ID: 321142
Sample Name: fattura.exe
Cookbook: default.jbs
Time: 12:35:24
Date: 20/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

Table of Contents 2
Analysis Report fattura.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Threatname: Agenttesla 4
Yara Overview 4
Memory Dumps 4
Unpacked PEs 5
Sigma Overview 5
System Summary: 5
Signature Overview 5
AV Detection: 5
Networking: 5
Key, Mouse, Clipboard, Microphone and Screen Capturing: 5
System Summary: 5
Malware Analysis System Evasion: 6
HIPS / PFW / Operating System Protection Evasion: 6
Stealing of Sensitive Information: 6
Remote Access Functionality: 6
Mitre Att&ck Matrix 6
Behavior Graph 7
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 8
URLs 8
Domains and IPs 9
Contacted Domains 9
URLs from Memory and Binaries 9
Contacted IPs 10
Public 10
General Information 10
Simulations 11
Behavior and APIs 11
Joe Sandbox View / Context 11
IPs 11
Domains 12
ASN 12
JA3 Fingerprints 12
Dropped Files 12
Created / dropped Files 12
Static File Info 13
General 13
File Icon 13
Static PE Info 13
General 13
Entrypoint Preview 14
Data Directories 15

Sections 16
Resources 16
Imports 16
Network Behavior 16
Snort IDS Alerts 16
Network Port Distribution 16
TCP Packets 16
UDP Packets 17
DNS Queries 18
DNS Answers 18
SMTP Packets 18
Code Manipulations 19
Statistics 19
Behavior 19
System Behavior 19
Analysis Process: fattura.exe PID: 3984 Parent PID: 5820 19
General 19
File Activities 20
File Created 20
File Written 20
File Read 20
Analysis Process: RegAsm.exe PID: 2456 Parent PID: 3984 21
General 21
Analysis Process: RegAsm.exe PID: 864 Parent PID: 3984 21
General 21
File Activities 21
File Created 21
File Read 21
Disassembly 22
Code Analysis 22

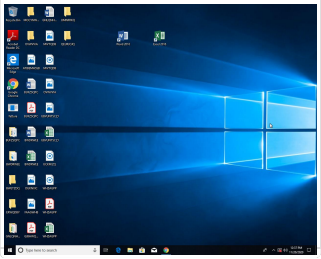
Analysis Report fattura.exe

Overview

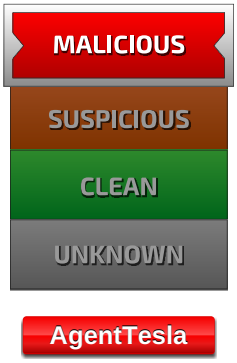
General Information

Sample Name:	fattura.exe
Analysis ID:	321142
MD5:	ac16b512e9de93..
SHA1:	85eff7055833458..
SHA256:	2112f6c6abb4fe8..
Tags:	AgentTesla

Most interesting Screenshot:



Detection

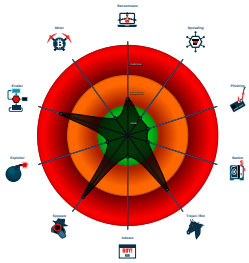


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Sigma detected: RegAsm connects …
- Snort IDS alert for network traffic (e.…
- Yara detected AgentTesla
- Installs a global keyboard hook
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Tries to harvest and steal Putty / Wi…
- Tries to harvest and steal browser in…

Classification



Startup

- **System is w10x64**
- fattura.exe (PID: 3984 cmdline: 'C:\Users\user\Desktop\fattura.exe' MD5: AC16B512E9DE9308FA69B78AF1FAED07)
  - RegAsm.exe (PID: 2456 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe MD5: 6FD7592411112729BF6B1F2F6C34899F)
  - RegAsm.exe (PID: 864 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe MD5: 6FD7592411112729BF6B1F2F6C34899F)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Username: ": "wDrIkJ7y7Qr0a",
  "URL: ": "http://LoTLRwkC9qh4QyRRa.com",
  "To: ": "info.greatdeck@greatdeck.co",
  "ByHost: ": "mail.greatdeck.co:587",
  "Password: ": "yX93LyJE",
  "From: ": "info.greatdeck@greatdeck.co"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000003.663757971.00000000057F5000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.667877836.0000000004B03000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.669949286.00000000057F5000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.669771908.0000000005512000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000002.00000002.919344490.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 4 entries				

Unpacked PEs

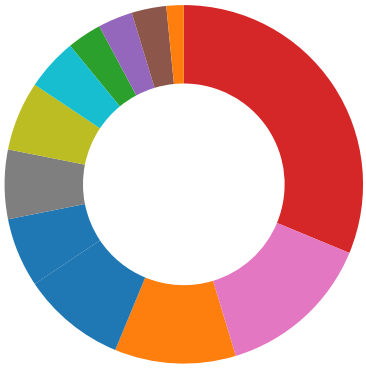
Source	Rule	Description	Author	Strings
2.2.RegAsm.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.fattura.exe.5510000.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

System Summary:

Sigma detected: RegAsm connects to smtp port

Signature Overview



- AV Detection
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- 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

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

System Summary:

Malware Analysis System Evasion:

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)

HIPS / PFW / Operating System Protection Evasion:

Maps a DLL or memory area into another process

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected AgentTesla

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal browser information (history, passwords, etc)

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

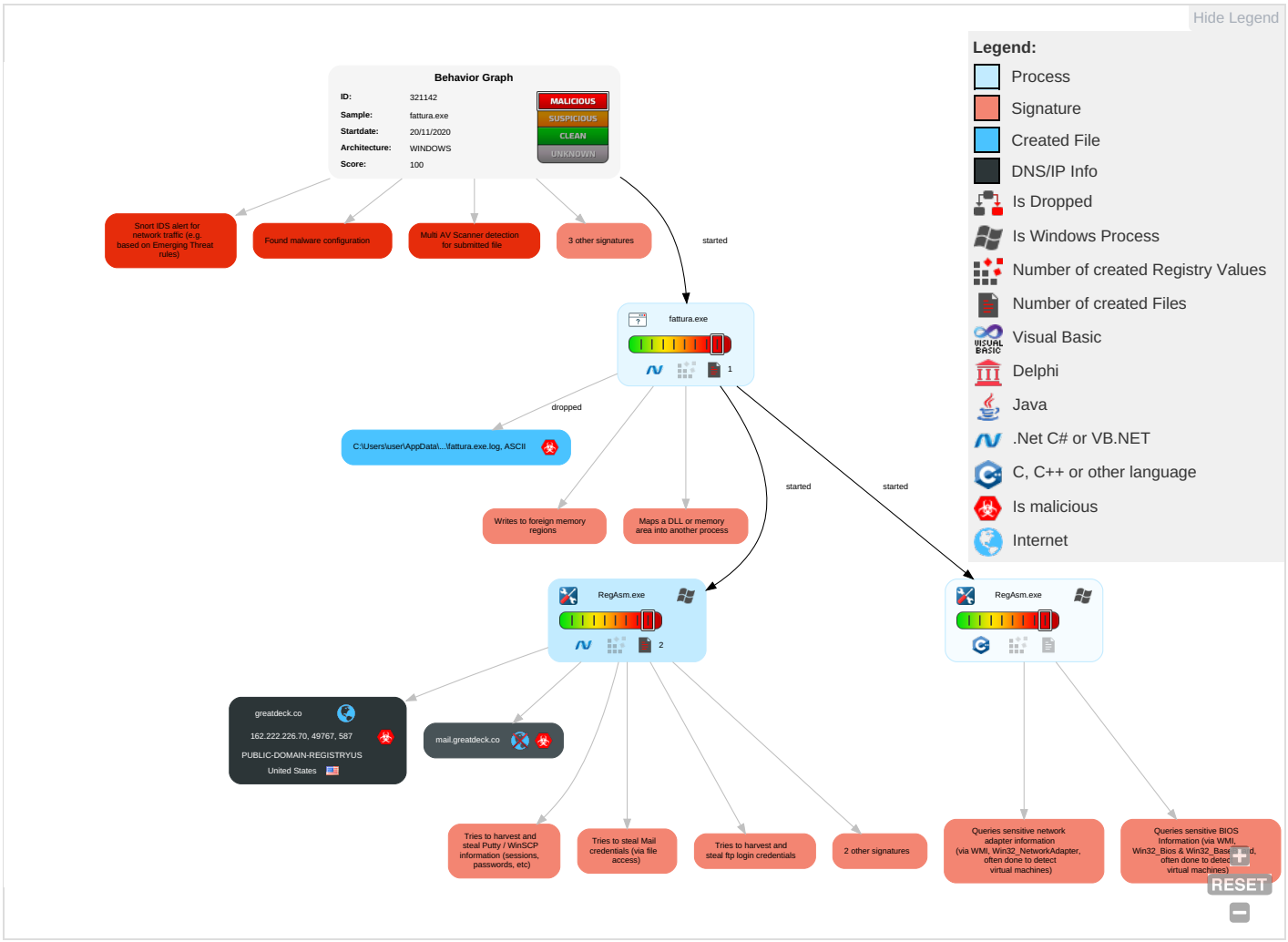
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Contr
Valid Accounts	Windows Management Instrumentation 2 1 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1	OS Credential Dumping 2	Account Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Process Injection 2 1 2	Obfuscated Files or Information 2	Input Capture 1 1	System Information Discovery 1 1 4	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non-Stand Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Software Packing 3	Credentials in Registry 1	Query Registry 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Application Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	DLL Side-Loading 1	NTDS	Security Software Discovery 1 1 1	Distributed Component Object Model	Input Capture 1 1	Scheduled Transfer	Application Layer Protocol 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Virtualization/Sandbox Evasion 1 3	SSH	Clipboard Data 1	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 3	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 2 1 2	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Owner/User Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Prot
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Proto

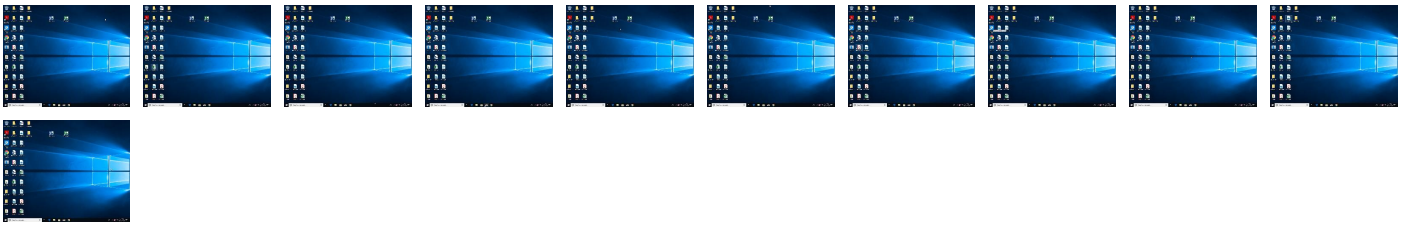
Behavior Graph



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
fattura.exe	25%	ReversingLabs	ByteCode-MSIL.Infostealer.DarkStealer	
fattura.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.RegAsm.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
0.2.fattura.exe.5510000.1.unpack	100%	Avira	HEUR/AGEN.1138205		Download File

Domains

Source	Detection	Scanner	Label	Link
greatdeck.co	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://greatdeck.co	0%	Avira URL Cloud	safe	
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	
http://mail.greatdeck.co	0%	Avira URL Cloud	safe	
http://LoTLRwkC9qh4QyRRa.comP	0%	Avira URL Cloud	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://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://Bvcujr.com	0%	Avira URL Cloud	safe	
http://LoTLRwkC9qh4QyRRa.com	0%	Avira URL Cloud	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

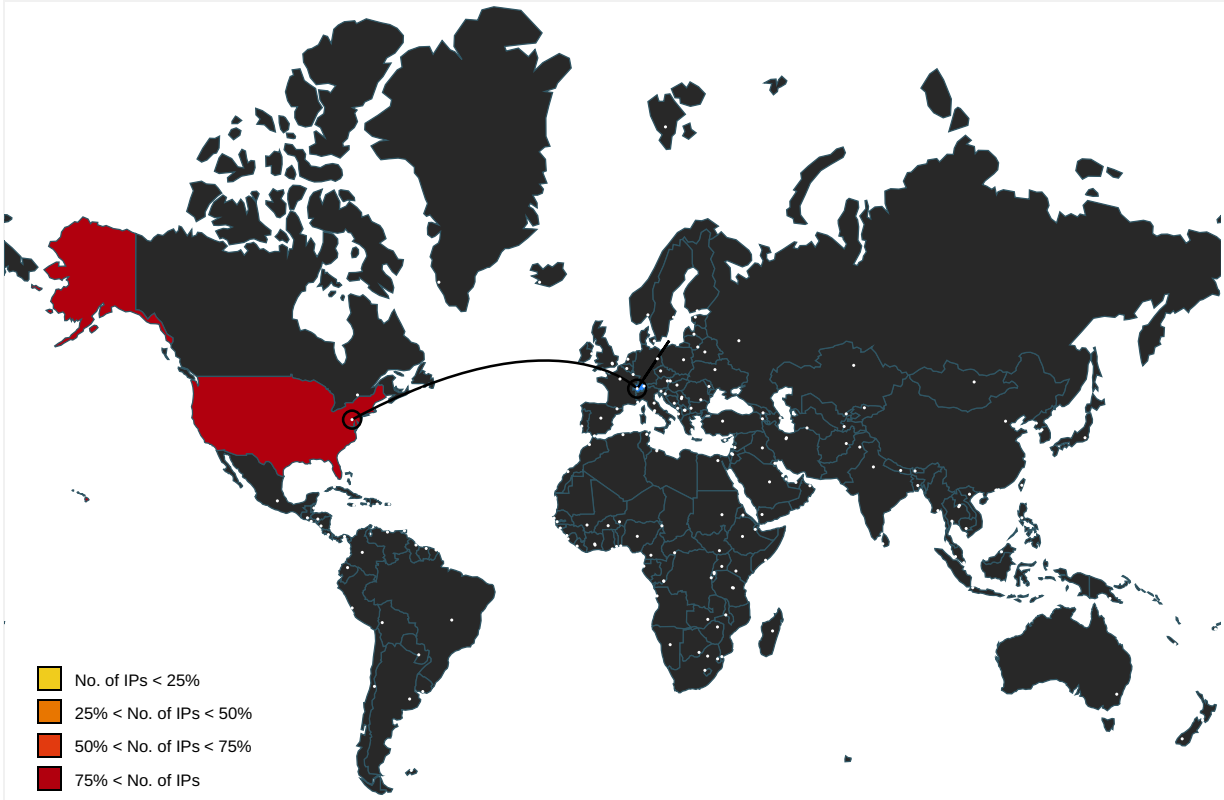
Name	IP	Active	Malicious	Antivirus Detection	Reputation
greatdeck.co	162.222.226.70	true	true	• 1%, Virustotal, Browse	unknown
mail.greatdeck.co	unknown	unknown	true		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://greatdeck.co	RegAsm.exe, 00000002.00000002.920950784.0000000002DDA000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://127.0.0.1:HTTP/1.1	RegAsm.exe, 00000002.00000002.920493622.0000000002A81000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://DynDns.comDynDNS	RegAsm.exe, 00000002.00000002.920493622.0000000002A81000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://mail.greatdeck.co	RegAsm.exe, 00000002.00000002.920950784.0000000002DDA000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://LoTLRwkC9qh4QyRRa.comP	RegAsm.exe, 00000002.00000002.920893237.0000000002D98000.00000004.00000001.sdmp	false	• Avira URL Cloud: 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, 00000002.00000002.920493622.0000000002A81000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.telegram.org/bot%telegramapi%/	fattura.exe, 00000000.00000003.663757971.00000000057F5000.00000004.00000001.sdmp, RegAsm.exe, 00000002.00000002.919344490.0000000000402000.00000040.00000001.sdmp	false		high
http://https://api.telegram.org/bot%telegramapi%/sendDocumentdocument----------x	RegAsm.exe, 00000002.00000002.920493622.0000000002A81000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	fattura.exe, 00000000.00000003.663757971.00000000057F5000.00000004.00000001.sdmp, RegAsm.exe, 00000002.00000002.919344490.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://Bvcujr.com	RegAsm.exe, 00000002.00000002.920493622.0000000002A81000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://LoTLRwkC9qh4QyRRa.com	RegAsm.exe, 00000002.00000002.920893237.0000000002D98000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://api.ipify.orgGETMozilla/5.0	RegAsm.exe, 00000002.00000002.920493622.0000000002A81000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.222.226.70	unknown	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	321142
Start date:	20.11.2020
Start time:	12:35:24
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 53s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	fattura.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:	16
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@5/1@2/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.4% (good quality ratio 0.3%) • Quality average: 68% • Quality standard deviation: 24.6%
HCA Information:	• Successful, ratio: 100% • 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): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 52.147.198.201, 104.43.139.144, 104.43.193.48, 51.104.139.180, 52.155.217.156, 20.54.26.129, 205.185.216.42, 205.185.216.10, 95.101.22.134, 95.101.22.125 • Excluded domains from analysis (whitelisted): displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, arc.msn.com.nsatc.net, db3p-ris-pf-prod-atm.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, cds.d2s7q6s2.hwcdn.net, a1449.dscg2.akamai.net, arc.msn.com, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus16.cloudapp.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, ris.api.iris.microsoft.com, umwatsonrouting.trafficmanager.net, audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.trafficmanager.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • 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

Time	Type	Description
12:36:29	API Interceptor	840x Sleep call for process: RegAsm.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
162.222.226.70	Zahlung.exe	Get hash	malicious	Browse	
	Zahlung.exe	Get hash	malicious	Browse	
	Lieferadresse.exe	Get hash	malicious	Browse	
	Shipment address.exe	Get hash	malicious	Browse	
	dettagli di pagamento.exe	Get hash	malicious	Browse	
	Zahlungskopie.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.AdWare.Amonetize.arhz.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.Siggen11.2816.22071.exe	Get hash	malicious	Browse	
	http://https://spark.adobe.com/page/s4liZTtRbzbxD	Get hash	malicious	Browse	
	http://https://1drv.ms/u/s!Aj1pdKAYa9n0gTIji9Ijnr6xK0RL?e=HEGTEl	Get hash	malicious	Browse	
	Purchase-Order2750.html	Get hash	malicious	Browse	
	http://https://jcbintegrador.com.pe/ddgghhf67643bhjbhdfbdocpdf	Get hash	malicious	Browse	
	http://larryyoungpavlngz.com/0s	Get hash	malicious	Browse	
	http://https://linkprotect.cudasvc.com/url?a=https%3a%2f%2fartecorpus.net%2fwp-includes%2fSimplePie%2fParse%2fowa.php%2findex.html%3fl%3d_JeHFUq_VJOXK0QWHtoGYDw_Product-UserID%26%23charles.teel%40goodmanmfg.com&c=E,1,rYcxrrvcAzv2WFpvjh62IzTFJoxfScVTKXZV3aj80Afb6YKCrifwPWMgT9kxNyr4CqCYIochrADK8LmpYhp1FsBFERt0zZ1-TqzxuvkiNiScqD-ywXqZOePgJg,,&typo=1	Get hash	malicious	Browse	
	http://https://aerosurcolombia.com/AUSSIE.html	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PUBLIC-DOMAIN-REGISTRYUS	PO1.xlsx	Get hash	malicious	Browse	• 208.91.199.223
	QKLQkaCe9M.exe	Get hash	malicious	Browse	• 208.91.199.224
	Zahlung.exe	Get hash	malicious	Browse	• 162.222.226.70
	0hgHwEkIWY.exe	Get hash	malicious	Browse	• 208.91.198.143
	Swift Copy.exe	Get hash	malicious	Browse	• 208.91.199.224
	Shipping Details_PDF.exe	Get hash	malicious	Browse	• 208.91.199.225
	Zahlung.exe	Get hash	malicious	Browse	• 162.222.226.70
	Lieferadresse.exe	Get hash	malicious	Browse	• 162.222.226.70
	RFQ_SMKM19112020.xlsx	Get hash	malicious	Browse	• 208.91.199.224
	Order List.xlsx	Get hash	malicious	Browse	• 208.91.199.225
	Shipping doc.pdf.exe	Get hash	malicious	Browse	• 208.91.198.143
	OrV86zxFWHW1j0f.exe	Get hash	malicious	Browse	• 208.91.199.224
	XDMBhLJxD1Qf7JW.exe	Get hash	malicious	Browse	• 208.91.199.224
	me4qssWAMQ.exe	Get hash	malicious	Browse	• 208.91.199.225
	Vd58qg0dhp.exe	Get hash	malicious	Browse	• 208.91.199.223
	15egpuWfT3.exe	Get hash	malicious	Browse	• 208.91.199.224
	PO_287104.exe	Get hash	malicious	Browse	• 208.91.198.225
	Machine drawing.exe	Get hash	malicious	Browse	• 199.79.63.24
	Shipping Details.exe	Get hash	malicious	Browse	• 208.91.198.143
	Wrong Transfer Payment - Chk Clip Copy.exe	Get hash	malicious	Browse	• 208.91.199.223

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\fattura.exe.log	
Process:	C:\Users\user\Desktop\fattura.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	315
Entropy (8bit):	5.350410246151501
Encrypted:	false
SSDEEP:	6:Q3La/xwcE73FKDLIP12MUAvvr3tDLIP12MUAvvR+uTL2LDY3U21v:Q3La/hg1KDLI4M9tDLI4MWuPk21v
MD5:	EE0BB4B63A030A0BF7087CB0AEBD07BC
SHA1:	9A4ADFB6336E22D49503B4B99FFC25A7882AE202
SHA-256:	6CBBAF20B7871B931A8A0B1D54890DC0E6C9ED78E7DEC5E2AB2F6D12DF349DFF
SHA-512:	47644A669A15A83D0BAA1F801BB34E36B1F8FE700E5C7A4396D684FE85AFFF6B32F511AEDD0E304DB48383E04A5044CA1B313D559737F5CD967CC00F8FDFC38B
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.86086603352849
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	fattura.exe
File size:	618496
MD5:	ac16b512e9de9308fa69b78af1faed07
SHA1:	85eff7055833458712baa0facf48269317d38bff
SHA256:	2112f6c6abb4fe84e62fd5ff70f880413b3e54610535b1bd1e5d9ca64d6206f5
SHA512:	9c325aa0df68ccbc8398ad3bd181c7084d88ee7ee51b49639f730bbdbd15f3fbcf1fb3361701d411ccbf70e1b599a9a854f37e2e1d1a37cb5474cefaa5dee4a0
SSDEEP:	12288:IvFCnJw4N72vng/saho7+NeB0uUo8ndBuymcGuBQqvlQOx:8FuiQy/GHhfG0uUUyfGuBQ0lQO
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....y._.....h..... .....@.. .....G.....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4987ce
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5FB779C3 [Fri Nov 20 08:09:39 2020 UTC]

General

TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
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:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x9877c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x9a000	0x242	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x9c000	0xc	.reloc
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	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x967d4	0x96800	False	0.918727938123	data	7.86592227679	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x9a000	0x242	0x400	False	0.310546875	data	3.56952524932	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x9c000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_MANIFEST	0x9a058	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

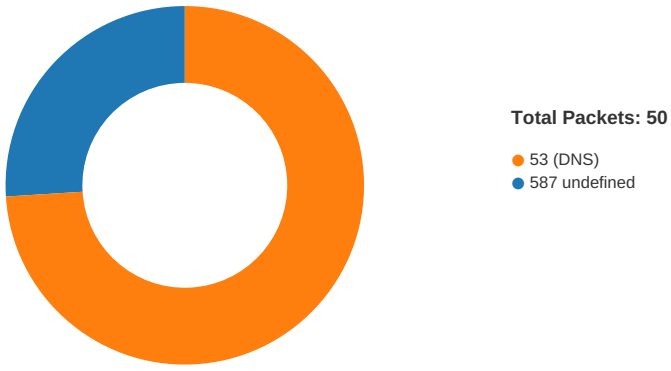
DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/20/20-12:37:56.843422	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49767	587	192.168.2.4	162.222.226.70

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 12:37:55.461395025 CET	49767	587	192.168.2.4	162.222.226.70
Nov 20, 2020 12:37:55.610898018 CET	587	49767	162.222.226.70	192.168.2.4
Nov 20, 2020 12:37:55.611006021 CET	49767	587	192.168.2.4	162.222.226.70
Nov 20, 2020 12:37:55.984190941 CET	587	49767	162.222.226.70	192.168.2.4
Nov 20, 2020 12:37:55.984671116 CET	49767	587	192.168.2.4	162.222.226.70

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 12:37:56.124622107 CET	587	49767	162.222.226.70	192.168.2.4
Nov 20, 2020 12:37:56.125966072 CET	49767	587	192.168.2.4	162.222.226.70
Nov 20, 2020 12:37:56.265924931 CET	587	49767	162.222.226.70	192.168.2.4
Nov 20, 2020 12:37:56.266896963 CET	49767	587	192.168.2.4	162.222.226.70
Nov 20, 2020 12:37:56.408432961 CET	587	49767	162.222.226.70	192.168.2.4
Nov 20, 2020 12:37:56.409766912 CET	49767	587	192.168.2.4	162.222.226.70
Nov 20, 2020 12:37:56.549482107 CET	587	49767	162.222.226.70	192.168.2.4
Nov 20, 2020 12:37:56.550213099 CET	49767	587	192.168.2.4	162.222.226.70
Nov 20, 2020 12:37:56.693073988 CET	587	49767	162.222.226.70	192.168.2.4
Nov 20, 2020 12:37:56.693809032 CET	49767	587	192.168.2.4	162.222.226.70
Nov 20, 2020 12:37:56.834487915 CET	587	49767	162.222.226.70	192.168.2.4
Nov 20, 2020 12:37:56.834531069 CET	587	49767	162.222.226.70	192.168.2.4
Nov 20, 2020 12:37:56.843421936 CET	49767	587	192.168.2.4	162.222.226.70
Nov 20, 2020 12:37:56.843632936 CET	49767	587	192.168.2.4	162.222.226.70
Nov 20, 2020 12:37:56.844202995 CET	49767	587	192.168.2.4	162.222.226.70
Nov 20, 2020 12:37:56.844362974 CET	49767	587	192.168.2.4	162.222.226.70
Nov 20, 2020 12:37:56.984949112 CET	587	49767	162.222.226.70	192.168.2.4
Nov 20, 2020 12:37:56.986042976 CET	587	49767	162.222.226.70	192.168.2.4
Nov 20, 2020 12:37:56.988037109 CET	587	49767	162.222.226.70	192.168.2.4
Nov 20, 2020 12:37:57.038861990 CET	49767	587	192.168.2.4	162.222.226.70

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 12:36:16.977535009 CET	49257	53	192.168.2.4	8.8.8.8
Nov 20, 2020 12:36:17.004702091 CET	53	49257	8.8.8.8	192.168.2.4
Nov 20, 2020 12:36:17.671792030 CET	62389	53	192.168.2.4	8.8.8.8
Nov 20, 2020 12:36:17.698962927 CET	53	62389	8.8.8.8	192.168.2.4
Nov 20, 2020 12:36:22.558243990 CET	49910	53	192.168.2.4	8.8.8.8
Nov 20, 2020 12:36:22.585186958 CET	53	49910	8.8.8.8	192.168.2.4
Nov 20, 2020 12:36:23.203993082 CET	55854	53	192.168.2.4	8.8.8.8
Nov 20, 2020 12:36:23.231062889 CET	53	55854	8.8.8.8	192.168.2.4
Nov 20, 2020 12:36:23.943427086 CET	64549	53	192.168.2.4	8.8.8.8
Nov 20, 2020 12:36:23.970490932 CET	53	64549	8.8.8.8	192.168.2.4
Nov 20, 2020 12:36:24.589713097 CET	63153	53	192.168.2.4	8.8.8.8
Nov 20, 2020 12:36:24.616849899 CET	53	63153	8.8.8.8	192.168.2.4
Nov 20, 2020 12:36:25.329967022 CET	52991	53	192.168.2.4	8.8.8.8
Nov 20, 2020 12:36:25.365650892 CET	53	52991	8.8.8.8	192.168.2.4
Nov 20, 2020 12:36:26.143235922 CET	53700	53	192.168.2.4	8.8.8.8
Nov 20, 2020 12:36:26.170371056 CET	53	53700	8.8.8.8	192.168.2.4
Nov 20, 2020 12:36:26.951157093 CET	51726	53	192.168.2.4	8.8.8.8
Nov 20, 2020 12:36:26.978349924 CET	53	51726	8.8.8.8	192.168.2.4
Nov 20, 2020 12:36:27.769819975 CET	56794	53	192.168.2.4	8.8.8.8
Nov 20, 2020 12:36:27.796899080 CET	53	56794	8.8.8.8	192.168.2.4
Nov 20, 2020 12:36:28.403497934 CET	56534	53	192.168.2.4	8.8.8.8
Nov 20, 2020 12:36:28.432039976 CET	53	56534	8.8.8.8	192.168.2.4
Nov 20, 2020 12:36:29.310445070 CET	56627	53	192.168.2.4	8.8.8.8
Nov 20, 2020 12:36:29.337625027 CET	53	56627	8.8.8.8	192.168.2.4
Nov 20, 2020 12:36:35.495567083 CET	56621	53	192.168.2.4	8.8.8.8
Nov 20, 2020 12:36:35.522701025 CET	53	56621	8.8.8.8	192.168.2.4
Nov 20, 2020 12:36:36.298536062 CET	63116	53	192.168.2.4	8.8.8.8
Nov 20, 2020 12:36:36.325670004 CET	53	63116	8.8.8.8	192.168.2.4
Nov 20, 2020 12:36:36.802314043 CET	64078	53	192.168.2.4	8.8.8.8
Nov 20, 2020 12:36:36.829503059 CET	53	64078	8.8.8.8	192.168.2.4
Nov 20, 2020 12:36:36.985817909 CET	64801	53	192.168.2.4	8.8.8.8
Nov 20, 2020 12:36:37.012861013 CET	53	64801	8.8.8.8	192.168.2.4
Nov 20, 2020 12:36:37.792067051 CET	61721	53	192.168.2.4	8.8.8.8
Nov 20, 2020 12:36:37.819253922 CET	53	61721	8.8.8.8	192.168.2.4
Nov 20, 2020 12:36:38.596724987 CET	51255	53	192.168.2.4	8.8.8.8
Nov 20, 2020 12:36:38.624023914 CET	53	51255	8.8.8.8	192.168.2.4
Nov 20, 2020 12:36:51.646224976 CET	61522	53	192.168.2.4	8.8.8.8
Nov 20, 2020 12:36:51.682312012 CET	53	61522	8.8.8.8	192.168.2.4
Nov 20, 2020 12:36:52.176069021 CET	52337	53	192.168.2.4	8.8.8.8
Nov 20, 2020 12:36:52.203248024 CET	53	52337	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 12:36:52.608827114 CET	55046	53	192.168.2.4	8.8.8.8
Nov 20, 2020 12:36:52.644793987 CET	53	55046	8.8.8.8	192.168.2.4
Nov 20, 2020 12:36:52.972162962 CET	49612	53	192.168.2.4	8.8.8.8
Nov 20, 2020 12:36:52.999258995 CET	53	49612	8.8.8.8	192.168.2.4
Nov 20, 2020 12:36:53.243901014 CET	49285	53	192.168.2.4	8.8.8.8
Nov 20, 2020 12:36:53.270951986 CET	53	49285	8.8.8.8	192.168.2.4
Nov 20, 2020 12:36:53.451519966 CET	50601	53	192.168.2.4	8.8.8.8
Nov 20, 2020 12:36:53.487291098 CET	53	50601	8.8.8.8	192.168.2.4
Nov 20, 2020 12:36:53.873852015 CET	60875	53	192.168.2.4	8.8.8.8
Nov 20, 2020 12:36:53.900839090 CET	53	60875	8.8.8.8	192.168.2.4
Nov 20, 2020 12:36:54.320349932 CET	56448	53	192.168.2.4	8.8.8.8
Nov 20, 2020 12:36:54.355807066 CET	53	56448	8.8.8.8	192.168.2.4
Nov 20, 2020 12:36:55.006170988 CET	59172	53	192.168.2.4	8.8.8.8
Nov 20, 2020 12:36:55.041843891 CET	53	59172	8.8.8.8	192.168.2.4
Nov 20, 2020 12:36:55.609106064 CET	62420	53	192.168.2.4	8.8.8.8
Nov 20, 2020 12:36:55.636136055 CET	53	62420	8.8.8.8	192.168.2.4
Nov 20, 2020 12:36:56.182677984 CET	60579	53	192.168.2.4	8.8.8.8
Nov 20, 2020 12:36:56.220634937 CET	53	60579	8.8.8.8	192.168.2.4
Nov 20, 2020 12:37:01.435817957 CET	50183	53	192.168.2.4	8.8.8.8
Nov 20, 2020 12:37:01.463015079 CET	53	50183	8.8.8.8	192.168.2.4
Nov 20, 2020 12:37:11.987037897 CET	61531	53	192.168.2.4	8.8.8.8
Nov 20, 2020 12:37:12.014147043 CET	53	61531	8.8.8.8	192.168.2.4
Nov 20, 2020 12:37:12.183083057 CET	49228	53	192.168.2.4	8.8.8.8
Nov 20, 2020 12:37:12.210105896 CET	53	49228	8.8.8.8	192.168.2.4
Nov 20, 2020 12:37:14.860816002 CET	59794	53	192.168.2.4	8.8.8.8
Nov 20, 2020 12:37:14.899347067 CET	53	59794	8.8.8.8	192.168.2.4
Nov 20, 2020 12:37:46.295819998 CET	55916	53	192.168.2.4	8.8.8.8
Nov 20, 2020 12:37:46.323276043 CET	53	55916	8.8.8.8	192.168.2.4
Nov 20, 2020 12:37:47.459675074 CET	52752	53	192.168.2.4	8.8.8.8
Nov 20, 2020 12:37:47.505688906 CET	53	52752	8.8.8.8	192.168.2.4
Nov 20, 2020 12:37:55.364053965 CET	60542	53	192.168.2.4	8.8.8.8
Nov 20, 2020 12:37:55.399847984 CET	53	60542	8.8.8.8	192.168.2.4
Nov 20, 2020 12:37:55.411382914 CET	60689	53	192.168.2.4	8.8.8.8
Nov 20, 2020 12:37:55.446657896 CET	53	60689	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 20, 2020 12:37:55.364053965 CET	192.168.2.4	8.8.8.8	0x256f	Standard query (0)	mail.greatdeck.co	A (IP address)	IN (0x0001)
Nov 20, 2020 12:37:55.411382914 CET	192.168.2.4	8.8.8.8	0xd81d	Standard query (0)	mail.greatdeck.co	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 20, 2020 12:37:55.399847984 CET	8.8.8.8	192.168.2.4	0x256f	No error (0)	mail.great deck.co	greatdeck.co		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 12:37:55.399847984 CET	8.8.8.8	192.168.2.4	0x256f	No error (0)	greatdeck.co		162.222.226.70	A (IP address)	IN (0x0001)
Nov 20, 2020 12:37:55.446657896 CET	8.8.8.8	192.168.2.4	0xd81d	No error (0)	mail.great deck.co	greatdeck.co		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 12:37:55.446657896 CET	8.8.8.8	192.168.2.4	0xd81d	No error (0)	greatdeck.co		162.222.226.70	A (IP address)	IN (0x0001)

SMTP Packets

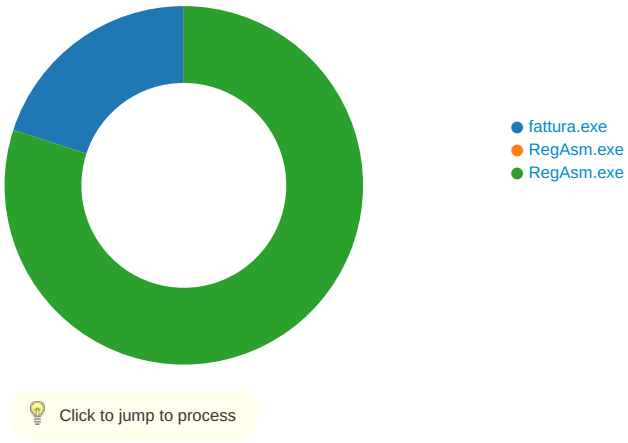
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Nov 20, 2020 12:37:55.984190941 CET	587	49767	162.222.226.70	192.168.2.4	220-bh-37.webhostbox.net ESMTP Exim 4.93 #2 Fri, 20 Nov 2020 11:37:55 +0000 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Nov 20, 2020 12:37:55.984671116 CET	49767	587	192.168.2.4	162.222.226.70	EHLO 813848

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Nov 20, 2020 12:37:56.124622107 CET	587	49767	162.222.226.70	192.168.2.4	250-bh-37.webhostbox.net Hello 813848 [84.17.52.25] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Nov 20, 2020 12:37:56.125966072 CET	49767	587	192.168.2.4	162.222.226.70	AUTH login aW5mby5ncmVhdGRlY2tAZ3JlYXRkZWNrLmNv
Nov 20, 2020 12:37:56.265924931 CET	587	49767	162.222.226.70	192.168.2.4	334 UGFzc3dvcmQ6
Nov 20, 2020 12:37:56.408432961 CET	587	49767	162.222.226.70	192.168.2.4	235 Authentication succeeded
Nov 20, 2020 12:37:56.409766912 CET	49767	587	192.168.2.4	162.222.226.70	MAIL FROM:<info.greatdeck@greatdeck.co>
Nov 20, 2020 12:37:56.549482107 CET	587	49767	162.222.226.70	192.168.2.4	250 OK
Nov 20, 2020 12:37:56.550213099 CET	49767	587	192.168.2.4	162.222.226.70	RCPT TO:<info.greatdeck@greatdeck.co>
Nov 20, 2020 12:37:56.693073988 CET	587	49767	162.222.226.70	192.168.2.4	250 Accepted
Nov 20, 2020 12:37:56.693809032 CET	49767	587	192.168.2.4	162.222.226.70	DATA
Nov 20, 2020 12:37:56.834531069 CET	587	49767	162.222.226.70	192.168.2.4	354 Enter message, ending with "." on a line by itself
Nov 20, 2020 12:37:56.844362974 CET	49767	587	192.168.2.4	162.222.226.70	.
Nov 20, 2020 12:37:56.988037109 CET	587	49767	162.222.226.70	192.168.2.4	250 OK id=1kg4jk-000fJo-Os

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: fattura.exe PID: 3984 Parent PID: 5820

General

Start time:	12:36:16
Start date:	20/11/2020
Path:	C:\Users\user\Desktop\fattura.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\fattura.exe'
Imagebase:	0xb00000
File size:	618496 bytes

MD5 hash:	AC16B512E9DE9308FA69B78AF1FAED07
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: 00000000.00000003.663757971.00000000057F5000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.667877836.0000000004B03000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.669949286.00000000057F5000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.669771908.0000000005512000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\fattura.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D48C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\fattura.exe.log	unknown	315	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 33	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_3	success or wait	1	6D48C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D155705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D15CA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0B03DE	ReadFile

Analysis Process: RegAsm.exe PID: 2456 Parent PID: 3984

General

Start time:	12:36:21
Start date:	20/11/2020
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Imagebase:	0x330000
File size:	64616 bytes
MD5 hash:	6FD7592411112729BF6B1F2F6C34899F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: RegAsm.exe PID: 864 Parent PID: 3984

General

Start time:	12:36:21
Start date:	20/11/2020
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Imagebase:	0x650000
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: 00000002.00000002.919344490.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.920493622.0000000002A81000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	moderate

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	6D17CF06	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	6D17CF06	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	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	8173	end of file	1	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D155705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4095	success or wait	1	6D15CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	8173	end of file	1	6D15CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D15CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BFC1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BFC1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4096	success or wait	1	6BFC1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4096	end of file	1	6BFC1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4095	success or wait	1	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	8173	end of file	1	6D155705	unknown
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6BFC1B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\5f99d503-92fb-4a4a-b437-bfdf082b471f	unknown	4096	success or wait	1	6BFC1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6BFC1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6BFC1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6BFC1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6BFC1B4F	ReadFile

Disassembly

Code Analysis