEST	443	49712	172.217.23.33	192.168.2.7
Apr 15, 2021 14:03:48.891490936 CEST	443	49712	172.217.23.33	192.168.2.7
Apr 15, 2021 14:03:48.891549110 CEST	49712	443	192.168.2.7	172.217.23.33
Apr 15, 2021 14:03:48.891566992 CEST	49712	443	192.168.2.7	172.217.23.33
Apr 15, 2021 14:03:48.893946886 CEST	443	49712	172.217.23.33	192.168.2.7
Apr 15, 2021 14:03:48.893965960 CEST	443	49712	172.217.23.33	192.168.2.7
Apr 15, 2021 14:03:48.894023895 CEST	49712	443	192.168.2.7	172.217.23.33
Apr 15, 2021 14:03:48.894038916 CEST	49712	443	192.168.2.7	172.217.23.33
Apr 15, 2021 14:03:48.896811008 CEST	443	49712	172.217.23.33	192.168.2.7
Apr 15, 2021 14:03:48.896835089 CEST	443	49712	172.217.23.33	192.168.2.7
Apr 15, 2021 14:03:48.896909952 CEST	49712	443	192.168.2.7	172.217.23.33

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 15, 2021 14:03:48.896928072 CEST	49712	443	192.168.2.7	172.217.23.33
Apr 15, 2021 14:03:48.899534941 CEST	443	49712	172.217.23.33	192.168.2.7
Apr 15, 2021 14:03:48.899559975 CEST	443	49712	172.217.23.33	192.168.2.7
Apr 15, 2021 14:03:48.899627924 CEST	49712	443	192.168.2.7	172.217.23.33
Apr 15, 2021 14:03:48.902324915 CEST	443	49712	172.217.23.33	192.168.2.7
Apr 15, 2021 14:03:48.902348042 CEST	443	49712	172.217.23.33	192.168.2.7
Apr 15, 2021 14:03:48.902396917 CEST	49712	443	192.168.2.7	172.217.23.33
Apr 15, 2021 14:03:48.902439117 CEST	49712	443	192.168.2.7	172.217.23.33
Apr 15, 2021 14:03:48.905139923 CEST	443	49712	172.217.23.33	192.168.2.7
Apr 15, 2021 14:03:48.905163050 CEST	443	49712	172.217.23.33	192.168.2.7
Apr 15, 2021 14:03:48.905225992 CEST	49712	443	192.168.2.7	172.217.23.33
Apr 15, 2021 14:03:48.905249119 CEST	49712	443	192.168.2.7	172.217.23.33
Apr 15, 2021 14:03:48.907919884 CEST	443	49712	172.217.23.33	192.168.2.7
Apr 15, 2021 14:03:48.907943964 CEST	443	49712	172.217.23.33	192.168.2.7
Apr 15, 2021 14:03:48.907994032 CEST	49712	443	192.168.2.7	172.217.23.33
Apr 15, 2021 14:03:48.908011913 CEST	49712	443	192.168.2.7	172.217.23.33
Apr 15, 2021 14:03:48.910749912 CEST	443	49712	172.217.23.33	192.168.2.7
Apr 15, 2021 14:03:48.910773993 CEST	443	49712	172.217.23.33	192.168.2.7

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 15, 2021 14:02:58.001298904 CEST	60501	53	192.168.2.7	8.8.8.8
Apr 15, 2021 14:02:58.028203964 CEST	53775	53	192.168.2.7	8.8.8.8
Apr 15, 2021 14:02:58.058664083 CEST	53	60501	8.8.8.8	192.168.2.7
Apr 15, 2021 14:02:58.078428984 CEST	53	53775	8.8.8.8	192.168.2.7
Apr 15, 2021 14:02:58.918658972 CEST	51837	53	192.168.2.7	8.8.8.8
Apr 15, 2021 14:02:58.971151114 CEST	53	51837	8.8.8.8	192.168.2.7
Apr 15, 2021 14:03:01.249994040 CEST	55411	53	192.168.2.7	8.8.8.8
Apr 15, 2021 14:03:01.313597918 CEST	53	55411	8.8.8.8	192.168.2.7
Apr 15, 2021 14:03:02.082735062 CEST	63668	53	192.168.2.7	8.8.8.8
Apr 15, 2021 14:03:02.132936001 CEST	53	63668	8.8.8.8	192.168.2.7
Apr 15, 2021 14:03:25.237613916 CEST	54640	53	192.168.2.7	8.8.8.8
Apr 15, 2021 14:03:25.297434092 CEST	53	54640	8.8.8.8	192.168.2.7
Apr 15, 2021 14:03:34.548943043 CEST	58739	53	192.168.2.7	8.8.8.8
Apr 15, 2021 14:03:34.601429939 CEST	53	58739	8.8.8.8	192.168.2.7
Apr 15, 2021 14:03:35.794125080 CEST	60338	53	192.168.2.7	8.8.8.8
Apr 15, 2021 14:03:35.847773075 CEST	53	60338	8.8.8.8	192.168.2.7
Apr 15, 2021 14:03:46.109419107 CEST	58717	53	192.168.2.7	8.8.8.8
Apr 15, 2021 14:03:46.161365986 CEST	53	58717	8.8.8.8	192.168.2.7
Apr 15, 2021 14:03:47.373816967 CEST	59762	53	192.168.2.7	8.8.8.8
Apr 15, 2021 14:03:47.439893961 CEST	53	59762	8.8.8.8	192.168.2.7
Apr 15, 2021 14:03:47.792176008 CEST	54329	53	192.168.2.7	8.8.8.8
Apr 15, 2021 14:03:47.840761900 CEST	53	54329	8.8.8.8	192.168.2.7
Apr 15, 2021 14:03:48.000417948 CEST	58052	53	192.168.2.7	8.8.8.8
Apr 15, 2021 14:03:48.065246105 CEST	53	58052	8.8.8.8	192.168.2.7
Apr 15, 2021 14:03:49.373032093 CEST	54008	53	192.168.2.7	8.8.8.8
Apr 15, 2021 14:03:49.422008991 CEST	53	54008	8.8.8.8	192.168.2.7
Apr 15, 2021 14:03:50.169035912 CEST	59451	53	192.168.2.7	8.8.8.8
Apr 15, 2021 14:03:50.217751026 CEST	53	59451	8.8.8.8	192.168.2.7
Apr 15, 2021 14:03:51.300374031 CEST	52914	53	192.168.2.7	8.8.8.8
Apr 15, 2021 14:03:51.352650881 CEST	53	52914	8.8.8.8	192.168.2.7
Apr 15, 2021 14:03:51.501138926 CEST	64569	53	192.168.2.7	8.8.8.8
Apr 15, 2021 14:03:51.553962946 CEST	53	64569	8.8.8.8	192.168.2.7
Apr 15, 2021 14:03:53.317539930 CEST	52816	53	192.168.2.7	8.8.8.8
Apr 15, 2021 14:03:53.366446018 CEST	53	52816	8.8.8.8	192.168.2.7
Apr 15, 2021 14:03:53.370409966 CEST	50781	53	192.168.2.7	8.8.8.8
Apr 15, 2021 14:03:53.431273937 CEST	53	50781	8.8.8.8	192.168.2.7
Apr 15, 2021 14:03:53.534626007 CEST	54230	53	192.168.2.7	8.8.8.8
Apr 15, 2021 14:03:53.591490030 CEST	53	54230	8.8.8.8	192.168.2.7
Apr 15, 2021 14:03:53.930619955 CEST	54911	53	192.168.2.7	8.8.8.8
Apr 15, 2021 14:03:53.995644093 CEST	53	54911	8.8.8.8	192.168.2.7
Apr 15, 2021 14:03:54.716515064 CEST	49958	53	192.168.2.7	8.8.8.8
Apr 15, 2021 14:03:54.765275955 CEST	53	49958	8.8.8.8	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 15, 2021 14:03:55.815452099 CEST	50860	53	192.168.2.7	8.8.8.8
Apr 15, 2021 14:03:55.864136934 CEST	53	50860	8.8.8.8	192.168.2.7
Apr 15, 2021 14:03:57.120651960 CEST	50452	53	192.168.2.7	8.8.8.8
Apr 15, 2021 14:03:57.171350956 CEST	53	50452	8.8.8.8	192.168.2.7
Apr 15, 2021 14:03:58.016098022 CEST	59730	53	192.168.2.7	8.8.8.8
Apr 15, 2021 14:03:58.064745903 CEST	53	59730	8.8.8.8	192.168.2.7
Apr 15, 2021 14:03:59.269495964 CEST	59310	53	192.168.2.7	8.8.8.8
Apr 15, 2021 14:03:59.318136930 CEST	53	59310	8.8.8.8	192.168.2.7
Apr 15, 2021 14:04:03.113909960 CEST	51919	53	192.168.2.7	8.8.8.8
Apr 15, 2021 14:04:03.165693998 CEST	53	51919	8.8.8.8	192.168.2.7
Apr 15, 2021 14:04:03.949346066 CEST	64296	53	192.168.2.7	8.8.8.8
Apr 15, 2021 14:04:03.998048067 CEST	53	64296	8.8.8.8	192.168.2.7
Apr 15, 2021 14:04:04.109407902 CEST	56680	53	192.168.2.7	8.8.8.8
Apr 15, 2021 14:04:04.170857906 CEST	53	56680	8.8.8.8	192.168.2.7
Apr 15, 2021 14:04:07.334784985 CEST	58820	53	192.168.2.7	8.8.8.8
Apr 15, 2021 14:04:07.383415937 CEST	53	58820	8.8.8.8	192.168.2.7
Apr 15, 2021 14:04:09.763413906 CEST	60983	53	192.168.2.7	8.8.8.8
Apr 15, 2021 14:04:09.829746008 CEST	53	60983	8.8.8.8	192.168.2.7
Apr 15, 2021 14:04:37.423278093 CEST	49247	53	192.168.2.7	8.8.8.8
Apr 15, 2021 14:04:37.480350971 CEST	53	49247	8.8.8.8	192.168.2.7
Apr 15, 2021 14:04:38.373917103 CEST	52286	53	192.168.2.7	8.8.8.8
Apr 15, 2021 14:04:38.422718048 CEST	53	52286	8.8.8.8	192.168.2.7
Apr 15, 2021 14:04:39.550192118 CEST	56064	53	192.168.2.7	8.8.8.8
Apr 15, 2021 14:04:39.601758957 CEST	53	56064	8.8.8.8	192.168.2.7
Apr 15, 2021 14:04:40.353152037 CEST	63744	53	192.168.2.7	8.8.8.8
Apr 15, 2021 14:04:40.401917934 CEST	53	63744	8.8.8.8	192.168.2.7
Apr 15, 2021 14:04:43.477310896 CEST	61457	53	192.168.2.7	8.8.8.8
Apr 15, 2021 14:04:43.536140919 CEST	53	61457	8.8.8.8	192.168.2.7
Apr 15, 2021 14:05:00.910329103 CEST	58367	53	192.168.2.7	8.8.8.8
Apr 15, 2021 14:05:01.012533903 CEST	53	58367	8.8.8.8	192.168.2.7
Apr 15, 2021 14:05:01.575809956 CEST	60599	53	192.168.2.7	8.8.8.8
Apr 15, 2021 14:05:01.816560984 CEST	53	60599	8.8.8.8	192.168.2.7
Apr 15, 2021 14:05:02.398222923 CEST	59571	53	192.168.2.7	8.8.8.8
Apr 15, 2021 14:05:02.455689907 CEST	53	59571	8.8.8.8	192.168.2.7
Apr 15, 2021 14:05:02.689614058 CEST	52689	53	192.168.2.7	8.8.8.8
Apr 15, 2021 14:05:02.754874945 CEST	53	52689	8.8.8.8	192.168.2.7
Apr 15, 2021 14:05:02.902904034 CEST	50290	53	192.168.2.7	8.8.8.8
Apr 15, 2021 14:05:02.990034103 CEST	53	50290	8.8.8.8	192.168.2.7
Apr 15, 2021 14:05:03.557638884 CEST	60427	53	192.168.2.7	8.8.8.8
Apr 15, 2021 14:05:03.686425924 CEST	53	60427	8.8.8.8	192.168.2.7
Apr 15, 2021 14:05:04.432878017 CEST	56209	53	192.168.2.7	8.8.8.8
Apr 15, 2021 14:05:04.489887953 CEST	53	56209	8.8.8.8	192.168.2.7
Apr 15, 2021 14:05:05.141227961 CEST	59582	53	192.168.2.7	8.8.8.8
Apr 15, 2021 14:05:05.198559999 CEST	53	59582	8.8.8.8	192.168.2.7
Apr 15, 2021 14:05:06.189922094 CEST	60949	53	192.168.2.7	8.8.8.8
Apr 15, 2021 14:05:06.250034094 CEST	53	60949	8.8.8.8	192.168.2.7
Apr 15, 2021 14:05:07.184478045 CEST	58542	53	192.168.2.7	8.8.8.8
Apr 15, 2021 14:05:07.241842031 CEST	53	58542	8.8.8.8	192.168.2.7
Apr 15, 2021 14:05:07.915469885 CEST	59179	53	192.168.2.7	8.8.8.8
Apr 15, 2021 14:05:07.972846031 CEST	53	59179	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 15, 2021 14:03:48.000417948 CEST	192.168.2.7	8.8.8.8	0xe7be	Standard query (0)	doc-0s-04-docs.googleusercontent.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 15, 2021 14:03:48.065246105 CEST	8.8.8.8	192.168.2.7	0xe7be	No error (0)	doc-0s-04-docs.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 15, 2021 14:03:48.065246105 CEST	8.8.8.8	192.168.2.7	0xe7be	No error (0)	googlehosted.l.googleusercontent.com		172.217.23.33	A (IP address)	IN (0x0001)

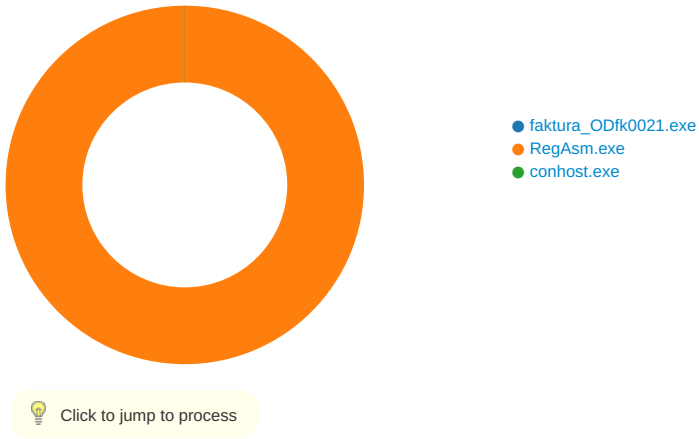
HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 15, 2021 14:03:48.170511961 CEST	172.217.23.33	443	192.168.2.7	49712	CN=*.googleusercontent.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Mar 16 20:32:57 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Jun 08 21:32:56 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: faktura_ODfk0021.exe PID: 3784 Parent PID: 5672

General

Start time:	14:03:03
Start date:	15/04/2021
Path:	C:\Users\user\Desktop\faktura_ODfk0021.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\faktura_ODfk0021.exe'

Imagebase:	0x400000
File size:	73728 bytes
MD5 hash:	B7B1644FCE14205ACECBE822DF95749A
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: 6328 Parent PID: 3784

General

Start time:	14:03:25
Start date:	15/04/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\faktura_ODfk0021.exe'
Imagebase:	0x840000
File size:	64616 bytes
MD5 hash:	6FD7592411112729BF6B1F2F6C34899F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.499283716.000000001DA11000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000002.499283716.000000001DA11000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader, Description: Yara detected GuLoader, Source: 00000003.00000002.491326318.0000000000C21000.00000040.00000001.sdmp, Author: Joe Security
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	C22197	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	C22197	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	C22197	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	C22197	InternetOpenUrlA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	C22197	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	C22197	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	6CB1CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CB1CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4095	success or wait	1	6CAF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	8173	end of file	1	6CAF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CAF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CAF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CA503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4095	success or wait	1	6CAFCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	8173	end of file	1	6CAFCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CAFCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CA503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CA503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CA503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CA503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CAF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CAF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6B961B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6B961B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4096	success or wait	1	6B961B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4096	end of file	1	6B961B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4095	success or wait	1	6CAF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	8173	end of file	1	6CAF5705	unknown

Analysis Process: conhost.exe PID: 6336 Parent PID: 6328

General

Start time:	14:03:25
Start date:	15/04/2021
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