ID: 632619
Sample Name: Fattura Proforma (C) n 31.exe
Cookbook: default.jbs
Time: 20:34:50
Date: 23/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

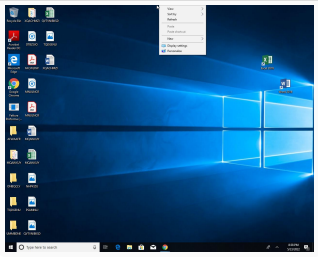
Windows Analysis Report

Fattura Proforma (C) n 31.exe

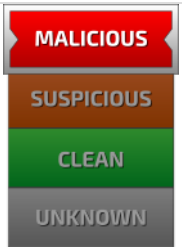
Overview

General Information

Sample Name:	Fattura Proforma (C) n 31.exe
Analysis ID:	632619
MD5:	f9f9551391f1537..
SHA1:	c81a7c0b39cd21..
SHA256:	6c2b7249173f72..
Tags:	agenttesla exe
Infos:	



Detection



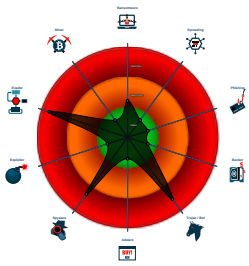
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Tries to steal Mail credentials (via fi…
- Tries to harvest and steal ftp login c…
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…
- Yara detected Generic Downloader

Classification



Process Tree

- **System is w10x64**
- Fattura Proforma (C) n 31.exe (PID: 6892 cmdline: "C:\Users\user\Desktop\Fattura Proforma (C) n 31.exe" MD5: F9F9551391F15378D87182B087A0984E)
  - Fattura Proforma (C) n 31.exe (PID: 4984 cmdline: C:\Users\user\Desktop\Fattura Proforma (C) n 31.exe MD5: F9F9551391F15378D87182B087A0984E)
  - Fattura Proforma (C) n 31.exe (PID: 6268 cmdline: C:\Users\user\Desktop\Fattura Proforma (C) n 31.exe MD5: F9F9551391F15378D87182B087A0984E)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "Username": "Werner.Wagner@celoric.com",
  "Password": "LP#qETg8",
  "Host": "smtp.celoric.com"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000000.469102375.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000007.00000000.469102375.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000007.00000000.469793315.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000007.00000000.469793315.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000001.00000002.474516321.0000000003EC1000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 19 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.Fattura Proforma (C) n 31.exe.4038208.3.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.Fattura Proforma (C) n 31.exe.4038208.3.raw.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
1.2.Fattura Proforma (C) n 31.exe.4038208.3.raw.unpack	JoeSecurity_GenericDownloader_1	Yara detected Generic Downloader	Joe Security	
1.2.Fattura Proforma (C) n 31.exe.4038208.3.raw.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x30c22:$s1: get_kbok • 0x31565:$s2: get_CHoo • 0x3219f:$s3: set_passwordIsSet • 0x30a26:$s4: get_enableLog • 0x3509a:$s8: torbrowser • 0x33a76:$s10: logins • 0x333ee:$s11: credential • 0x2fe47:$g1: get_Clipboard • 0x2fe55:$g2: get_Keyboard • 0x2fe62:$g3: get_Password • 0x31404:$g4: get_CtrlKeyDown • 0x31414:$g5: get_ShiftKeyDown • 0x31425:$g6: get_AltKeyDown
1.2.Fattura Proforma (C) n 31.exe.40023e8.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 49 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking

Yara detected Generic Downloader

System Summary

Malicious sample detected (through community Yara rule)

.NET source code contains very large array initializations

Data Obfuscation

.NET source code contains potential unpacker

Malware Analysis System Evasion

Yara detected AntiVM3

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

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

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

HIPS / PFW / Operating System Protection Evasion

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected AgentTesla

Tries to steal Mail credentials (via file / registry access)

Tries to harvest and steal ftp login credentials

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

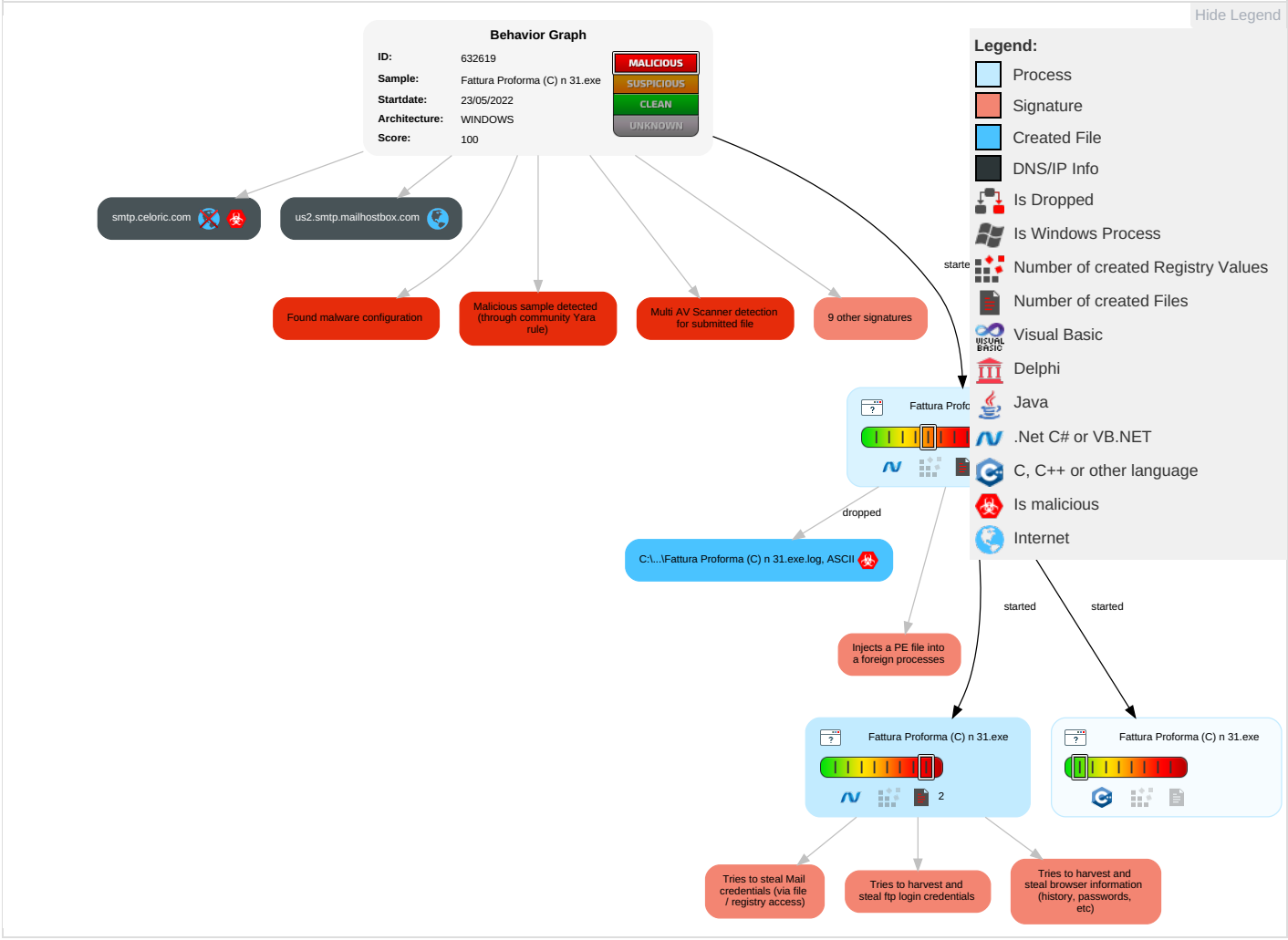
Remote Access Functionality

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	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 1 1 Windows Management Instrumentation	Path Interception	1 1 1 Process Injection	1 Masquerading	2 OS Credential Dumping	2 1 1 Security Software Discovery	Remote Services	1 Email Collection	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	LSASS Memory	1 Process Discovery	Remote Desktop Protocol	1 1 Archive Collected Data	Exfiltration Over Bluetooth	1 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 3 1 Virtualization/Sandbox Evasion	Security Account Manager	1 3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	2 Data from Local System	Automated Exfiltration	1 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 1 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 1 3 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 Obfuscated Files or Information	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 3 Software Packing	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Fattura Proforma (C) n 31.exe	25%	Virustotal		Browse
Fattura Proforma (C) n 31.exe	20%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
Fattura Proforma (C) n 31.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.0.Fattura Proforma (C) n 31.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File
7.0.Fattura Proforma (C) n 31.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
7.2.Fattura Proforma (C) n 31.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
7.0.Fattura Proforma (C) n 31.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
7.0.Fattura Proforma (C) n 31.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File
7.0.Fattura Proforma (C) n 31.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
smtp.celoric.com	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://pjLE02r21MVNC.com	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://www.sajatypeworks.com2	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	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://www.carterandcone.comwity	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnT	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://smtp.celoric.com	0%	Avira URL Cloud	safe	
http://www.carterandcone.comcerE	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://https://api.ipify.org%$	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://rzfHpn.com	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.comead_	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.coma	0%	URL Reputation	safe	
http://www.tiro.comf	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	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://www.tiro.com_	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
us2.smtp.mailhostbox.com	162.222.225.29	true	false		high
smtp.celoric.com	unknown	unknown	true	• 1%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://pjLE02r21MVNC.com	Fattura Proforma (C) n 31.exe, 00000007.00000002.694265183.0000000002B0D000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://127.0.0.1:HTTP/1.1	Fattura Proforma (C) n 31.exe, 00000007.00000002.692745771.00000000027B1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	Fattura Proforma (C) n 31.exe, 00000001.00000002.478450021.0000000007012000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	Fattura Proforma (C) n 31.exe, 00000001.00000002.478450021.0000000007012000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	Fattura Proforma (C) n 31.exe, 00000001.00000002.478450021.0000000007012000.00000004.00000800.00020000.00000000.sdmp	false		high
http://DynDns.comDynDNS	Fattura Proforma (C) n 31.exe, 00000007.00000002.692745771.00000000027B1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com2	Fattura Proforma (C) n 31.exe, 00000001.00000003.427581616.0000000005E1B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	Fattura Proforma (C) n 31.exe, 00000001.00000002.478450021.0000000007012000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	Fattura Proforma (C) n 31.exe, 00000001.00000002.478450021.0000000007012000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://us2.smtp.mailhostbox.com	Fattura Proforma (C) n 31.exe, 00000007.00000002.694282802.0000000002B13000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	Fattura Proforma (C) n 31.exe, 00000007.00000002.692745771.00000000027B1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	Fattura Proforma (C) n 31.exe, 00000001.00000002.478450021.0000000007012000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.carterandcone.comwity	Fattura Proforma (C) n 31.exe, 00000001.00000003.433392009.0000000005E05000.00000004.00000800.00020000.00000000.sdmp, Fattura Proforma (C) n 31.exe, 00000001.00000003.435190604.0000000005E0D000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cnT	Fattura Proforma (C) n 31.exe, 00000001.00000003.430766280.0000000005E08000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.com	Fattura Proforma (C) n 31.exe, 00000001.00000002.478450021.0000000007012000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://smtp.celoric.com	Fattura Proforma (C) n 31.exe, 00000007.00000002.694282802.0000000002B13000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	Fattura Proforma (C) n 31.exe, 00000001.00000002.478450021.0000000007012000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.carterandcone.comcerE	Fattura Proforma (C) n 31.exe, 00000001.00000003.433392009.0000000005E05000.00000004.00000800.00020000.00000000.sdmp, Fattura Proforma (C) n 31.exe, 00000001.00000003.435302266.0000000005E0E000.00000004.00000800.00020000.00000000.sdmp, Fattura Proforma (C) n 31.exe, 00000001.00000003.435254801.0000000005E0E000.00000004.00000800.00020000.00000000.sdmp, Fattura Proforma (C) n 31.exe, 00000001.00000003.435190604.0000000005E0D000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.kr	Fattura Proforma (C) n 31.exe, 00000001.00000002.478450021.0000000007012000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.com	Fattura Proforma (C) n 31.exe, 00000001.00000003.433392009.0000000005E05000.00000004.00000800.00020000.00000000.sdmp, Fattura Proforma (C) n 31.exe, 00000001.00000003.435190604.0000000005E0D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.ipify.org%$	Fattura Proforma (C) n 31.exe, 00000007.00000002.692745771.00000000027B1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.carterandcone.coml	Fattura Proforma (C) n 31.exe, 00000001.00000002.478450021.0000000007012000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.com	Fattura Proforma (C) n 31.exe, 00000001.00000002.478450021.0000000007012000.00000004.00000800.00020000.00000000.sdmp, Fattura Proforma (C) n 31.exe, 00000001.00000003.427581616.0000000005E1B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	Fattura Proforma (C) n 31.exe, 00000001.00000002.478450021.0000000007012000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	Fattura Proforma (C) n 31.exe, 00000001.00000002.478450021.0000000007012000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	Fattura Proforma (C) n 31.exe, 00000001.00000002.478450021.0000000007012000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	Fattura Proforma (C) n 31.exe, 00000001.00000002.478450021.0000000007012000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	Fattura Proforma (C) n 31.exe, 00000001.00000002.478450021.0000000007012000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	Fattura Proforma (C) n 31.exe, 00000001.00000002.478450021.0000000007012000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	Fattura Proforma (C) n 31.exe, 00000001.00000002.478450021.0000000007012000.00000004.00000800.00020000.00000000.sdmp	false		high
http://rzfHpn.com	Fattura Proforma (C) n 31.exe, 00000007.00000002.692745771.00000000027B1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	Fattura Proforma (C) n 31.exe, 00000001.00000002.478450021.0000000007012000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	Fattura Proforma (C) n 31.exe, 00000001.00000002.478450021.0000000007012000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	Fattura Proforma (C) n 31.exe, 00000001.00000002.478450021.0000000007012000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://api.ipify.org%GETMozilla/5.0	Fattura Proforma (C) n 31.exe, 00000007.00000002.692745771.00000000027B1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://www.fonts.com	Fattura Proforma (C) n 31.exe, 00000001.00000002.478450021.0000000007012000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	Fattura Proforma (C) n 31.exe, 00000001.00000002.478450021.0000000007012000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comead_	Fattura Proforma (C) n 31.exe, 00000001.00000003.433392009.0000000005E05000.00000004.00000800.00020000.00000000.sdmp, Fattura Proforma (C) n 31.exe, 00000001.00000003.435302266.0000000005E0E000.00000004.00000800.00020000.00000000.sdmp, Fattura Proforma (C) n 31.exe, 00000001.00000003.435254801.0000000005E0E000.00000004.00000800.00020000.00000000.sdmp, Fattura Proforma (C) n 31.exe, 00000001.00000003.435190604.0000000005E0D000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.sajatypeworks.coma	Fattura Proforma (C) n 31.exe, 00000001.00000003.427581616.0000000005E1B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.comf	Fattura Proforma (C) n 31.exe, 00000001.00000003.430955587.0000000005E08000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	Fattura Proforma (C) n 31.exe, 00000001.00000002.478450021.0000000007012000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	Fattura Proforma (C) n 31.exe, 00000001.00000002.478450021.0000000007012000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	Fattura Proforma (C) n 31.exe, 00000001.00000002.478450021.0000000007012000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	Fattura Proforma (C) n 31.exe, 00000001.00000002.474516321.0000000003EC1000.00000004.00000800.00020000.00000000.sdmp, Fattura Proforma (C) n 31.exe, 00000007.00000000.469102375.0000000402000.00000040.00000400.00020000.00000000.sdmp, Fattura Proforma (C) n 31.exe, 00000007.00000000.467636633.0000000004020000.00000040.00000400.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.com_	Fattura Proforma (C) n 31.exe, 00000001.00000003.430955587.0000000005E08000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	632619
Start date and time: 23/05/202220:34:50	2022-05-23 20:34:50 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 47s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Fattura Proforma (C) n 31.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:	23
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@2/0
EGA Information:	• Successful, ratio: 66.7%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): www.bing.com, ris.api.iris.microsoft.com, client.wns.windows.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, ctldl.windowsupdate.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Execution Graph export aborted for target Fattura Proforma (C) n 31.exe, PID 4984 because there are no executed function
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.

Simulations

Behavior and APIs

Time	Type	Description
20:36:12	API Interceptor	601x Sleep call for process: Fattura Proforma (C) n 31.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Fattura Proforma (C) n 31.exe.log

Process:	C:\Users\user\Desktop\Fattura Proforma (C) n 31.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1308
Entropy (8bit):	5.345811588615766
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84FsXE8:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzu
MD5:	2E016B886BDB8389D2DD0867BE55F87B
SHA1:	25D28EF2ACBB41764571E06E11BF4C05DD0E2F8B
SHA-256:	1D037CF00A8849E6866603297F85D3DABE09535E72EDD2636FB7D0F6C7DA3427
SHA-512:	C100729153954328AA2A77EECB2A3CBD03CB7E8E23D736000F890B17AAA50BA87745E30FB9E2B0D61E16DCA45694C79B4CE09B9F4475220BEB38CAEA546CFC2A
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",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..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.897680685593599
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 Proforma (C) n 31.exe
File size:	962560
MD5:	f9f9551391f15378d87182b087a0984e
SHA1:	c81a7c0b39cd213adb431813114cecd856190411
SHA256:	6c2b7249173f7259dad5915a88a0b571644fed8140cd0268a88395e2308a44e4
SHA512:	fb1319234b9a521e229247481fd7d9679802173f88391ac09be690467f243bd99e92dfe5b78f1eea01ceea247646c25cd3547fa879d98ccda2ff422104625a10
SSDEEP:	12288:02iN4d+uMWLHMHdhmePHbo6P5HajTUM5TdwG1VgUbN4FmJEirtm:01diCPhTnHwcGcgE
TLSH:	1F250221B2E58B49E9BE8BF4893052902776BD1AB5B0E61F4CD234CD3931B06DB51F63
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...n..b.....0.....6.... .....@.. ....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4ec236
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:	0x628B966E [Mon May 23 14:13:02 2022 UTC]
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

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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xec1e4	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xee000	0x68c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xf0000	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
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	0xea23c	0xea400	False	0.91296608191	data	7.90435959734	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xee000	0x68c	0x800	False	0.34521484375	data	3.60282141071	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xf0000	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_VERSION	0xee090	0x3fc	data		
RT_MANIFEST	0xee49c	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright Delaware Technical Community College 2016
Assembly Version	1.0.0.0
InternalName	RemotingXmlConfigFileD.exe
FileVersion	1.0.0.0
CompanyName	Delaware Technical Community College
LegalTrademarks	
Comments	
ProductName	Census Project
ProductVersion	1.0.0.0
FileDescription	Census Project
OriginalFilename	RemotingXmlConfigFileD.exe

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 23, 2022 20:38:04.784327984 CEST	56523	53	192.168.2.5	8.8.8.8
May 23, 2022 20:38:04.984673977 CEST	53	56523	8.8.8.8	192.168.2.5
May 23, 2022 20:38:04.988503933 CEST	58904	53	192.168.2.5	8.8.8.8
May 23, 2022 20:38:05.020514011 CEST	53	58904	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 23, 2022 20:38:04.784327984 CEST	192.168.2.5	8.8.8.8	0x215d	Standard query (0)	smtp.celoric.com	A (IP address)	IN (0x0001)
May 23, 2022 20:38:04.988503933 CEST	192.168.2.5	8.8.8.8	0x8e83	Standard query (0)	smtp.celoric.com	A (IP address)	IN (0x0001)

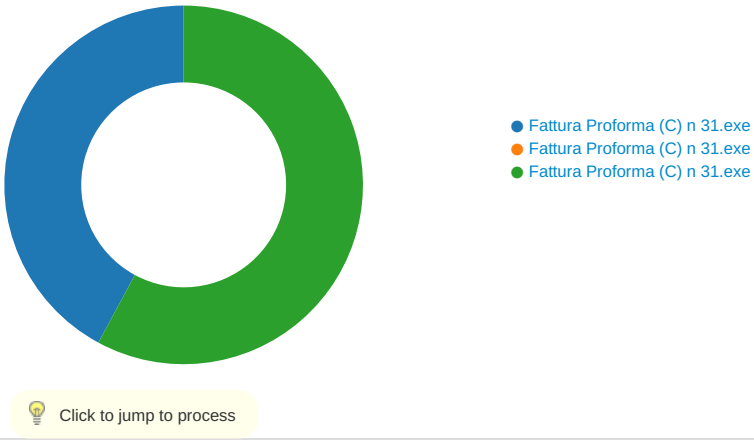
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 23, 2022 20:38:04.984673977 CEST	8.8.8.8	192.168.2.5	0x215d	No error (0)	smtp.celoric.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
May 23, 2022 20:38:04.984673977 CEST	8.8.8.8	192.168.2.5	0x215d	No error (0)	us2.smtp.mailhostbox.com		162.222.225.29	A (IP address)	IN (0x0001)
May 23, 2022 20:38:04.984673977 CEST	8.8.8.8	192.168.2.5	0x215d	No error (0)	us2.smtp.mailhostbox.com		208.91.198.46	A (IP address)	IN (0x0001)
May 23, 2022 20:38:04.984673977 CEST	8.8.8.8	192.168.2.5	0x215d	No error (0)	us2.smtp.mailhostbox.com		162.222.225.16	A (IP address)	IN (0x0001)
May 23, 2022 20:38:04.984673977 CEST	8.8.8.8	192.168.2.5	0x215d	No error (0)	us2.smtp.mailhostbox.com		208.91.198.38	A (IP address)	IN (0x0001)
May 23, 2022 20:38:05.020514011 CEST	8.8.8.8	192.168.2.5	0x8e83	No error (0)	smtp.celoric.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
May 23, 2022 20:38:05.020514011 CEST	8.8.8.8	192.168.2.5	0x8e83	No error (0)	us2.smtp.mailhostbox.com		208.91.198.38	A (IP address)	IN (0x0001)
May 23, 2022 20:38:05.020514011 CEST	8.8.8.8	192.168.2.5	0x8e83	No error (0)	us2.smtp.mailhostbox.com		162.222.225.29	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 23, 2022 20:38:05.020514011 CEST	8.8.8.8	192.168.2.5	0x8e83	No error (0)	us2.smtp.mailhostbox.com		162.222.225.16	A (IP address)	IN (0x0001)
May 23, 2022 20:38:05.020514011 CEST	8.8.8.8	192.168.2.5	0x8e83	No error (0)	us2.smtp.mailhostbox.com		208.91.198.46	A (IP address)	IN (0x0001)

Statistics

Behavior



System Behavior

Analysis Process: Fattura Proforma (C) n 31.exe PID: **6892**, Parent PID: **5964**

General

Target ID:	1
Start time:	20:36:00
Start date:	23/05/2022
Path:	C:\Users\user\Desktop\Fattura Proforma (C) n 31.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Fattura Proforma (C) n 31.exe"
Imagebase:	0x9e0000
File size:	962560 bytes
MD5 hash:	F9F9551391F15378D87182B087A0984E
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: 00000001.00000002.474516321.0000000003EC1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.474516321.0000000003EC1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.473781350.0000000002F02000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_zgRAT, Description: Detects zgRAT, Source: 00000001.00000002.479896370.0000000007B00000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.474922718.00000000040A8000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.474922718.00000000040A8000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

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	6E3ACF06	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	6E3ACF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Fattura Proforma (C) n 31.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E6BC78D	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 Proforma (C) n 31.exe.log	0	1308	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 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 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 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	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089"," C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6E6BC907	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	6E385705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E385705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E2E03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E38CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E2E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E2E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E2E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E2E03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E385705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E385705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D1F1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D1F1B4F	ReadFile

Analysis Process: Fattura Proforma (C) n 31.exe PID: **4984**, Parent PID: **6892**

General	
Target ID:	5
Start time:	20:36:18
Start date:	23/05/2022
Path:	C:\Users\user\Desktop\Fattura Proforma (C) n 31.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\Fattura Proforma (C) n 31.exe
Imagebase:	0x420000
File size:	962560 bytes
MD5 hash:	F9F9551391F15378D87182B087A0984E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: Fattura Proforma (C) n 31.exe PID: **6268**, Parent PID: **6892**

General	
Target ID:	7
Start time:	20:36:19
Start date:	23/05/2022
Path:	C:\Users\user\Desktop\Fattura Proforma (C) n 31.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Fattura Proforma (C) n 31.exe
Imagebase:	0x480000
File size:	962560 bytes
MD5 hash:	F9F9551391F15378D87182B087A0984E
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: 00000007.00000000.469102375.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000007.00000000.469102375.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000000.469793315.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000007.00000000.469793315.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000000.468372244.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000007.00000000.468372244.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.690586626.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000007.00000002.690586626.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000000.467636633.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000007.00000000.467636633.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.692745771.00000000027B1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000007.00000002.692745771.00000000027B1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_AgentTeslaV3, Description: AgentTeslaV3 infostealer payload, Source: 00000007.00000002.692745771.00000000027B1000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen
Reputation:	low

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	6E3ACF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6E3ACF06	unknown

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	6E385705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E385705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E2E03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E38CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E2E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E2E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E2E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E2E03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E385705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E385705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D1F1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D1F1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D1F1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D1F1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6D1F1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6D1F1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6D1F1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6D1F1B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\c3d0bcad-59c3-41fa-89dd-89b9005799af	unknown	4096	success or wait	1	6D1F1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6D1F1B4F	ReadFile

Disassembly

No disassembly