ID: 458949
Sample Name: Purchase Order to be treated on Request Imediatiely po09735-08837-8478.exe
Cookbook: default.jbs
Time: 22:23:18
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

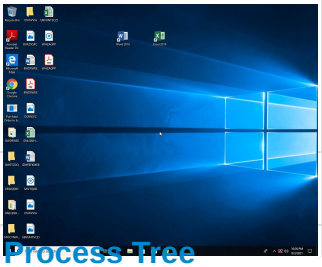
Windows Analysis Report Purchase Order to be treated …

Overview

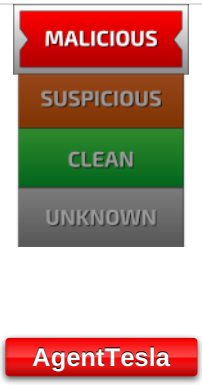
General Information

Sample Name:	Purchase Order to be treated on Request Imediatiely po09735-08837-8478.exe
Analysis ID:	458949
MD5:	acecd4bf504c791..
SHA1:	02d038f99c805f4..
SHA256:	f69b1078008e3e2.
Tags:	exe null
Infos:	

Most interesting Screenshot:



Detection



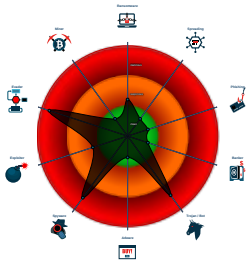
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected AgentTesla
- Yara detected AntiVM3
- .NET source code contains very larg…
- Found evasive API chain (trying to d…
- Initial sample is a PE file and has a …
- Injects a PE file into a foreign proce…
- Installs a global keyboard hook
- Machine Learning detection for dropp…

Classification



Process Tree

- **System is w10x64**
- Purchase Order to be treated on Request Imediatiely po09735-08837-8478.exe (PID: 6708 cmdline: 'C:\Users\user\Desktop\Purchase Order to be treated on Request Imediatiely po09735-08837-8478.exe' MD5: ACECD4BF504C7910E3D65CEA16C63F10)
  - schtasks.exe (PID: 7088 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\HQCVwZi' /XML 'C:\Users\user\AppData\Local\Temp\tmp8725.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 7096 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - Purchase Order to be treated on Request Imediatiely po09735-08837-8478.exe (PID: 7140 cmdline: C:\Users\user\Desktop\Purchase Order to be treated on Request Imediatiely po09735-08837-8478.exe MD5: ACECD4BF504C7910E3D65CEA16C63F10)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Username": "sales1@ashtavinayaka.com",
  "Password": "123456789",
  "Host": "smtpout.secureserver.net"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.919985835.00000000036A7000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.676811837.00000000034D1000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000007.00000002.919719729.0000000003621000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000007.00000002.919719729.000000000362 1000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000000.00000002.678480420.00000000044D 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 8 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
7.2.Purchase Order to be treated on Request Imediatiely po09735-08837-8478.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
7.2.Purchase Order to be treated on Request Imediatiely po09735-08837-8478.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.Purchase Order to be treated on Request Imediatiely po09735-08837-8478.exe.4781128.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.Purchase Order to be treated on Request Imediatiely po09735-08837-8478.exe.4781128.2.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.Purchase Order to be treated on Request Imediatiely po09735-08837-8478.exe.4781128.2.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 5 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Machine Learning detection for sample

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

System Summary:

.NET source code contains very large strings

Initial sample is a PE file and has a suspicious name

Boot Survival:

Uses schtasks.exe or at.exe to add and modify task schedules

Malware Analysis System Evasion:

Yara detected AntiVM3

Found evasive API chain (trying to detect sleep duration tampering with parallel thread)

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

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

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

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

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:

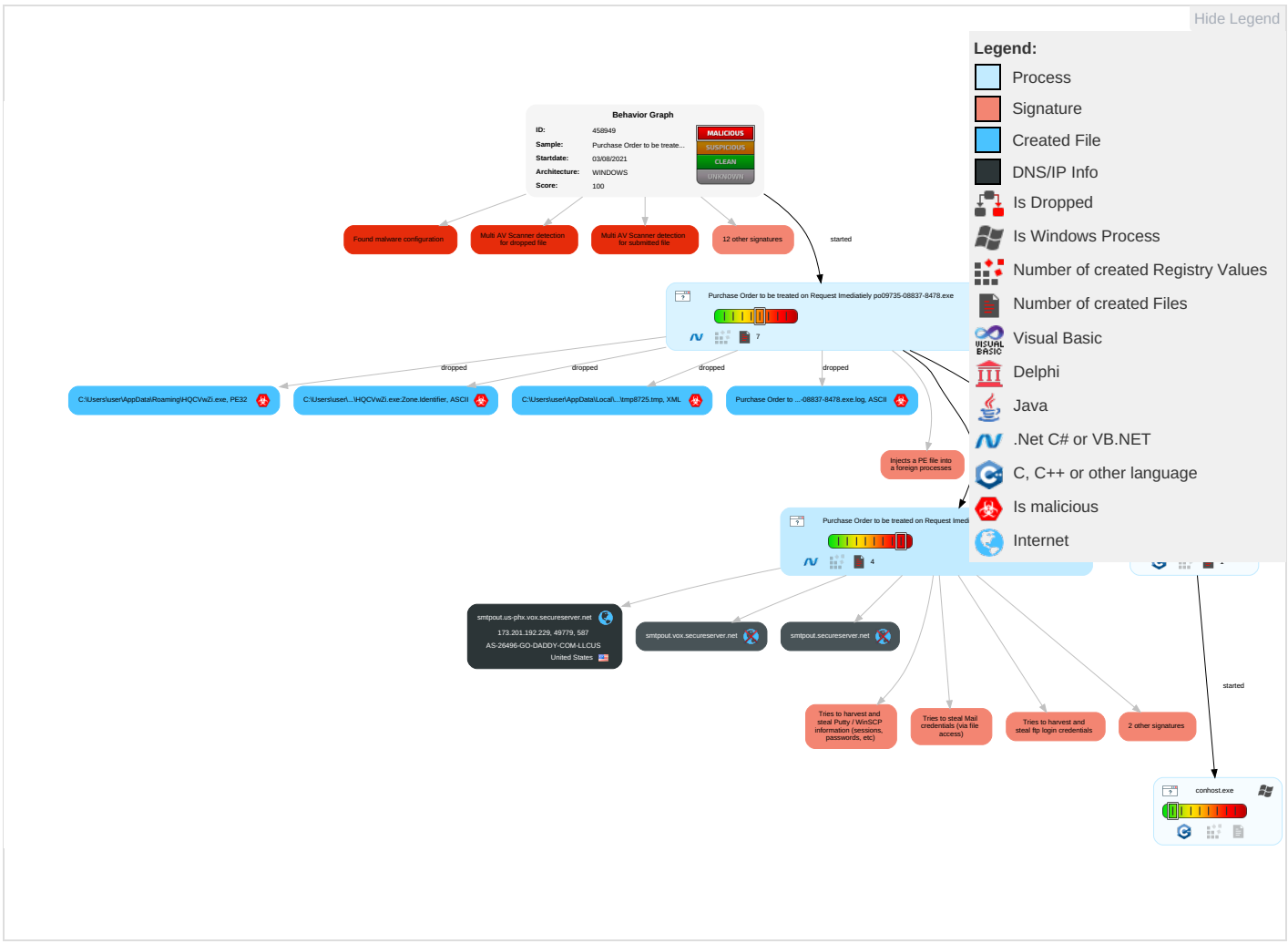
Yara detected AgentTesla

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Valid Accounts	Windows Management Instrumentation 2 1 1	Scheduled Task/Job 1	Access Token Manipulation 1	Disable or Modify Tools 1 1	OS Credential Dumping 2	Account Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Network Medium
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Process Injection 1 1 2	Obfuscated Files or Information 3 1	Input Capture 1 1 1	File and Directory Discovery 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth
Domain Accounts	Scheduled Task/Job 1	Logon Script (Windows)	Scheduled Task/Job 1	Software Packing 2	Credentials in Registry 1	System Information Discovery 1 1 4	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltr
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Masquerading 1	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture 1 1 1	Scheduled Trans
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Virtualization/Sandbox Evasion 1 3 1	LSA Secrets	Security Software Discovery 3 1 1	SSH	Keylogging	Data Transfer Siz Limits
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Access Token Manipulation 1	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over Channel
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 1 2	DCSync	Virtualization/Sandbox Evasion 1 3 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Proto
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encry Non-C2 Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encr Non-C2 Protocol
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	Remote System Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obf Non-C2 Protocol

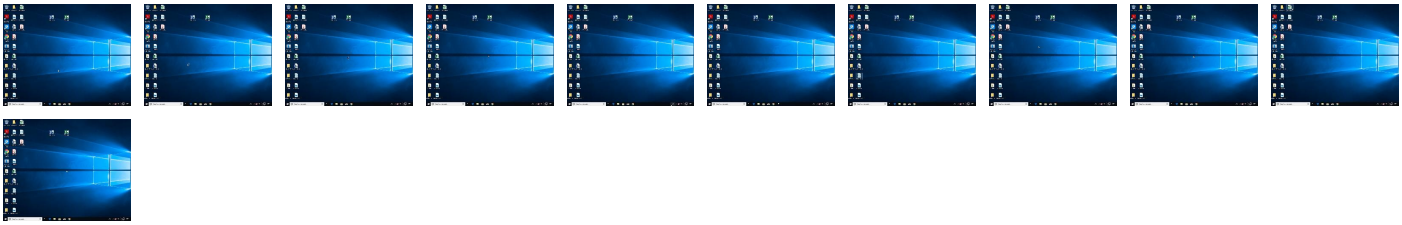
Behavior Graph



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
Purchase Order to be treated on Request Imediatiely po09735-08837-8478.exe	51%	Virustotal		Browse
Purchase Order to be treated on Request Imediatiely po09735-08837-8478.exe	49%	Metadefender		Browse
Purchase Order to be treated on Request Imediatiely po09735-08837-8478.exe	79%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
Purchase Order to be treated on Request Imediatiely po09735-08837-8478.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\HQCVwZi.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\HQCVwZi.exe	49%	Metadefender		Browse
C:\Users\user\AppData\Roaming\HQCVwZi.exe	79%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.2.Purchase Order to be treated on Request Imediatiely po09735-08837-8478.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cnLog_	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://BPvj8ZMVWAgX.com	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.fontbureau.comalsF	0%	URL Reputation	safe	
http://www.founder.com.cn/cnD	0%	Avira URL Cloud	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.fontbureau.comgrita	0%	URL Reputation	safe	
http://www.fonts.comic	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/MI1	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnl-gy	0%	Avira URL Cloud	safe	
http://www.carterandcone.comTC1	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.fontbureau.comalso	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/ft3	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://https://static.hummingbird.me/anime/poster_images/000/010/716/large/0fd8df1b586e60a0b1591cd8555c072f	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.carterandcone.comgy	0%	Avira URL Cloud	safe	
http://www.carterandcone.comc	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.sandoll.co.krn	0%	Avira URL Cloud	safe	
http://www.sandoll.co.krl	0%	URL Reputation	safe	
http://QpvHvE.com	0%	Avira URL Cloud	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.fontbureau.comituF	0%	URL Reputation	safe	
http://www.carterandcone.comint	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.tiro.comc	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
smtpout.us-phx.vox.secureserver.net	173.201.192.229	true	false		high
smtpout.secureserver.net	unknown	unknown	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
173.201.192.229	smtpout.us-phx.vox.secureserver.net	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	false

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458949
Start date:	03.08.2021
Start time:	22:23:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 21s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Purchase Order to be treated on Request Imediatiely po09735-08837-8478.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:	20
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@6/4@1/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 3.4% (good quality ratio 1.9%) • Quality average: 43.8% • Quality standard deviation: 40.2%
HCA Information:	• Successful, ratio: 99% • 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

Simulations

Behavior and APIs

Time	Type	Description
22:24:16	API Interceptor	931x Sleep call for process: Purchase Order to be treated on Request Imediatiely po09735-08837-8478.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
173.201.192.229	TNT Einvoice No TNTMX9853 Consignment Notification Delivery_pdf.exe	Get hash	malicious	Browse	
	RFQ0723272983.exe	Get hash	malicious	Browse	
	XUNgjfaf6u.exe	Get hash	malicious	Browse	
	http://blog.ploytrip.com/z9cr/Pages/UxiQlIomnGiGKODewvEaBYLyCJh/	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
smtpout.us-phx.vox.secureserver.net	TNT Einvoice No TNTMX9853 Consignment Notification Delivery_pdf.exe	Get hash	malicious	Browse	• 173.201.192.229

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS-26496-GO-DADDY-COM-LLCUS	9JzK89dRiaBYTuN.exe	Get hash	malicious	Browse	• 184.168.131.241
	SWIFT REF GO 20210730SFT21020137.exe	Get hash	malicious	Browse	• 148.66.138.106
	UEe8hqOnX7fBM9G.exe	Get hash	malicious	Browse	• 184.168.131.241
	PaymentAdvice.exe	Get hash	malicious	Browse	• 184.168.131.241
	transferred $95,934.55 pdf.exe	Get hash	malicious	Browse	• 184.168.131.241
	rL3Wx4zKD4.exe	Get hash	malicious	Browse	• 184.168.131.241
	ORDER_0009_PDF.exe	Get hash	malicious	Browse	• 184.168.131.241
	mssecsvc.exe	Get hash	malicious	Browse	• 184.168.224.141
	Purchase Requirements.exe	Get hash	malicious	Browse	• 192.169.220.85
	DHL Shipment Notification.PDF.exe	Get hash	malicious	Browse	• 104.238.68.196
	PO_0008.exe	Get hash	malicious	Browse	• 104.238.68.196
	QVwfduoULs.exe	Get hash	malicious	Browse	• 184.168.131.241
	Scan#0068-46c3365.exe	Get hash	malicious	Browse	• 184.168.131.241
	INVOICE - Q0002255 - LKJIN001 (29-07-21)-pdf.exe	Get hash	malicious	Browse	• 198.71.232.11
	QUOTATION LIST FOR NEW ORDER 8121.exe	Get hash	malicious	Browse	• 192.169.150.189
	P4tH618mxp	Get hash	malicious	Browse	• 148.72.252.199
	bh68pCGom0.exe	Get hash	malicious	Browse	• 166.62.103.55
	GSJ1vGT2WQ	Get hash	malicious	Browse	• 160.153.44.213
	AMxAyl1FvN.doc	Get hash	malicious	Browse	• 107.180.29.18
	fzyVEFy0O2.exe	Get hash	malicious	Browse	• 184.168.131.241

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\Purchase Order to be treated on Request Imediatiely po09735-08837-8478.exe.log

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\Purchase Order to be treated on Request Imediatiely po09735-08837-8478.exe.log	
Process:	C:\Users\user\Desktop\Purchase Order to be treated on Request Imediatiely po09735-08837-8478.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	664
Entropy (8bit):	5.288448637977022
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10Ug+9Yz9t0U29hJ5g1B0U2ukyrFk70U2xANlW3ANv:MLF20NaL3z2p29hJ5g522rW2xAi3A9
MD5:	B1DB55991C3DA14E35249AEA1BC357CA
SHA1:	0DD2D91198FDEF296441B12F1A906669B279700C
SHA-256:	34D3E48321D5010AD2BD1F3F0B728077E4F5A7F70D66FA36B57E5209580B6BDC
SHA-512:	BE38A31888C9C2F8047FA9C99672CB985179D325107514B7500DDA9523AE3E1D20B45EACC4E6C8A5D096360D0FBB98A120E63F38FFE324DF8A0559F6890CC80
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Runtime.Remo#\35774dc3cd31b4550ab06c3354cf4ba5\System.Runtime.Remoting.ni.dll",0..

C:\Users\user\AppData\Local\Temp\tmp8725.tmp	
Process:	C:\Users\user\Desktop\Purchase Order to be treated on Request Imediatiely po09735-08837-8478.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1640
Entropy (8bit):	5.185657434237342
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGX0tn:cbhK79lNQR/rydbz9I3YODOLNdq3ly
MD5:	A42B7A7960DA158169C73159ACD24DD7
SHA1:	6DD169607FE37D32F88AFF7163D2DC4C61C6BAF8
SHA-256:	D3A4D67113C58B174808205E61A91D25AA24DEBBFBAC86E1D28A1A47FC0A90ED
SHA-512:	B8E80E0923B3072A0746D85EFADF7C789549BBDC14BAC56FA9C85B013D14542814BF5C9CCB2EDC21C38F45B1C440F778B444214AA4BF3B8384939DB7BC3B515
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Roaming\HQCVwZi.exe	
Process:	C:\Users\user\Desktop\Purchase Order to be treated on Request Imediatiely po09735-08837-8478.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1133568
Entropy (8bit):	6.898861952674989
Encrypted:	false
SSDEEP:	24576:dxJNVQfW3q5/d3sK64JTFui2Q1zht6ype:nJN9nK64JTF32Q1r
MD5:	ACECD4BF504C7910E3D65CEA16C63F10
SHA1:	02D038F99C805F46BB6EB75CD0E2831A149B770C
SHA-256:	F69B1078008E3E2F37009B44A13C722C84A5115E99FDA915916264AB7D95FFE1
SHA-512:	4659380B670EBA061141DAC66621D85D77E53504BE642E8C5F660B46BEC436EF4DF09FBC283883E2362A04A9516E1E9375A214FFB7B40B6BBA9EF422CF225277
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 49%, Browse • Antivirus: ReversingLabs, Detection: 79%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....B.....a... .....@.. ....@.....`a..K..... ..... ..H.....text....A... ...B..... ..`.rsrc.....D.....@..@.rel oc.....J.....@..B.....a.....H.....8...$.....\K.....0..&.....+.&...(....(.....(.....o....*.....0.....+.&.+.&. ....8.....(....8*... .....E.....R...8)...& ....8.....(.....(....9....& ....8.....(.....(.....(.... ....9....&.*...^+.&...(....o....(....*.+.&..*..+.&..*.F+.&.+.&...(....*...+.&..*..+.&..*..0.....+.&.+.&. . ...80...s.....s.....s.....8*... .....E.....

C:\Users\user\AppData\Roaming\HQCVwZi.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\Purchase Order to be treated on Request Imediatiely po09735-08837-8478.exe

C:\Users\user\AppData\Roaming\HQCVwZi.exe:Zone.Identifier	
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.898861952674989
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:	Purchase Order to be treated on Request Imediatiely po09735-08837-8478.exe
File size:	1133568
MD5:	acecd4bf504c7910e3d65cea16c63f10
SHA1:	02d038f99c805f46bb6eb75cd0e2831a149b770c
SHA256:	f69b1078008e3e2f37009b44a13c722c84a5115e99fda915916264ab7d95ffe1
SHA512:	4659380b670eba061141dac66621d85d77e53504be642e8c5f660b46bec436ef4df09fbc283883e2362a04a9516e1e9375a214ffb7b40b6bba9ef422cf225277
SSDEEP:	24576:dxJNVQfW3q5/d3sK64JTFui2Q1zht6ype:nJN9nK64JTF32Q1r
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....B.....a... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x5161ae
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x610204AB [Thu Jul 29 01:30:19 2021 UTC]
TLS Callbacks:	

General

CLR (.Net) Version:	v2.0.50727
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

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x1141b4	0x114200	False	0.617443908443	data	6.90411210423	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x118000	0x5ac	0x600	False	0.42578125	data	4.0783402747	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x11a000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 22:25:48.601164103 CEST	192.168.2.4	8.8.8.8	0xd0a4	Standard query (0)	smtpout.secureserver.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 22:25:48.634552002 CEST	8.8.8.8	192.168.2.4	0xd0a4	No error (0)	smtpout.secureserver.net	smtpout.vox.secureserver.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 22:25:48.634552002 CEST	8.8.8.8	192.168.2.4	0xd0a4	No error (0)	smtpout.vox.secureserver.net	smtpout.us-phx.vox.secureserver.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 22:25:48.634552002 CEST	8.8.8.8	192.168.2.4	0xd0a4	No error (0)	smtpout.us-phx.vox.secureserver.net		173.201.192.229	A (IP address)	IN (0x0001)
Aug 3, 2021 22:25:48.634552002 CEST	8.8.8.8	192.168.2.4	0xd0a4	No error (0)	smtpout.us-phx.vox.secureserver.net		173.201.193.101	A (IP address)	IN (0x0001)
Aug 3, 2021 22:25:48.634552002 CEST	8.8.8.8	192.168.2.4	0xd0a4	No error (0)	smtpout.us-phx.vox.secureserver.net		68.178.252.229	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 22:25:48.634552002 CEST	8.8.8.8	192.168.2.4	0xd0a4	No error (0)	smtpout.us-phx.vox.secureserver.net		68.178.252.101	A (IP address)	IN (0x0001)
Aug 3, 2021 22:25:48.634552002 CEST	8.8.8.8	192.168.2.4	0xd0a4	No error (0)	smtpout.us-phx.vox.secureserver.net		173.201.192.101	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Aug 3, 2021 22:25:49.007302046 CEST	587	49779	173.201.192.229	192.168.2.4	220 p3plsmtpa07-08.prod.phx3.secureserver.net :SMTPAUTH: B0yymmylZxud2 : ESMTP server p3plsmtpa07-08.prod.phx3.secureserver.net ready
Aug 3, 2021 22:25:49.007816076 CEST	49779	587	192.168.2.4	173.201.192.229	EHLO 216554
Aug 3, 2021 22:25:49.181849957 CEST	587	49779	173.201.192.229	192.168.2.4	250-p3plsmtpa07-08.prod.phx3.secureserver.net hello [84.17.52.25], secureserver.net 250-HELP 250-AUTH LOGIN PLAIN 250-SIZE 30000000 250-PIPELINING 250-8BITMIME 250-STARTTLS 250 OK

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Purchase Order to be treated on Request Imediatiely po09735-08837-8478.exe PID: 6708 Parent PID: 5872

General

Start time:	22:24:07
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\Purchase Order to be treated on Request Imediatiely po09735-08837-8478.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Purchase Order to be treated on Request Imediatiely po09735-08837-8478.exe'
Imagebase:	0xe20000
File size:	1133568 bytes
MD5 hash:	ACECD4BF504C7910E3D65CEA16C63F10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.676811837.00000000034D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.678480420.00000000044D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.678480420.00000000044D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.677627509.0000000003675000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 7088 Parent PID: 6708

General

Start time:	22:24:17
Start date:	03/08/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\HQCVwZi' /XML 'C:\Users\user\AppData\Local\Temp\tmp8725.tmp'
Imagebase:	0xb30000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 7096 Parent PID: 7088

General

Start time:	22:24:18
Start date:	03/08/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: Purchase Order to be treated on Request Imediatiely po09735-08837-8478.exe PID: 7140 Parent PID: 6708

General

Start time:	22:24:18
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\Purchase Order to be treated on Request Imediatiely po09735-08837-8478.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Purchase Order to be treated on Request Imediatiely po09735-08837-8478.exe
Imagebase:	0xea0000
File size:	1133568 bytes
MD5 hash:	ACECD4BF504C7910E3D65CEA16C63F10
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: 00000007.00000002.919985835.00000000036A7000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.919719729.0000000003621000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000007.00000002.919719729.0000000003621000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.917197559.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000007.00000002.917197559.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Disassembly

Code Analysis