ID: 345000
Sample Name: New Order.exe
Cookbook: default.jbs
Time: 15:38:37
Date: 27/01/2021
Version: 31.0.0 Emerald

Table of Contents

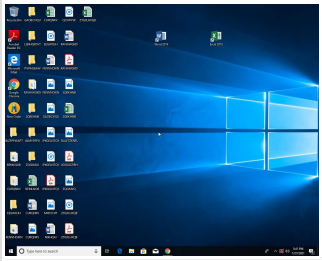
Analysis Report New Order.exe

Overview

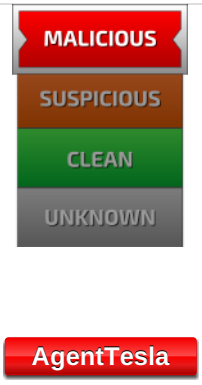
General Information

Sample Name:	New Order.exe
Analysis ID:	345000
MD5:	3462afcbdb0969b.
SHA1:	6429f37abdf26c9..
SHA256:	112f430a8cc28d3..
Tags:	AgentTesla exe

Most interesting Screenshot:



Detection



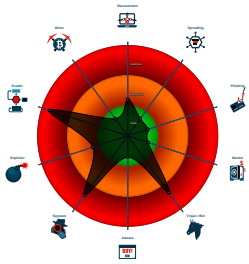
AgentTesla

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…
- Sigma detected: Scheduled temp file…
- Snort IDS alert for network traffic (e….
- Yara detected AgentTesla
- Yara detected AntiVM_3
- .NET source code contains potentia…
- .NET source code contains very larg…
- C2 URLs / IPs found in malware con…
- Initial sample is a PE file and has a …
- Machine Learning detection for dropp…
- Machine Learning detection for samp…

Classification



Startup

- **System is w10x64**
- New Order.exe (PID: 5976 cmdline: 'C:\Users\user\Desktop\New Order.exe' MD5: 3462AFCBDB0969B7F24B42F0E42C7988)
  - schtasks.exe (PID: 6120 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\veTETlsQyxlWT' /XML 'C:\Users\user\AppData\Local\Temp\tmpC36D.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6116 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - New Order.exe (PID: 4652 cmdline: {path} MD5: 3462AFCBDB0969B7F24B42F0E42C7988)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Username: ": "xTnivYecyez3mEL",
  "URL: ": "https://sO7lUZh6d9PCQs.org",
  "To: ": "wonder@pulpdant.com",
  "ByHost: ": "smtp.pulpdant.com:587",
  "Password: ": "7uA2gBhi",
  "From: ": "wonder@pulpdant.com"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.365195256.000000000336 1000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000003.00000002.690207756.000000000308 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000003.00000002.690207756.000000000308 1000.00000004.00000001.sdmp	JoeSecurity_CredentialSte aler	Yara detected Credential Stealer	Joe Security	
00000003.00000002.687646589.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.365875763.00000000042E 9000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 4 entries				

Unpacked PEs

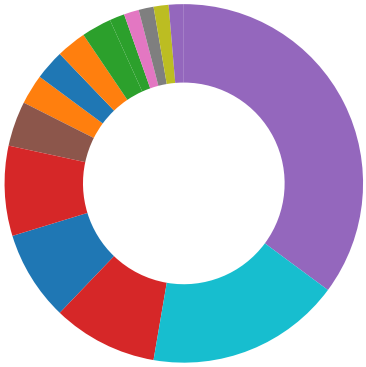
Source	Rule	Description	Author	Strings
3.2.New Order.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



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

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Machine Learning detection for sample

Compliance:

Uses 32bit PE files

Contains modern PE file flags such as dynamic base (ASLR) or NX

Networking:

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

C2 URLs / IPs found in malware configuration

System Summary:

.NET source code contains very large array initializations

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

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

Malware Analysis System Evasion:

Yara detected AntiVM_3

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)

Queries sensitive video device information (via WMI, Win32_VideoController, often done to detect virtual machines)

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

Stealing of Sensitive Information:

Yara detected AgentTesla

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

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

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

Remote Access Functionality:

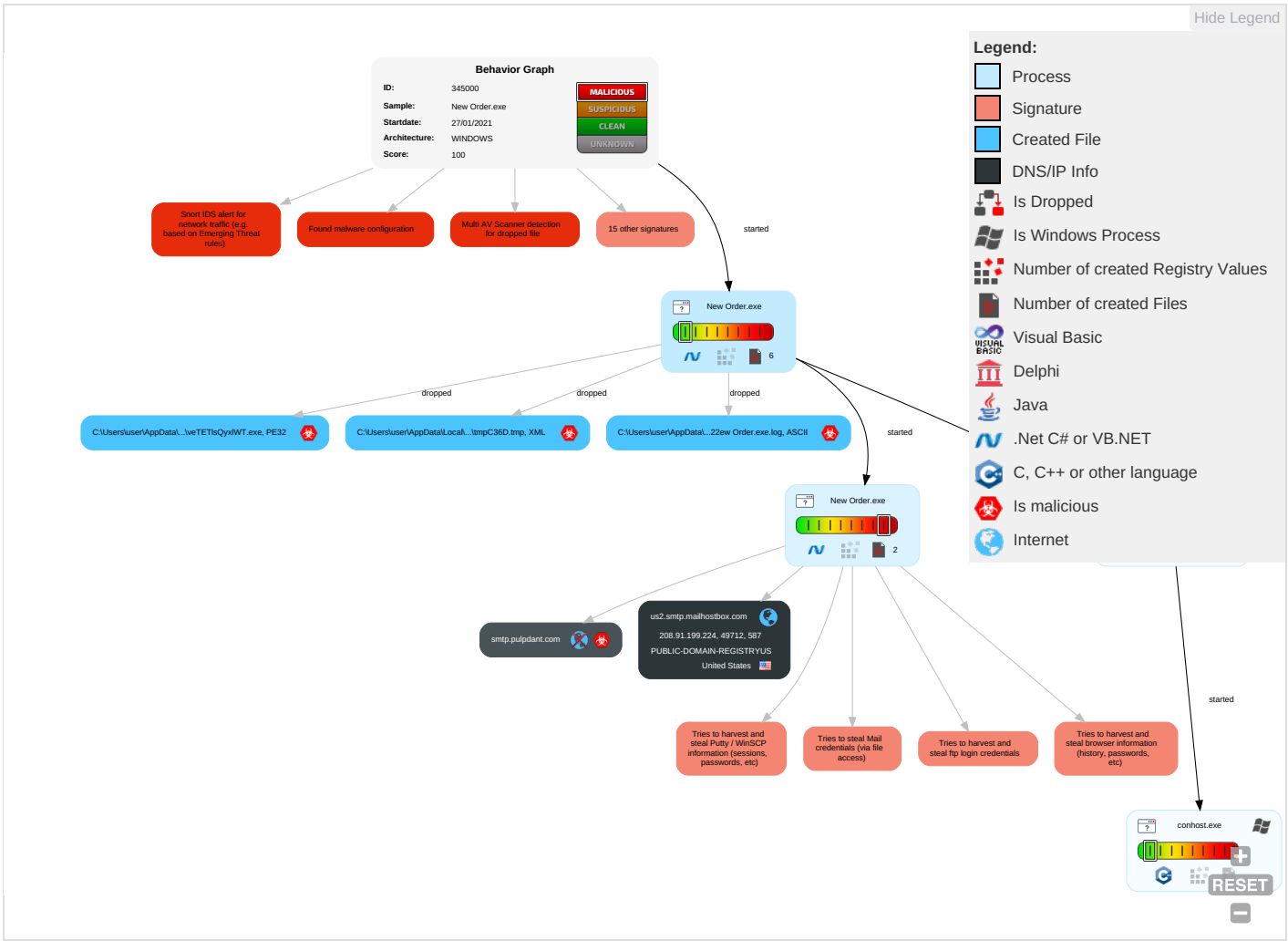
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 3 1 1	DLL Side-Loading 1	DLL Side-Loading 1	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	Scheduled Task/Job 1	Process Injection 1 2	Deobfuscate/Decode Files or Information 1	Credentials in Registry 1	System Information Discovery 1 1 4	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Scheduled Task/Job 1	Obfuscated Files or Information 3	Security Account Manager	Security Software Discovery 4 2 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 1 2	NTDS	Virtualization/Sandbox Evasion 2 4	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Laye Protocol 1 1 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	DLL Side-Loading 1	LSA Secrets	Process Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1	Cached Domain Credentials	Application Window Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 2 4	DCSync	Remote System 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	Process Injection 1 2	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Laye Protocol

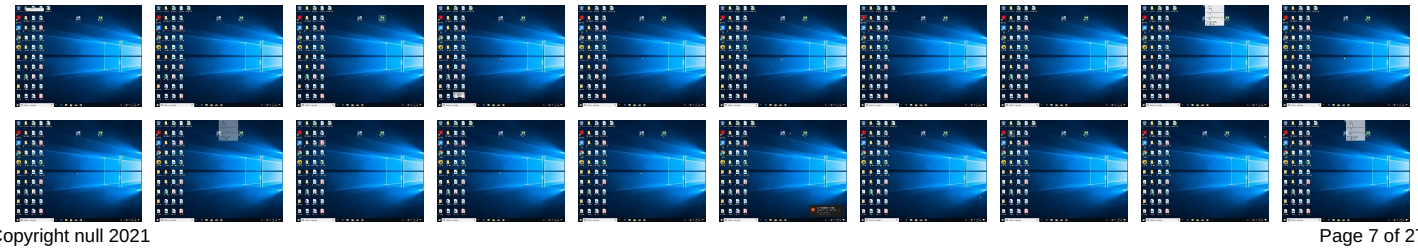
Behavior Graph



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
New Order.exe	25%	Virustotal		Browse
New Order.exe	28%	ReversingLabs	ByteCode-MSIL.Packed.Generic	
New Order.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\veTETlsQyxlWT.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\veTETlsQyxlWT.exe	28%	ReversingLabs	ByteCode-MSIL.Packed.Generic	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.New Order.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
smtp.pulpdant.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	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://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://SgOtfE.com	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://https://api.ipify.org%$	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	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.founder.com.cn/cn/cThe	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://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://https://sO7lUZh6d9PCQs.org	0%	Avira URL Cloud	safe	
http://smtp.pulpdant.com	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	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://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	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://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	208.91.199.224	true	false		high
smtp.pulpdant.com	unknown	unknown	true	• 0%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://sO7lUZh6d9PCQs.org	true	• Avira URL Cloud: safe	unknown

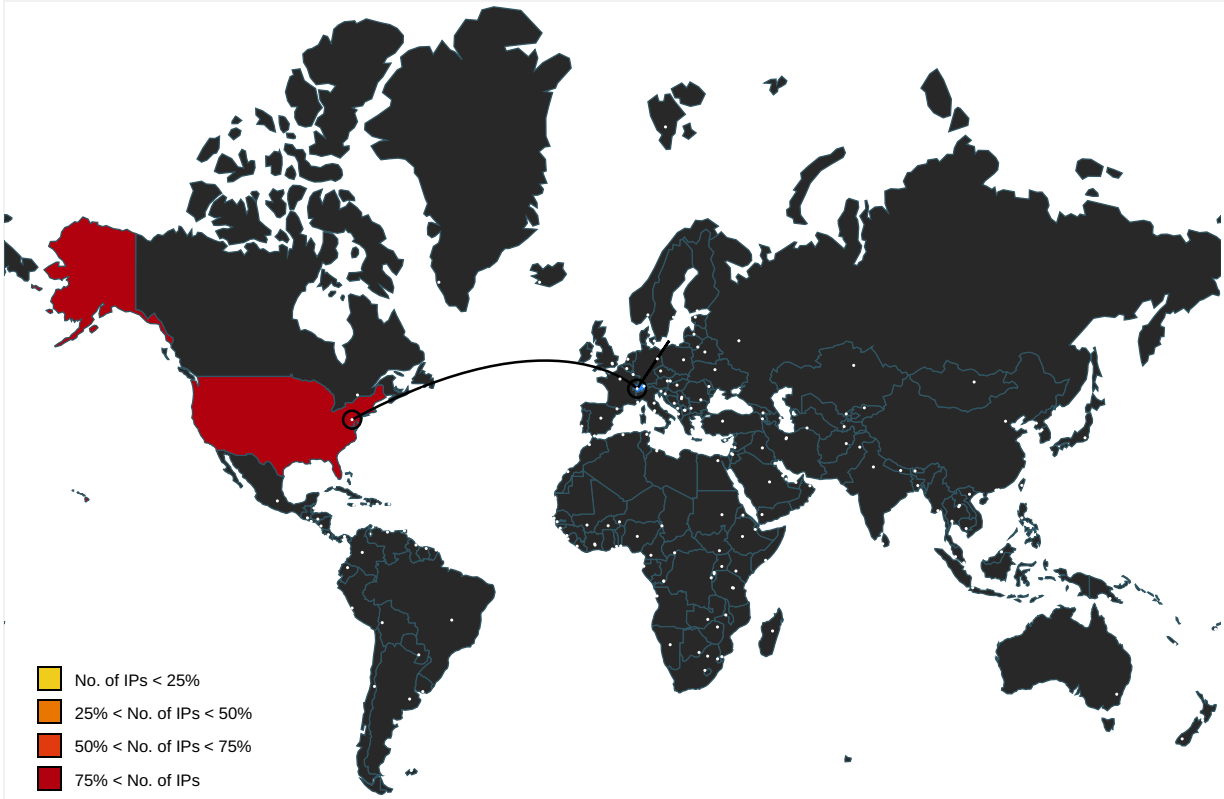
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	New Order.exe, 00000003.00000002.690207756.0000000003081000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.apache.org/licenses/LICENSE-2.0	New Order.exe, 00000000.00000002.370232451.0000000007462000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com	New Order.exe, 00000000.00000002.370232451.0000000007462000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	New Order.exe, 00000000.00000002.370232451.0000000007462000.00000004.00000001.sdmp	false		high
http://DynDns.comDynDNS	New Order.exe, 00000003.00000002.690207756.0000000003081000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	New Order.exe, 00000000.00000002.370232451.0000000007462000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	New Order.exe, 00000000.00000002.370232451.0000000007462000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://us2.smtp.mailhostbox.com	New Order.exe, 00000003.00000002.691773465.00000000033DE000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	New Order.exe, 00000003.00000002.690207756.0000000003081000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	New Order.exe, 00000000.00000002.370232451.0000000007462000.00000004.00000001.sdmp	false		high
http://SgOtfE.com	New Order.exe, 00000003.00000002.690207756.0000000003081000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.tiro.com	New Order.exe, 00000000.000000 02.370232451.0000000007462000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	New Order.exe, 00000000.000000 02.370232451.0000000007462000. 00000004.00000001.sdmp	false		high
http://www.goodfont.co.kr	New Order.exe, 00000000.000000 02.370232451.0000000007462000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.org%$	New Order.exe, 00000003.000000 02.690207756.0000000003081000. 00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.carterandcone.coml	New Order.exe, 00000000.000000 02.370232451.0000000007462000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	New Order.exe, 00000000.000000 02.370232451.0000000007462000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	New Order.exe, 00000000.000000 02.370232451.0000000007462000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	New Order.exe, 00000000.000000 02.370232451.0000000007462000. 00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	New Order.exe, 00000000.000000 02.370232451.0000000007462000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	New Order.exe, 00000000.000000 02.370232451.0000000007462000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	New Order.exe, 00000000.000000 02.370232451.0000000007462000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	New Order.exe, 00000000.000000 02.370232451.0000000007462000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	New Order.exe, 00000000.000000 02.370232451.0000000007462000. 00000004.00000001.sdmp	false		high
http://smtp.pulpdant.com	New Order.exe, 00000003.000000 02.691773465.00000000033DE000. 00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	New Order.exe, 00000000.000000 02.370232451.0000000007462000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	New Order.exe, 00000000.000000 02.370232451.0000000007462000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	New Order.exe, 00000000.000000 02.370232451.0000000007462000. 00000004.00000001.sdmp	false		high
http://https://api.ipify.org%GETMozilla/5.0	New Order.exe, 00000003.000000 02.690207756.0000000003081000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.fonts.com	New Order.exe, 00000000.000000 02.370232451.0000000007462000. 00000004.00000001.sdmp	false		high
http://www.sandoll.co.kr	New Order.exe, 00000000.000000 02.370232451.0000000007462000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	New Order.exe, 00000000.000000 02.370232451.0000000007462000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	New Order.exe, 00000000.000000 02.370232451.0000000007462000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	New Order.exe, 00000000.000000 02.365090129.00000000032E1000. 00000004.00000001.sdmp	false		high
http://www.sakkal.com	New Order.exe, 00000000.000000 02.370232451.0000000007462000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • 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	New Order.exe, 00000000.00000002.365875763.00000000042E9000.00000004.00000001.sdmp, New Order.exe, 00000003.00000002.687646589.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
208.91.199.224	unknown	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	345000
Start date:	27.01.2021
Start time:	15:38:37
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 29s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	New Order.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:	9
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@6/3@2/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 93% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 104.43.193.48, 168.61.161.212, 67.26.81.254, 8.248.121.254, 8.241.123.254, 67.27.159.254, 67.27.158.126, 23.210.248.85 • Excluded domains from analysis (whitelisted): fs.microsoft.com, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, skypedataprdcolcus15.cloudapp.net, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
15:39:38	API Interceptor	989x Sleep call for process: New Order.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
208.91.199.224	AWB 9899691012 TRACKING INFO_pdf.exe	Get hash	malicious	Browse	
	para.exe	Get hash	malicious	Browse	
	New Order #21076.exe	Get hash	malicious	Browse	
	New order.PDF.exe	Get hash	malicious	Browse	
	7xCBr7CChD.exe	Get hash	malicious	Browse	
	Purchase Order no 7770022460.exe	Get hash	malicious	Browse	
	ezs8BPdIwM.exe	Get hash	malicious	Browse	
	FedEx Receipt.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	UAE CHEMEX RFQ.exe	Get hash	malicious	Browse	
	UAE CHEMEX PPMC.exe	Get hash	malicious	Browse	
	quote 2021.exe	Get hash	malicious	Browse	
	MV Double Miracle.exe	Get hash	malicious	Browse	
	PO-SOT215006A.exe	Get hash	malicious	Browse	
	invoice No 8882.exe	Get hash	malicious	Browse	
	Y3fwLpzaXNZPaT6.exe	Get hash	malicious	Browse	
	Proforma Invoice.exe	Get hash	malicious	Browse	
	BANK SWIFT.xlsx	Get hash	malicious	Browse	
	Shipping_Document.exe	Get hash	malicious	Browse	
	DUBAI HC21RED21.exe	Get hash	malicious	Browse	
	December_Document_.doc	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
us2.smtp.mailhostbox.com	DHL_SD-0127.exe	Get hash	malicious	Browse	• 208.91.199.223
	HTG-9087650.exe	Get hash	malicious	Browse	• 208.91.198.143
	TACSAL.xlsx	Get hash	malicious	Browse	• 208.91.199.225
	PO#21010028 - SYINDAC QT-00820_pdf.exe	Get hash	malicious	Browse	• 208.91.199.223
	para.exe	Get hash	malicious	Browse	• 208.91.199.225
	AWB 9899691012 TRACKING INFO_pdf.exe	Get hash	malicious	Browse	• 208.91.199.224
	para.exe	Get hash	malicious	Browse	• 208.91.199.224
	SIC_9827906277.pdf.exe	Get hash	malicious	Browse	• 208.91.198.143
	Quotation Prices.exe	Get hash	malicious	Browse	• 208.91.199.225
	SecuriteInfo.com.Trojan.PackedNET.519.20020.exe	Get hash	malicious	Browse	• 208.91.199.225
	SSE_SOA2021.doc	Get hash	malicious	Browse	• 208.91.198.143
	HTG-9066543.exe	Get hash	malicious	Browse	• 208.91.199.223
	New Order #21076.exe	Get hash	malicious	Browse	• 208.91.199.224
	HTMY-209871640.exe	Get hash	malicious	Browse	• 208.91.198.143
	SecuriteInfo.com.Artemis707F61F6A223.exe	Get hash	malicious	Browse	• 208.91.199.225
	New order.PDF.exe	Get hash	malicious	Browse	• 208.91.199.224
	SOA.exe	Get hash	malicious	Browse	• 208.91.199.225
	7xCBr7CChD.exe	Get hash	malicious	Browse	• 208.91.199.224
	Purchase Order no 7770022460.exe	Get hash	malicious	Browse	• 208.91.199.224
	Payment slip.exe	Get hash	malicious	Browse	• 208.91.198.143

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PUBLIC-DOMAIN-REGISTRYUS	DHL_SD-0127.exe	Get hash	malicious	Browse	• 208.91.199.223
	Statement of Account as of Jan_27 2021.xlsm	Get hash	malicious	Browse	• 208.91.199.150
	HTG-9087650.exe	Get hash	malicious	Browse	• 208.91.198.143
	TACSAL.xlsx	Get hash	malicious	Browse	• 208.91.199.225
	PO#21010028 - SYINDAC QT-00820_pdf.exe	Get hash	malicious	Browse	• 208.91.199.223
	para.exe	Get hash	malicious	Browse	• 208.91.199.225
	AWB 9899691012 TRACKING INFO_pdf.exe	Get hash	malicious	Browse	• 208.91.199.224
	para.exe	Get hash	malicious	Browse	• 208.91.199.224
	SIC_9827906277.pdf.exe	Get hash	malicious	Browse	• 208.91.198.143
	Quotation Prices.exe	Get hash	malicious	Browse	• 208.91.199.223
	SecuriteInfo.com.Trojan.PackedNET.519.20020.exe	Get hash	malicious	Browse	• 208.91.199.225
	Shipping_Details.exe	Get hash	malicious	Browse	• 204.11.58.28
	Request.xlsx	Get hash	malicious	Browse	• 103.53.40.13
	HTG-9066543.exe	Get hash	malicious	Browse	• 208.91.199.223
	vA0mtZ7JzJ.exe	Get hash	malicious	Browse	• 216.10.246.131
	New Order #21076.exe	Get hash	malicious	Browse	• 208.91.199.224
	k.dll	Get hash	malicious	Browse	• 162.215.252.76
	HTMY-209871640.exe	Get hash	malicious	Browse	• 208.91.198.143
	SecuriteInfo.com.Artemis707F61F6A223.exe	Get hash	malicious	Browse	• 208.91.199.225
	SecuriteInfo.com.Trojan.DownLoader36.37393.26064.exe	Get hash	malicious	Browse	• 43.225.55.205

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\New Order.exe.log	
Process:	C:\Users\user\Desktop\New Order.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:	moderate, 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

C:\Users\user\AppData\Local\Temp\tmpC36D.tmp	
Process:	C:\Users\user\Desktop\New Order.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1658
Entropy (8bit):	5.158121730065876
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7h2ulNMFp2O/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB3N7jBtn:cbha7JlNQV/rydbz9I3YODOLNdq3HL
MD5:	A2AC6FF93CAA0763F08A2260EA6B020F
SHA1:	C199D8254A59E5AFC0EE0BB74C59CBD492883793
SHA-256:	F0B6CE4BC288CD1665C764377B297D65ED685D43B36531851603A9E9E68025BD
SHA-512:	5A877C6550BA90D15BBD11342A29D443A7BE3B2A70563CBBB9B410DB582A4BD04F2A19F2E87F487D876F6785CA89D0B14610F1360F47A7332924BDAC3FA9F23
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>.. <StartWhenAvail

C:\Users\user\AppData\Roaming\veTETlsQyxlWT.exe	
Process:	C:\Users\user\Desktop\New Order.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	833024
Entropy (8bit):	7.3889428875564445
Encrypted:	false
SSDEEP:	12288:liqfu19XBtqKuCwaBDKKHvlBQ+8mlOYaB+:lSXBtq9ZaskX188aB
MD5:	3462AFCBDB0969B7F24B42F0E42C7988
SHA1:	6429F37ABDF26C93793ECCDD8DC0ECAFFB149655
SHA-256:	112F430A8CC28D3889163BBAF9811C74C3D2AF2C9AF672D16F0F7888DF6D51E2
SHA-512:	4656F47988A96F6ABB0E27D2C6A8BDFA69B41BC75A67B2C7D99EF45A4755E81450DA02434CA2F7CC7A5441B99810DC90E372C74214FF723A3400B2AEF359502
Malicious:	**true**

C:\Users\user\AppData\Roaming\veTETlsQyxlWT.exe	
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 28%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....L.`.....0.....R.... .....@.. ..... ..... ..@.....O..... ..... ..H.....text...X.... ..... ..`.rsrc.....@..@.reloc..... .....@..B.....4.....H.....d...._.....y....=.....&.(.....*...0..9.....~.....,".r...p.....(....o....s.....~.....+..*....0.....~.....+..*"....*.0 ..!.....(....r1..p~....o.....t.....+..*".(.....*Vr?..p....rK..p....*^..}.....(.....(.....*.0..J.....r[..pr...p(....&.(....t!...o.....#..r...p.o....(....r...p...(....&...*.....%&.# ....0..+.....,..{.....+.. ..,...{....o .....(!....*..0.....s"...}.....s"...}.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.3889428875564445
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.exe
File size:	833024
MD5:	3462afcbdb0969b7f24b42f0e42c7988
SHA1:	6429f37abdf26c93793eccdd8dc0ecaffb149655
SHA256:	112f430a8cc28d3889163bbaf9811c74c3d2af2c9af672d16f0f7888df6d51e2
SHA512:	4656f47988a96f6abb0e27d2c6a8bdfa69b41bc75a67b2c7d99ef45a4755e81450da02434ca2f7cc7a5441b99810dc90e372c74214ff723a3400b2aef3595029
SSDEEP:	12288:liqfu19XBtqKuCwaBDKKHvlBQ+8mlOYaB+:lSXBtq9ZaskX188aB
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....L.`.....0.....R.... .....@.. ....@.....

File Icon

Icon Hash:	e0dc9e0e1e9296e8

Static PE Info

General

Entrypoint:	0x4bc152
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:	0x60114C8A [Wed Jan 27 11:20:42 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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xbc100	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xbe000	0x10e98	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xd0000	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	0xba158	0xba200	False	0.680431235309	data	7.54927053001	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xbe000	0x10e98	0x11000	False	0.133099724265	data	4.5074360494	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0xd0000	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_ICON	0xbe100	0x10828	data		
RT_GROUP_ICON	0xce938	0x14	data		
RT_VERSION	0xce95c	0x33c	data		
RT_MANIFEST	0xceca8	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

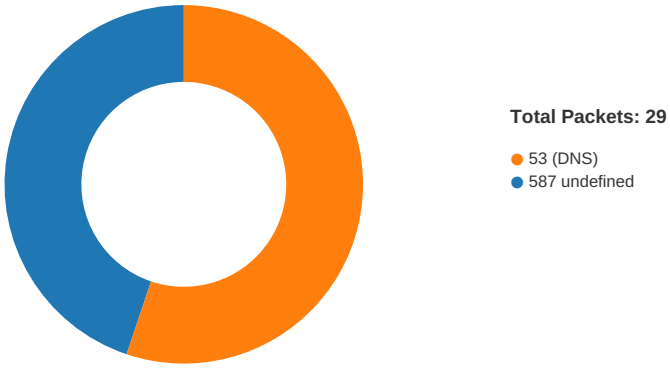
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2017
Assembly Version	1.0.0.0
InternalName	XWRTgP.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	HotelMgmtSystem
ProductVersion	1.0.0.0
FileDescription	HotelMgmtSystem
OriginalFilename	XWRTgP.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/27/21-15:41:27.530383	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49712	587	192.168.2.6	208.91.199.224

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 15:41:25.937750101 CET	49712	587	192.168.2.6	208.91.199.224
Jan 27, 2021 15:41:26.110754013 CET	587	49712	208.91.199.224	192.168.2.6
Jan 27, 2021 15:41:26.110937119 CET	49712	587	192.168.2.6	208.91.199.224
Jan 27, 2021 15:41:26.470077038 CET	587	49712	208.91.199.224	192.168.2.6
Jan 27, 2021 15:41:26.470530987 CET	49712	587	192.168.2.6	208.91.199.224
Jan 27, 2021 15:41:26.646051884 CET	587	49712	208.91.199.224	192.168.2.6
Jan 27, 2021 15:41:26.646081924 CET	587	49712	208.91.199.224	192.168.2.6
Jan 27, 2021 15:41:26.648472071 CET	49712	587	192.168.2.6	208.91.199.224
Jan 27, 2021 15:41:26.822031975 CET	587	49712	208.91.199.224	192.168.2.6
Jan 27, 2021 15:41:26.823117971 CET	49712	587	192.168.2.6	208.91.199.224
Jan 27, 2021 15:41:26.998219013 CET	587	49712	208.91.199.224	192.168.2.6
Jan 27, 2021 15:41:26.999209881 CET	49712	587	192.168.2.6	208.91.199.224
Jan 27, 2021 15:41:27.173307896 CET	587	49712	208.91.199.224	192.168.2.6
Jan 27, 2021 15:41:27.173909903 CET	49712	587	192.168.2.6	208.91.199.224
Jan 27, 2021 15:41:27.355223894 CET	587	49712	208.91.199.224	192.168.2.6
Jan 27, 2021 15:41:27.355609894 CET	49712	587	192.168.2.6	208.91.199.224
Jan 27, 2021 15:41:27.528959990 CET	587	49712	208.91.199.224	192.168.2.6
Jan 27, 2021 15:41:27.530383110 CET	49712	587	192.168.2.6	208.91.199.224
Jan 27, 2021 15:41:27.530602932 CET	49712	587	192.168.2.6	208.91.199.224
Jan 27, 2021 15:41:27.534472942 CET	49712	587	192.168.2.6	208.91.199.224
Jan 27, 2021 15:41:27.534578085 CET	49712	587	192.168.2.6	208.91.199.224
Jan 27, 2021 15:41:27.705373049 CET	587	49712	208.91.199.224	192.168.2.6
Jan 27, 2021 15:41:27.709623098 CET	587	49712	208.91.199.224	192.168.2.6
Jan 27, 2021 15:41:27.807670116 CET	587	49712	208.91.199.224	192.168.2.6
Jan 27, 2021 15:41:27.851052999 CET	49712	587	192.168.2.6	208.91.199.224

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 15:39:27.138477087 CET	58931	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:39:27.197932959 CET	53	58931	8.8.8.8	192.168.2.6
Jan 27, 2021 15:39:28.445102930 CET	57725	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:39:28.507457972 CET	53	57725	8.8.8.8	192.168.2.6
Jan 27, 2021 15:39:29.423366070 CET	49283	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:39:29.471323013 CET	53	49283	8.8.8.8	192.168.2.6
Jan 27, 2021 15:39:30.419294119 CET	58377	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:39:30.469995022 CET	53	58377	8.8.8.8	192.168.2.6
Jan 27, 2021 15:39:31.702112913 CET	55074	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:39:31.762833118 CET	53	55074	8.8.8.8	192.168.2.6
Jan 27, 2021 15:39:32.712439060 CET	54513	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:39:32.760235071 CET	53	54513	8.8.8.8	192.168.2.6
Jan 27, 2021 15:39:34.033950090 CET	62044	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:39:34.084796906 CET	53	62044	8.8.8.8	192.168.2.6
Jan 27, 2021 15:39:35.238338947 CET	63791	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:39:35.286547899 CET	53	63791	8.8.8.8	192.168.2.6
Jan 27, 2021 15:39:36.279795885 CET	64267	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:39:36.327878952 CET	53	64267	8.8.8.8	192.168.2.6
Jan 27, 2021 15:39:37.301007986 CET	49448	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:39:37.351645947 CET	53	49448	8.8.8.8	192.168.2.6
Jan 27, 2021 15:39:38.282694101 CET	60342	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:39:38.330748081 CET	53	60342	8.8.8.8	192.168.2.6
Jan 27, 2021 15:39:39.464906931 CET	61346	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:39:39.512805939 CET	53	61346	8.8.8.8	192.168.2.6
Jan 27, 2021 15:40:16.960711956 CET	51774	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:40:17.008583069 CET	53	51774	8.8.8.8	192.168.2.6
Jan 27, 2021 15:40:57.783761024 CET	56023	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:40:57.841753006 CET	53	56023	8.8.8.8	192.168.2.6
Jan 27, 2021 15:41:25.554264069 CET	58384	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:41:25.744374990 CET	53	58384	8.8.8.8	192.168.2.6
Jan 27, 2021 15:41:25.757422924 CET	60261	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:41:25.820508957 CET	53	60261	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 27, 2021 15:41:25.554264069 CET	192.168.2.6	8.8.8.8	0x1d95	Standard query (0)	smtp.pulpdant.com	A (IP address)	IN (0x0001)
Jan 27, 2021 15:41:25.757422924 CET	192.168.2.6	8.8.8.8	0x149	Standard query (0)	smtp.pulpdant.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 27, 2021 15:41:25.744374990 CET	8.8.8.8	192.168.2.6	0x1d95	No error (0)	smtp.pulpdant.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:41:25.744374990 CET	8.8.8.8	192.168.2.6	0x1d95	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Jan 27, 2021 15:41:25.744374990 CET	8.8.8.8	192.168.2.6	0x1d95	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Jan 27, 2021 15:41:25.744374990 CET	8.8.8.8	192.168.2.6	0x1d95	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Jan 27, 2021 15:41:25.744374990 CET	8.8.8.8	192.168.2.6	0x1d95	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Jan 27, 2021 15:41:25.820508957 CET	8.8.8.8	192.168.2.6	0x149	No error (0)	smtp.pulpdant.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:41:25.820508957 CET	8.8.8.8	192.168.2.6	0x149	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Jan 27, 2021 15:41:25.820508957 CET	8.8.8.8	192.168.2.6	0x149	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Jan 27, 2021 15:41:25.820508957 CET	8.8.8.8	192.168.2.6	0x149	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Jan 27, 2021 15:41:25.820508957 CET	8.8.8.8	192.168.2.6	0x149	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)

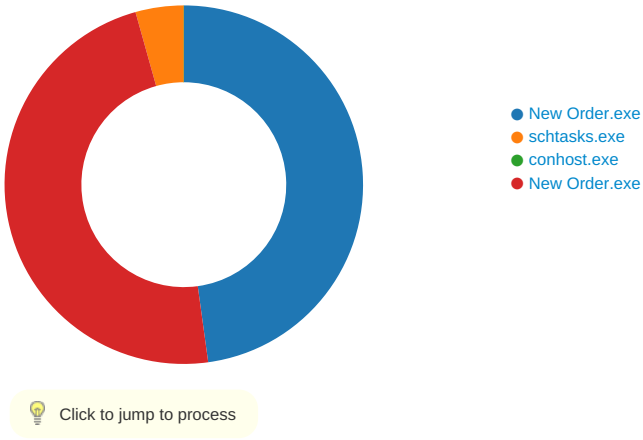
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 27, 2021 15:41:26.470077038 CET	587	49712	208.91.199.224	192.168.2.6	220 us2.outbound.mailhostbox.com ESMTP Postfix
Jan 27, 2021 15:41:26.470530987 CET	49712	587	192.168.2.6	208.91.199.224	EHLO 724536
Jan 27, 2021 15:41:26.646081924 CET	587	49712	208.91.199.224	192.168.2.6	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
Jan 27, 2021 15:41:26.648472071 CET	49712	587	192.168.2.6	208.91.199.224	AUTH login d29uZGVyQHB1bHBkYW50LmNvbQ==
Jan 27, 2021 15:41:26.822031975 CET	587	49712	208.91.199.224	192.168.2.6	334 UGFzc3dvcmQ6
Jan 27, 2021 15:41:26.998219013 CET	587	49712	208.91.199.224	192.168.2.6	235 2.7.0 Authentication successful
Jan 27, 2021 15:41:26.999209881 CET	49712	587	192.168.2.6	208.91.199.224	MAIL FROM:<wonder@pulpdant.com>
Jan 27, 2021 15:41:27.173307896 CET	587	49712	208.91.199.224	192.168.2.6	250 2.1.0 Ok
Jan 27, 2021 15:41:27.173909903 CET	49712	587	192.168.2.6	208.91.199.224	RCPT TO:<wonder@pulpdant.com>
Jan 27, 2021 15:41:27.355223894 CET	587	49712	208.91.199.224	192.168.2.6	250 2.1.5 Ok
Jan 27, 2021 15:41:27.355609894 CET	49712	587	192.168.2.6	208.91.199.224	DATA
Jan 27, 2021 15:41:27.528959990 CET	587	49712	208.91.199.224	192.168.2.6	354 End data with <CR><LF>.<CR><LF>
Jan 27, 2021 15:41:27.534578085 CET	49712	587	192.168.2.6	208.91.199.224	.
Jan 27, 2021 15:41:27.807670116 CET	587	49712	208.91.199.224	192.168.2.6	250 2.0.0 Ok: queued as 43E74D7BAE

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: New Order.exe PID: 5976 Parent PID: 5704

General

Start time:	15:39:32
Start date:	27/01/2021
Path:	C:\Users\user\Desktop\New Order.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\New Order.exe'
Imagebase:	0xf30000
File size:	833024 bytes
MD5 hash:	3462AFCBDB0969B7F24B42F0E42C7988
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: 00000000.00000002.365195256.0000000003361000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.365875763.00000000042E9000.00000004.00000001.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	6E11CF06	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	6E11CF06	unknown
C:\Users\user\AppData\Roaming\veTETlsQyxlWT.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CF61E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpC36D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CF67038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\New Order.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E42C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpC36D.tmp	success or wait	1	6CF66A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\veTETlsQyxlWT.exe	unknown	833024	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 8a 4c 11 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 a2 0b 00 00 12 01 00 00 00 00 00 52 c1 0b 00 00 20 00 00 00 e0 0b 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 20 0d 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L....L.`.......... ....0............R.... ....@.. ....@................	success or wait	1	6CF61B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpC36D.tmp	unknown	1658	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 65 6e 67 69 6e 65 65 72 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f	<?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>.. </Registratio	success or wait	1	6CF61B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\New Order.exe.log	unknown	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",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_v4.0.3	success or wait	1	6E42C907	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	6E0F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0F5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0FCA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF61B4F	ReadFile
C:\Users\user\Desktop\New Order.exe	unknown	833024	success or wait	1	6CF61B4F	ReadFile

Analysis Process: schtasks.exe PID: 6120 Parent PID: 5976

General

Start time:	15:39:42
Start date:	27/01/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\veTETlsQyxlWT' /XML 'C:\ Users\user\AppData\Local\Temp\tmpC36D.tmp'
Imagebase:	0x960000
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpC36D.tmp	unknown	2	success or wait	1	96AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpC36D.tmp	unknown	1659	success or wait	1	96ABD9	ReadFile

Analysis Process: conhost.exe PID: 6116 Parent PID: 6120

General

Start time:	15:39:42
Start date:	27/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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.exe PID: 4652 Parent PID: 5976

General

Start time:	15:39:43
Start date:	27/01/2021
Path:	C:\Users\user\Desktop\New Order.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xcb0000
File size:	833024 bytes
MD5 hash:	3462AFCBDB0969B7F24B42F0E42C7988
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.690207756.0000000003081000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000002.690207756.0000000003081000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.687646589.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E11CF06	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	6E11CF06	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	6E0F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0F5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0FCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF61B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CF61B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6CF61B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\de8c058c-b2d1-4c8c-8859-191fc05b8339	unknown	4096	success or wait	1	6CF61B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6CF61B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6CF61B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6CF61B4F	ReadFile

Disassembly

Code Analysis