ID: 382703
Sample Name:
NEW_ORDER.pdf.exe
Cookbook: default.jbs
Time: 14:57:10
Date: 06/04/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report NEW_ORDER.pdf.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Threatname: NanoCore 4
Yara Overview 5
Memory Dumps 5
Unpacked PEs 5
Sigma Overview 6
System Summary: 6
Signature Overview 6
AV Detection: 6
Networking: 6
E-Banking Fraud: 7
System Summary: 7
Data Obfuscation: 7
Boot Survival: 7
Hooking and other Techniques for Hiding and Protection: 7
Malware Analysis System Evasion: 7
HIPS / PFW / Operating System Protection Evasion: 7
Stealing of Sensitive Information: 7
Remote Access Functionality: 7
Mitre Att&ck Matrix 7
Behavior Graph 8
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 9
Domains 10
URLs 10
Domains and IPs 10
Contacted Domains 10
Contacted URLs 11
URLs from Memory and Binaries 11
Contacted IPs 12
Public 12
General Information 12
Simulations 14
Behavior and APIs 14
Joe Sandbox View / Context 14
IPs 14
Domains 15
ASN 15
JA3 Fingerprints 15
Dropped Files 15
Created / dropped Files 15
Static File Info 17
General 17
File Icon 17

Static PE Info 17
General 17
Entrypoint Preview 17
Data Directories 18
Sections 18
Resources 18
Imports 18
Version Infos 18
Network Behavior 19
Network Port Distribution 19
TCP Packets 19
UDP Packets 21
DNS Queries 22
DNS Answers 23
Code Manipulations 23
Statistics 23
Behavior 23
System Behavior 24
Analysis Process: NEW_ORDER.pdf.exe PID: 7156 Parent PID: 5904 24
General 24
File Activities 24
File Created 24
File Deleted 25
File Written 25
File Read 26
Analysis Process: schtasks.exe PID: 5124 Parent PID: 7156 27
General 27
File Activities 27
File Read 27
Analysis Process: conhost.exe PID: 5720 Parent PID: 5124 27
General 27
Analysis Process: RegSvcs.exe PID: 5832 Parent PID: 7156 28
General 28
File Activities 28
File Created 28
File Written 29
File Read 29
Disassembly 29
Code Analysis 29

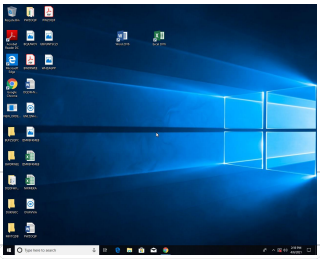
Analysis Report NEW_ORDER.pdf.exe

Overview

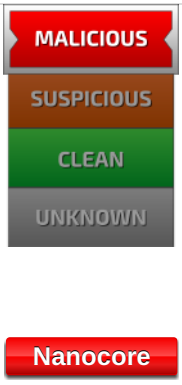
General Information

Sample Name:	NEW_ORDER.pdf.exe
Analysis ID:	382703
MD5:	17bdd9b47882dfb.
SHA1:	fba3196ceef380d..
SHA256:	5802e266beeabe..
Tags:	exe NanoCore
Infos:	

Most interesting Screenshot:



Detection



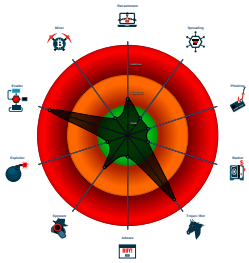
Nanocore

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

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file…
- Yara detected AntiVM3
- Yara detected Nanocore RAT
- .NET source code contains method …
- .NET source code contains potentia…
- C2 URLs / IPs found in malware con…

Classification



Startup

- **System is w10x64**
- NEW_ORDER.pdf.exe (PID: 7156 cmdline: 'C:\Users\user\Desktop\NEW_ORDER.pdf.exe' MD5: 17BDD9B47882DFBA3B0D800F94D7DBC1)
  - schtasks.exe (PID: 5124 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\lmZfKRr' /XML 'C:\Users\user\AppData\Local\Temp\tmp53CF.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5720 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RegSvcs.exe (PID: 5832 cmdline: {path} MD5: 2867A3817C9245F7CF518524DFD18F28)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "6f656d69-7475-8807-1300-000c0a4c",
  "Domain1": "185.140.53.138",
  "Domain2": "wealth2021.ddns.net",
  "Port": 20221,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Disable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "ClearZoneIdentifier": "Disable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Disable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.908113491.000000000514 0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
00000004.00000002.908113491.000000000514 0000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost
00000004.00000002.908113491.000000000514 0000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000004.00000002.903831602.000000000040 2000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8J YUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000004.00000002.903831602.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Click to see the 16 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.RegSvcs.exe.400000.0.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
4.2.RegSvcs.exe.400000.0.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
4.2.RegSvcs.exe.400000.0.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
4.2.RegSvcs.exe.400000.0.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfef5:$a: NanoCore • 0xff05:$a: NanoCore • 0x10139:$a: NanoCore • 0x1014d:$a: NanoCore • 0x1018d:$a: NanoCore • 0xff54:$b: ClientPlugin • 0x10156:$b: ClientPlugin • 0x10196:$b: ClientPlugin • 0x1007b:$c: ProjectData • 0x10a82:$d: DESCrypto • 0x1844e:$e: KeepAlive • 0x1643c:$g: LogClientMessage • 0x12637:$i: get_Connected • 0x10db8:$j: #=q • 0x10de8:$j: #=q • 0x10e04:$j: #=q • 0x10e34:$j: #=q • 0x10e50:$j: #=q • 0x10e6c:$j: #=q • 0x10e9c:$j: #=q • 0x10eb8:$j: #=q
4.2.RegSvcs.exe.5144629.9.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xb184:$x1: NanoCore.ClientPluginHost • 0xb1b1:$x2: IClientNetworkHost
Click to see the 35 entries				

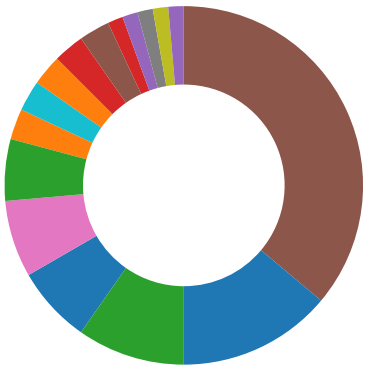
Sigma Overview

System Summary:

Sigma detected: NanoCore

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



- AV Detection
- Compliance
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- 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

Yara detected Nanocore RAT

Networking:

C2 URLs / IPs found in malware configuration

Uses dynamic DNS services

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

.NET source code contains method to dynamically call methods (often used by packers)

.NET source code contains potential unpacker

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Yara detected AntiVM3

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

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

Detected Nanocore Rat

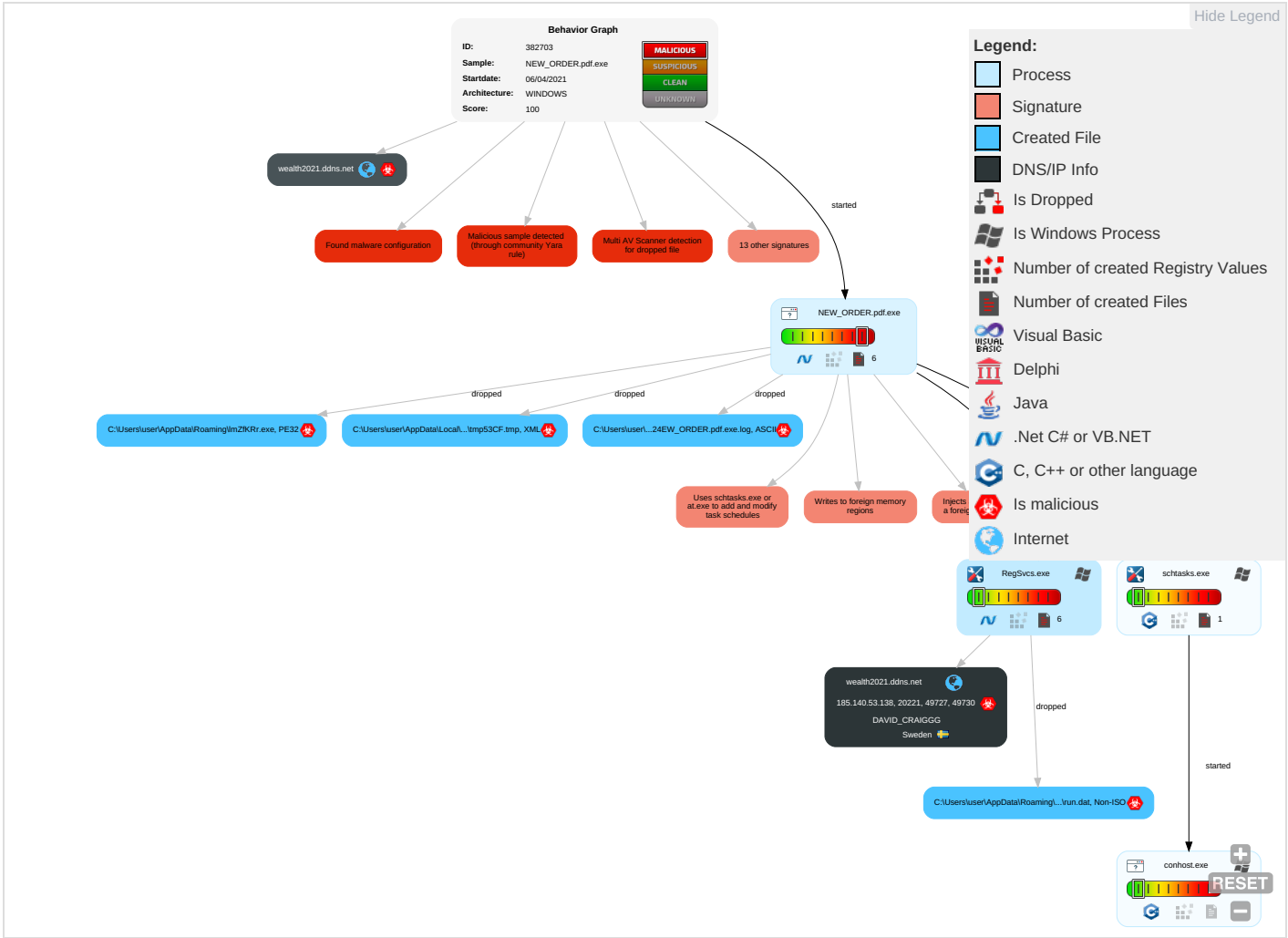
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects
Valid Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Process Injection 2 1 2	Masquerading 1 1	Input Capture 1 1	Security Software Discovery 2 1 1	Remote Services	Input Capture 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesd Insecur Networl Commu
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit Redirec Calls/SI

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Exploit Track D Locatio
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 2 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1	SIM Ca Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 2 1	Manipu Device Commu
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 1 2	Cached Domain Credentials	System Information Discovery 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammir Denial Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 2 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Access

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.pdf.exe	19%	Metadefender		Browse
NEW_ORDER.pdf.exe	47%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\lmZfKRr.exe	19%	Metadefender		Browse
C:\Users\user\AppData\Roaming\lmZfKRr.exe	54%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
4.2.RegSvcs.exe.5140000.8.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
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.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.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	
wealth2021.ddns.net	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://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	
185.140.53.138	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
wealth2021.ddns.net	185.140.53.138	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
wealth2021.ddns.net	true	• Avira URL Cloud: safe	unknown
185.140.53.138	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	NEW_ORDER.pdf.exe, 00000000.00000002.662939421.0000000006B12000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com	NEW_ORDER.pdf.exe, 00000000.00000002.662939421.0000000006B12000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	NEW_ORDER.pdf.exe, 00000000.00000002.662939421.0000000006B12000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	NEW_ORDER.pdf.exe, 00000000.00000002.662939421.0000000006B12000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	NEW_ORDER.pdf.exe, 00000000.00000002.662939421.0000000006B12000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	NEW_ORDER.pdf.exe, 00000000.00000002.662939421.0000000006B12000.00000004.00000001.sdmp	false		high
http://www.tiro.com	NEW_ORDER.pdf.exe, 00000000.00000002.662939421.0000000006B12000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	NEW_ORDER.pdf.exe, 00000000.00000002.662939421.0000000006B12000.00000004.00000001.sdmp	false		high
http://www.goodfont.co.kr	NEW_ORDER.pdf.exe, 00000000.00000002.662939421.0000000006B12000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	NEW_ORDER.pdf.exe, 00000000.00000002.662939421.0000000006B12000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	NEW_ORDER.pdf.exe, 00000000.00000002.662939421.0000000006B12000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	NEW_ORDER.pdf.exe, 00000000.00000002.662939421.0000000006B12000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	NEW_ORDER.pdf.exe, 00000000.00000002.662939421.0000000006B12000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	NEW_ORDER.pdf.exe, 00000000.00000002.662939421.0000000006B12000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	NEW_ORDER.pdf.exe, 00000000.00000002.662939421.0000000006B12000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	NEW_ORDER.pdf.exe, 00000000.00000002.662939421.0000000006B12000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	NEW_ORDER.pdf.exe, 00000000.00000002.662939421.0000000006B12000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	NEW_ORDER.pdf.exe, 00000000.00000002.662939421.0000000006B12000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	NEW_ORDER.pdf.exe, 00000000.00000002.662939421.0000000006B12000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	NEW_ORDER.pdf.exe, 00000000.00000002.662939421.0000000006B12000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tannerhelland.com/4660/dithering-eleven-algorithms-source-code/	NEW_ORDER.pdf.exe	false		high
http://www.fontbureau.com/designers8	NEW_ORDER.pdf.exe, 00000000.00000002.662939421.0000000006B12000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://github.com/Whiplash141/Whips-Image-Converter/releases/latest	NEW_ORDER.pdf.exe	false		high
http://www.fonts.com	NEW_ORDER.pdf.exe, 00000000.000000002.662939421.0000000006B12000.00000004.00000001.sdmp	false		high
http://www.sandoll.co.kr	NEW_ORDER.pdf.exe, 00000000.000000002.662939421.0000000006B12000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://stackoverflow.com/questions/5940188/how-to-convert-a-24-bit-png-to-3-bit-png-using-floyd-ste	NEW_ORDER.pdf.exe	false		high
http://www.efg2.com/Lab/Library/ImageProcessing/DHALF.TXT	NEW_ORDER.pdf.exe	false		high
http://www.urwpp.deDPlease	NEW_ORDER.pdf.exe, 00000000.000000002.662939421.0000000006B12000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	NEW_ORDER.pdf.exe, 00000000.000000002.662939421.0000000006B12000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	NEW_ORDER.pdf.exe, 00000000.000000002.665162901.0000000007943000.00000004.00000001.sdmp	false		high
http://www.sakkal.com	NEW_ORDER.pdf.exe, 00000000.000000002.662939421.0000000006B12000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.140.53.138	wealth2021.ddns.net	Sweden		209623	DAVID_CRAIGGG	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	382703
Start date:	06.04.2021

Start time:	14:57:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 17s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	NEW_ORDER.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:	19
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.evad.winEXE@6/4@11/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0% (good quality ratio 0%) • Quality average: 85% • Quality standard deviation: 17.6%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • TCP Packets have been reduced to 100 • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 13.107.246.254, 104.43.193.48, 52.147.198.201, 20.82.209.183, 92.122.213.194, 92.122.213.247, 13.88.21.125, 52.155.217.156, 20.54.26.129, 2.20.142.209, 2.20.142.210, 20.82.210.154, 52.255.188.83, 20.50.102.62 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, t-ring.msedge.net, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, t-9999.t-msedge.net, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, t-ring.t-9999.t-msedge.net, skypedataprdcolwus15.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.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/382703/sample/NEW_ORDER.pdf.exe

Simulations

Behavior and APIs

Time	Type	Description
14:57:58	API Interceptor	2x Sleep call for process: NEW_ORDER.pdf.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.140.53.138	Quotation_Request.pdf.exe	Get hash	malicious	Browse	
	URGENT_ORDER.pdf.exe	Get hash	malicious	Browse	
	Purchase_Order.pdf.exe	Get hash	malicious	Browse	
	1PH37n4Gva.exe	Get hash	malicious	Browse	
	35dbds3GQG.exe	Get hash	malicious	Browse	
	QXJGE2LOdP.exe	Get hash	malicious	Browse	
	O4m3hDFNbh.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	nrv_remittance#U007eorder#U007epayment.exe	Get hash	malicious	Browse	
	NEW ORDER REQUEST_EXPORT005JKL DOC.exe	Get hash	malicious	Browse	
	WIRE COPY ORDER T104484_PP.exe	Get hash	malicious	Browse	
	71AXBkD1wA.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
wealth2021.ddns.net	Quotation_Request.pdf.exe	Get hash	malicious	Browse	• 185.140.53.138
	URGENT_ORDER.pdf.exe	Get hash	malicious	Browse	• 185.140.53.138
	Purchase_Order.pdf.exe	Get hash	malicious	Browse	• 185.140.53.138

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DAVID_CRAIGGG	Doc_58YJ54-521DERG701-55YH701.exe	Get hash	malicious	Browse	• 185.140.53.230
	Quotation_Request.pdf.exe	Get hash	malicious	Browse	• 185.140.53.138
	FRQ_05694 revised quantity.exe	Get hash	malicious	Browse	• 185.140.53.69
	INVOICE 15112021.xlsx	Get hash	malicious	Browse	• 185.140.53.130
	URGENT_ORDER.pdf.exe	Get hash	malicious	Browse	• 185.140.53.138
	IMG-001982-AW00173-SSE73I.exe	Get hash	malicious	Browse	• 185.140.53.230
	FYI-Orderimg.exe	Get hash	malicious	Browse	• 185.140.53.67
	Purchase_Order.pdf.exe	Get hash	malicious	Browse	• 185.140.53.138
	PO-94765809570-Order pdf.exe	Get hash	malicious	Browse	• 185.140.53.7
	Commercial E-invoice.exe	Get hash	malicious	Browse	• 185.140.53.137
	Order23032021.xls	Get hash	malicious	Browse	• 185.140.53.130
	ZcQwvgqtuQ.exe	Get hash	malicious	Browse	• 91.193.75.245
	lKIPqaYkKB.exe	Get hash	malicious	Browse	• 185.140.53.161
	t5R60D503x.exe	Get hash	malicious	Browse	• 185.140.53.9
	Purchase OrderDated19032021.xls	Get hash	malicious	Browse	• 185.140.53.130
	0u1JLpIwRo.exe	Get hash	malicious	Browse	• 185.140.53.139
	PO-21322.xlsm	Get hash	malicious	Browse	• 185.165.153.116
	GT_0397337_03987638BNG.exe	Get hash	malicious	Browse	• 185.140.53.9
	5woB0vy0X6.exe	Get hash	malicious	Browse	• 185.140.53.139
	Doc_IMAGE-587HTY-9545-55401.exe	Get hash	malicious	Browse	• 185.140.53.230

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\NEW_ORDER.pdf.exe.log

Process:	C:\Users\user\Desktop\NEW_ORDER.pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	**true**
Reputation:	high, very likely benign file

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\NEW_ORDER.pdf.exe.log	
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\tmp53CF.tmp	
Process:	C:\Users\user\Desktop\NEW_ORDER.pdf.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1640
Entropy (8bit):	5.176392077301857
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGCaItn:cbhK79lNQR/rydbz9I3YODOLNdq3Z
MD5:	39E567FE518CA8EDB0AD37D54E7A6104
SHA1:	59C9DFBF1A6CB4EF179AE5B8FFBB37DE4571A5EE
SHA-256:	78F5BB3FDBB676F649A6165362193FF71DA638D9021B8AD8DC464C891EC84A42
SHA-512:	0A1E9A361C3F2FD0F0324A07F631E51830E4398D201798CA69A4112EABB88E37D1E2EB4C51B3E5D1D6CB7715F8901C6A3E551B730831D8C70C1C356EBA7B763
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	Non-ISO extended-ASCII text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:f7/t:Tl
MD5:	BA96EE5A0ADF7C7F588EAADA2E18CF3A
SHA1:	9F751596B956F6C75FD2E4F447979A0DDB859F08
SHA-256:	9D3F3D537AE6BDBD90E1CA94DCA09925A05D9CE84EA9FB0605F19BDF8676EFC1
SHA-512:	7EEBED8E803D20FB77A11215F5AE9B1070FA9F169A4021E4F38ADB14D082B4CA3EE6C8948028F0AD58DE8E1231E01749C0088F861EFA5CA5C905DB1E61DBBD05
Malicious:	**true**
Reputation:	low
Preview:	.....H

C:\Users\user\AppData\Roaming\lmZfKRr.exe	
Process:	C:\Users\user\Desktop\NEW_ORDER.pdf.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	812032
Entropy (8bit):	7.87719204655292
Encrypted:	false
SSDEEP:	12288:6ofCEqJj8Sm2zaxyc8flJ34zphf/ctoaTTrkY0tt7T4tWAOFNViq78PcuYl:6oaEqRMyVfl8n3gT4JbY8Ji2M
MD5:	17BDD9B47882DFBA3B0D800F94D7DBC1
SHA1:	FBA3196CEEF380D49C18322BA1201B1AFB9C9991
SHA-256:	5802E266BEEABE10852B45EE17C86E9C7C8B62BC155848C809D3781E1B7A9123
SHA-512:	5518F9FED2B8CBC3885954A30ADCB8756CED23EFF41C53A3F3DAEAD31F83169A84BD21E6636AA632A18E735B9519F25EA845370E382F7F92C0C4DFB360EE083
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 19%, Browse • Antivirus: ReversingLabs, Detection: 54%
Reputation:	low

C:\Users\user\AppData\Roaming\ImZfKRr.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....k`.....0..Z.....^v... .....@.. ..... ..@.....v..O..... ..... ..H.....text....X... ...Z..... ..`.rsrc.....\.....@..@.reloc..... .....b.....@..B.....@v.....H.....0.....r...p.+..*..0.....r...p.+..*"(.....*.0..G.....}.....}.....}..... ....}..... .....(.....b`. (.....b`.(....`}....*..0..D.....}.....}.....}.....}..... ....(.....b`.(.....b`.(....`}....*.0..+..... .....,.. .....+.....,.....+..*..0..>.....{.....{....Y(.....{.....{....Y(....X.{.....{....Y(....X.+..*...0.... .....{....(.....+..*....0.....".....(...

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.87719204655292
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.pdf.exe
File size:	812032
MD5:	17bdd9b47882dfba3b0d800f94d7dbc1
SHA1:	fba3196ceef380d49c18322ba1201b1afb9c9991
SHA256:	5802e266beeabe10852b45ee17c86e9c7c8b62bc155848c809d3781e1b7a9123
SHA512:	5518f9fed2b8cbc3885954a30adcb8756ced23eff41c53a3f3daead31f83169a84bd21e6636aa632a18e735b9519f25ea845370e382f7f92c0c4dfb360ee08f3
SSDEEP:	12288:6ofCEqJj8Sm2zaxyc8flJ34zphf/ctoaTTrkY0tt7T4tWAOFNViq78PcuYl:6oaEqRMyVfl8n3gT4JbY8Ji2M
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....k`.....0..Z.....^v... .....@.. ....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4c765e
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:	0x606B83FC [Mon Apr 5 21:41:16 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 eax, 00000000h
add byte ptr [eax], al
add byte ptr [ecx], al
add byte ptr [eax], al
add byte ptr [ebx], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [edx], al
add byte ptr [eax], al
add byte ptr [edx], al
add byte ptr [eax], al
add byte ptr [ecx], al
add byte ptr [eax], al
add dh, bh

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xc760c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xc8000	0x5ac	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xca000	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	0xc58ac	0xc5a00	False	0.899721052736	data	7.88331546414	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xc8000	0x5ac	0x600	False	0.424479166667	data	4.11601272417	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xca000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xc8090	0x31c	data		
RT_MANIFEST	0xc83bc	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

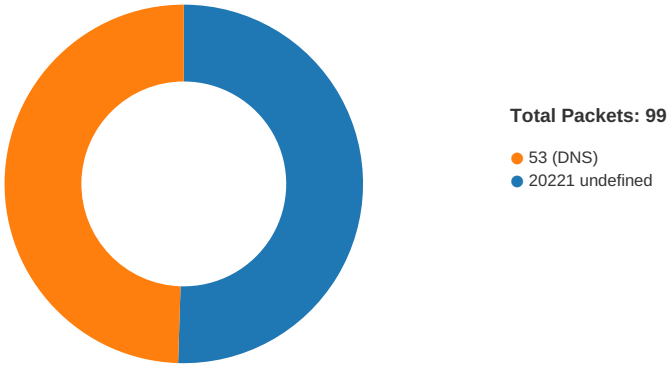
Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2014
Assembly Version	1.0.0.0

Description	Data
InternalName	y.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	SqlFormatter
ProductVersion	1.0.0.0
FileDescription	SqlFormatter
OriginalFilename	y.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 6, 2021 14:58:05.147273064 CEST	49727	20221	192.168.2.4	185.140.53.138
Apr 6, 2021 14:58:05.193897009 CEST	20221	49727	185.140.53.138	192.168.2.4
Apr 6, 2021 14:58:05.705436945 CEST	49727	20221	192.168.2.4	185.140.53.138
Apr 6, 2021 14:58:05.753998041 CEST	20221	49727	185.140.53.138	192.168.2.4
Apr 6, 2021 14:58:06.268091917 CEST	49727	20221	192.168.2.4	185.140.53.138
Apr 6, 2021 14:58:06.314373970 CEST	20221	49727	185.140.53.138	192.168.2.4
Apr 6, 2021 14:58:10.430963039 CEST	49730	20221	192.168.2.4	185.140.53.138
Apr 6, 2021 14:58:10.478168011 CEST	20221	49730	185.140.53.138	192.168.2.4
Apr 6, 2021 14:58:10.986983061 CEST	49730	20221	192.168.2.4	185.140.53.138
Apr 6, 2021 14:58:11.034450054 CEST	20221	49730	185.140.53.138	192.168.2.4
Apr 6, 2021 14:58:11.549582005 CEST	49730	20221	192.168.2.4	185.140.53.138
Apr 6, 2021 14:58:11.597069025 CEST	20221	49730	185.140.53.138	192.168.2.4
Apr 6, 2021 14:58:15.614948034 CEST	49732	20221	192.168.2.4	185.140.53.138
Apr 6, 2021 14:58:15.662126064 CEST	20221	49732	185.140.53.138	192.168.2.4
Apr 6, 2021 14:58:16.174989939 CEST	49732	20221	192.168.2.4	185.140.53.138
Apr 6, 2021 14:58:16.220699072 CEST	20221	49732	185.140.53.138	192.168.2.4
Apr 6, 2021 14:58:16.721911907 CEST	49732	20221	192.168.2.4	185.140.53.138
Apr 6, 2021 14:58:16.768621922 CEST	20221	49732	185.140.53.138	192.168.2.4
Apr 6, 2021 14:58:20.933881998 CEST	49736	20221	192.168.2.4	185.140.53.138
Apr 6, 2021 14:58:20.979547977 CEST	20221	49736	185.140.53.138	192.168.2.4
Apr 6, 2021 14:58:21.487879992 CEST	49736	20221	192.168.2.4	185.140.53.138
Apr 6, 2021 14:58:21.533593893 CEST	20221	49736	185.140.53.138	192.168.2.4
Apr 6, 2021 14:58:22.034960985 CEST	49736	20221	192.168.2.4	185.140.53.138
Apr 6, 2021 14:58:22.080630064 CEST	20221	49736	185.140.53.138	192.168.2.4
Apr 6, 2021 14:58:26.146341085 CEST	49738	20221	192.168.2.4	185.140.53.138
Apr 6, 2021 14:58:26.192018032 CEST	20221	49738	185.140.53.138	192.168.2.4
Apr 6, 2021 14:58:26.707721949 CEST	49738	20221	192.168.2.4	185.140.53.138

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 6, 2021 14:58:26.753480911 CEST	20221	49738	185.140.53.138	192.168.2.4
Apr 6, 2021 14:58:27.254050016 CEST	49738	20221	192.168.2.4	185.140.53.138
Apr 6, 2021 14:58:27.299705029 CEST	20221	49738	185.140.53.138	192.168.2.4
Apr 6, 2021 14:58:31.387415886 CEST	49740	20221	192.168.2.4	185.140.53.138
Apr 6, 2021 14:58:31.433103085 CEST	20221	49740	185.140.53.138	192.168.2.4
Apr 6, 2021 14:58:31.941874981 CEST	49740	20221	192.168.2.4	185.140.53.138
Apr 6, 2021 14:58:31.988670111 CEST	20221	49740	185.140.53.138	192.168.2.4
Apr 6, 2021 14:58:32.488835096 CEST	49740	20221	192.168.2.4	185.140.53.138
Apr 6, 2021 14:58:32.536633968 CEST	20221	49740	185.140.53.138	192.168.2.4
Apr 6, 2021 14:58:36.553973913 CEST	49746	20221	192.168.2.4	185.140.53.138
Apr 6, 2021 14:58:36.599664927 CEST	20221	49746	185.140.53.138	192.168.2.4
Apr 6, 2021 14:58:37.114222050 CEST	49746	20221	192.168.2.4	185.140.53.138
Apr 6, 2021 14:58:37.159900904 CEST	20221	49746	185.140.53.138	192.168.2.4
Apr 6, 2021 14:58:37.661113977 CEST	49746	20221	192.168.2.4	185.140.53.138
Apr 6, 2021 14:58:37.706602097 CEST	20221	49746	185.140.53.138	192.168.2.4
Apr 6, 2021 14:58:41.710304022 CEST	49753	20221	192.168.2.4	185.140.53.138
Apr 6, 2021 14:58:41.757996082 CEST	20221	49753	185.140.53.138	192.168.2.4
Apr 6, 2021 14:58:42.270863056 CEST	49753	20221	192.168.2.4	185.140.53.138
Apr 6, 2021 14:58:42.317116022 CEST	20221	49753	185.140.53.138	192.168.2.4
Apr 6, 2021 14:58:42.817785978 CEST	49753	20221	192.168.2.4	185.140.53.138
Apr 6, 2021 14:58:42.865220070 CEST	20221	49753	185.140.53.138	192.168.2.4
Apr 6, 2021 14:58:46.885031939 CEST	49756	20221	192.168.2.4	185.140.53.138
Apr 6, 2021 14:58:46.933924913 CEST	20221	49756	185.140.53.138	192.168.2.4
Apr 6, 2021 14:58:47.443211079 CEST	49756	20221	192.168.2.4	185.140.53.138
Apr 6, 2021 14:58:47.488663912 CEST	20221	49756	185.140.53.138	192.168.2.4
Apr 6, 2021 14:58:47.990066051 CEST	49756	20221	192.168.2.4	185.140.53.138
Apr 6, 2021 14:58:48.035806894 CEST	20221	49756	185.140.53.138	192.168.2.4
Apr 6, 2021 14:58:52.108846903 CEST	49760	20221	192.168.2.4	185.140.53.138
Apr 6, 2021 14:58:52.154328108 CEST	20221	49760	185.140.53.138	192.168.2.4
Apr 6, 2021 14:58:52.662341118 CEST	49760	20221	192.168.2.4	185.140.53.138
Apr 6, 2021 14:58:52.708293915 CEST	20221	49760	185.140.53.138	192.168.2.4
Apr 6, 2021 14:58:53.225085974 CEST	49760	20221	192.168.2.4	185.140.53.138
Apr 6, 2021 14:58:53.270534039 CEST	20221	49760	185.140.53.138	192.168.2.4
Apr 6, 2021 14:58:57.388636112 CEST	49769	20221	192.168.2.4	185.140.53.138
Apr 6, 2021 14:58:57.434137106 CEST	20221	49769	185.140.53.138	192.168.2.4
Apr 6, 2021 14:58:57.944029093 CEST	49769	20221	192.168.2.4	185.140.53.138
Apr 6, 2021 14:58:57.989775896 CEST	20221	49769	185.140.53.138	192.168.2.4
Apr 6, 2021 14:58:58.490963936 CEST	49769	20221	192.168.2.4	185.140.53.138
Apr 6, 2021 14:58:58.536823988 CEST	20221	49769	185.140.53.138	192.168.2.4
Apr 6, 2021 14:59:02.606455088 CEST	49770	20221	192.168.2.4	185.140.53.138
Apr 6, 2021 14:59:02.652405977 CEST	20221	49770	185.140.53.138	192.168.2.4
Apr 6, 2021 14:59:03.163347006 CEST	49770	20221	192.168.2.4	185.140.53.138
Apr 6, 2021 14:59:03.209135056 CEST	20221	49770	185.140.53.138	192.168.2.4
Apr 6, 2021 14:59:03.710362911 CEST	49770	20221	192.168.2.4	185.140.53.138
Apr 6, 2021 14:59:03.757666111 CEST	20221	49770	185.140.53.138	192.168.2.4
Apr 6, 2021 14:59:07.778412104 CEST	49772	20221	192.168.2.4	185.140.53.138
Apr 6, 2021 14:59:07.863007069 CEST	20221	49772	185.140.53.138	192.168.2.4
Apr 6, 2021 14:59:08.366944075 CEST	49772	20221	192.168.2.4	185.140.53.138
Apr 6, 2021 14:59:08.412867069 CEST	20221	49772	185.140.53.138	192.168.2.4
Apr 6, 2021 14:59:08.913778067 CEST	49772	20221	192.168.2.4	185.140.53.138
Apr 6, 2021 14:59:08.960371971 CEST	20221	49772	185.140.53.138	192.168.2.4
Apr 6, 2021 14:59:12.979665041 CEST	49774	20221	192.168.2.4	185.140.53.138
Apr 6, 2021 14:59:13.025278091 CEST	20221	49774	185.140.53.138	192.168.2.4
Apr 6, 2021 14:59:13.539076090 CEST	49774	20221	192.168.2.4	185.140.53.138
Apr 6, 2021 14:59:13.586205006 CEST	20221	49774	185.140.53.138	192.168.2.4
Apr 6, 2021 14:59:14.085994959 CEST	49774	20221	192.168.2.4	185.140.53.138
Apr 6, 2021 14:59:14.133135080 CEST	20221	49774	185.140.53.138	192.168.2.4
Apr 6, 2021 14:59:18.151887894 CEST	49778	20221	192.168.2.4	185.140.53.138
Apr 6, 2021 14:59:18.197343111 CEST	20221	49778	185.140.53.138	192.168.2.4
Apr 6, 2021 14:59:18.711524010 CEST	49778	20221	192.168.2.4	185.140.53.138
Apr 6, 2021 14:59:18.757230997 CEST	20221	49778	185.140.53.138	192.168.2.4
Apr 6, 2021 14:59:19.258344889 CEST	49778	20221	192.168.2.4	185.140.53.138
Apr 6, 2021 14:59:19.304474115 CEST	20221	49778	185.140.53.138	192.168.2.4
Apr 6, 2021 14:59:23.446026087 CEST	49780	20221	192.168.2.4	185.140.53.138

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 6, 2021 14:59:23.491497993 CEST	20221	49780	185.140.53.138	192.168.2.4
Apr 6, 2021 14:59:23.993082047 CEST	49780	20221	192.168.2.4	185.140.53.138
Apr 6, 2021 14:59:24.038691044 CEST	20221	49780	185.140.53.138	192.168.2.4
Apr 6, 2021 14:59:24.540031910 CEST	49780	20221	192.168.2.4	185.140.53.138
Apr 6, 2021 14:59:24.588740110 CEST	20221	49780	185.140.53.138	192.168.2.4
Apr 6, 2021 14:59:28.667238951 CEST	49785	20221	192.168.2.4	185.140.53.138
Apr 6, 2021 14:59:28.712775946 CEST	20221	49785	185.140.53.138	192.168.2.4
Apr 6, 2021 14:59:29.227895021 CEST	49785	20221	192.168.2.4	185.140.53.138
Apr 6, 2021 14:59:29.277070045 CEST	20221	49785	185.140.53.138	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 6, 2021 14:57:46.748694897 CEST	53	53097	8.8.8.8	192.168.2.4
Apr 6, 2021 14:58:07.602477074 CEST	49257	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:58:07.648535967 CEST	53	49257	8.8.8.8	192.168.2.4
Apr 6, 2021 14:58:09.684362888 CEST	62389	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:58:09.741121054 CEST	53	62389	8.8.8.8	192.168.2.4
Apr 6, 2021 14:58:11.050416946 CEST	49910	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:58:11.096380949 CEST	53	49910	8.8.8.8	192.168.2.4
Apr 6, 2021 14:58:17.354785919 CEST	55854	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:58:17.401576042 CEST	53	55854	8.8.8.8	192.168.2.4
Apr 6, 2021 14:58:18.336270094 CEST	64549	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:58:18.383507967 CEST	53	64549	8.8.8.8	192.168.2.4
Apr 6, 2021 14:58:20.874919891 CEST	63153	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:58:20.931477070 CEST	53	63153	8.8.8.8	192.168.2.4
Apr 6, 2021 14:58:21.728527069 CEST	52991	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:58:21.788741112 CEST	53	52991	8.8.8.8	192.168.2.4
Apr 6, 2021 14:58:26.085705042 CEST	53700	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:58:26.144759893 CEST	53	53700	8.8.8.8	192.168.2.4
Apr 6, 2021 14:58:28.425663948 CEST	51726	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:58:28.471601009 CEST	53	51726	8.8.8.8	192.168.2.4
Apr 6, 2021 14:58:31.320842028 CEST	56794	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:58:31.377226114 CEST	53	56794	8.8.8.8	192.168.2.4
Apr 6, 2021 14:58:34.628859043 CEST	56534	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:58:34.702776909 CEST	53	56534	8.8.8.8	192.168.2.4
Apr 6, 2021 14:58:35.198931932 CEST	56627	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:58:35.253509998 CEST	53	56627	8.8.8.8	192.168.2.4
Apr 6, 2021 14:58:35.688895941 CEST	56621	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:58:35.747694016 CEST	53	56621	8.8.8.8	192.168.2.4
Apr 6, 2021 14:58:35.822873116 CEST	63116	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:58:35.887654066 CEST	53	63116	8.8.8.8	192.168.2.4
Apr 6, 2021 14:58:36.201570988 CEST	64078	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:58:36.256244898 CEST	53	64078	8.8.8.8	192.168.2.4
Apr 6, 2021 14:58:36.819554090 CEST	64801	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:58:36.876899958 CEST	53	64801	8.8.8.8	192.168.2.4
Apr 6, 2021 14:58:37.470235109 CEST	61721	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:58:37.533876896 CEST	53	61721	8.8.8.8	192.168.2.4
Apr 6, 2021 14:58:38.127764940 CEST	51255	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:58:38.361290932 CEST	53	51255	8.8.8.8	192.168.2.4
Apr 6, 2021 14:58:39.233196974 CEST	61522	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:58:39.367219925 CEST	53	61522	8.8.8.8	192.168.2.4
Apr 6, 2021 14:58:40.333481073 CEST	52337	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:58:40.387959003 CEST	53	52337	8.8.8.8	192.168.2.4
Apr 6, 2021 14:58:40.933494091 CEST	55046	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:58:40.989588976 CEST	53	55046	8.8.8.8	192.168.2.4
Apr 6, 2021 14:58:42.355596066 CEST	49612	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:58:42.410073042 CEST	53	49612	8.8.8.8	192.168.2.4
Apr 6, 2021 14:58:46.368907928 CEST	49285	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:58:46.415062904 CEST	53	49285	8.8.8.8	192.168.2.4
Apr 6, 2021 14:58:47.166907072 CEST	50601	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:58:47.217428923 CEST	53	50601	8.8.8.8	192.168.2.4
Apr 6, 2021 14:58:48.060162067 CEST	60875	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:58:48.107306004 CEST	53	60875	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 6, 2021 14:58:49.156021118 CEST	56448	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:58:49.215174913 CEST	53	56448	8.8.8.8	192.168.2.4
Apr 6, 2021 14:58:52.061729908 CEST	59172	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:58:52.107770920 CEST	53	59172	8.8.8.8	192.168.2.4
Apr 6, 2021 14:58:52.903748989 CEST	62420	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:58:52.953758955 CEST	53	62420	8.8.8.8	192.168.2.4
Apr 6, 2021 14:58:53.029941082 CEST	60579	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:58:53.099467039 CEST	53	60579	8.8.8.8	192.168.2.4
Apr 6, 2021 14:58:55.085230112 CEST	50183	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:58:55.142219067 CEST	53	50183	8.8.8.8	192.168.2.4
Apr 6, 2021 14:58:57.291249037 CEST	61531	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:58:57.350332975 CEST	53	61531	8.8.8.8	192.168.2.4
Apr 6, 2021 14:59:02.557887077 CEST	49228	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:59:02.604027987 CEST	53	49228	8.8.8.8	192.168.2.4
Apr 6, 2021 14:59:03.820203066 CEST	59794	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:59:03.866555929 CEST	53	59794	8.8.8.8	192.168.2.4
Apr 6, 2021 14:59:11.376476049 CEST	55916	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:59:11.423827887 CEST	53	55916	8.8.8.8	192.168.2.4
Apr 6, 2021 14:59:16.137386084 CEST	52752	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:59:16.183969975 CEST	53	52752	8.8.8.8	192.168.2.4
Apr 6, 2021 14:59:16.904125929 CEST	60542	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:59:16.952917099 CEST	53	60542	8.8.8.8	192.168.2.4
Apr 6, 2021 14:59:17.676310062 CEST	60689	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:59:17.722225904 CEST	53	60689	8.8.8.8	192.168.2.4
Apr 6, 2021 14:59:18.516988993 CEST	64206	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:59:18.563946962 CEST	53	64206	8.8.8.8	192.168.2.4
Apr 6, 2021 14:59:23.389594078 CEST	50904	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:59:23.444430113 CEST	53	50904	8.8.8.8	192.168.2.4
Apr 6, 2021 14:59:23.781377077 CEST	57525	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:59:23.827682972 CEST	53	57525	8.8.8.8	192.168.2.4
Apr 6, 2021 14:59:24.987293959 CEST	53814	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:59:25.033330917 CEST	53	53814	8.8.8.8	192.168.2.4
Apr 6, 2021 14:59:26.107867002 CEST	53418	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:59:26.159982920 CEST	53	53418	8.8.8.8	192.168.2.4
Apr 6, 2021 14:59:27.300051928 CEST	62833	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:59:27.346029997 CEST	53	62833	8.8.8.8	192.168.2.4
Apr 6, 2021 14:59:28.606669903 CEST	59260	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:59:28.665932894 CEST	53	59260	8.8.8.8	192.168.2.4
Apr 6, 2021 14:59:29.426521063 CEST	49944	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:59:29.473968029 CEST	53	49944	8.8.8.8	192.168.2.4
Apr 6, 2021 14:59:31.196513891 CEST	63300	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:59:31.255347013 CEST	53	63300	8.8.8.8	192.168.2.4
Apr 6, 2021 14:59:33.841094971 CEST	61449	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:59:33.897640944 CEST	53	61449	8.8.8.8	192.168.2.4
Apr 6, 2021 14:59:54.621431112 CEST	51275	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:59:54.680380106 CEST	53	51275	8.8.8.8	192.168.2.4
Apr 6, 2021 14:59:59.856945038 CEST	63492	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:59:59.913978100 CEST	53	63492	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 6, 2021 14:58:20.874919891 CEST	192.168.2.4	8.8.8.8	0x41c0	Standard query (0)	wealth2021 .ddns.net	A (IP address)	IN (0x0001)
Apr 6, 2021 14:58:26.085705042 CEST	192.168.2.4	8.8.8.8	0xc9af	Standard query (0)	wealth2021 .ddns.net	A (IP address)	IN (0x0001)
Apr 6, 2021 14:58:31.320842028 CEST	192.168.2.4	8.8.8.8	0xb36b	Standard query (0)	wealth2021 .ddns.net	A (IP address)	IN (0x0001)
Apr 6, 2021 14:58:52.061729908 CEST	192.168.2.4	8.8.8.8	0x5b64	Standard query (0)	wealth2021 .ddns.net	A (IP address)	IN (0x0001)
Apr 6, 2021 14:58:57.291249037 CEST	192.168.2.4	8.8.8.8	0xfb07	Standard query (0)	wealth2021 .ddns.net	A (IP address)	IN (0x0001)
Apr 6, 2021 14:59:02.557887077 CEST	192.168.2.4	8.8.8.8	0xa550	Standard query (0)	wealth2021 .ddns.net	A (IP address)	IN (0x0001)
Apr 6, 2021 14:59:23.389594078 CEST	192.168.2.4	8.8.8.8	0x2ee3	Standard query (0)	wealth2021 .ddns.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 6, 2021 14:59:28.606669903 CEST	192.168.2.4	8.8.8.8	0x2cfb	Standard query (0)	wealth2021 .ddns.net	A (IP address)	IN (0x0001)
Apr 6, 2021 14:59:33.841094971 CEST	192.168.2.4	8.8.8.8	0x9973	Standard query (0)	wealth2021 .ddns.net	A (IP address)	IN (0x0001)
Apr 6, 2021 14:59:54.621431112 CEST	192.168.2.4	8.8.8.8	0x29f2	Standard query (0)	wealth2021 .ddns.net	A (IP address)	IN (0x0001)
Apr 6, 2021 14:59:59.856945038 CEST	192.168.2.4	8.8.8.8	0xb40c	Standard query (0)	wealth2021 .ddns.net	A (IP address)	IN (0x0001)

DNS Answers

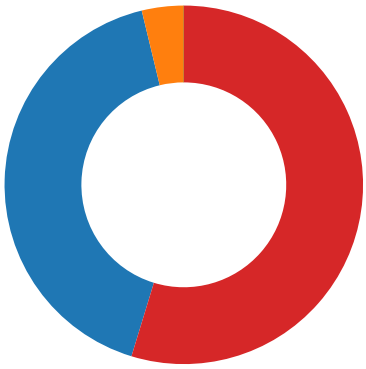
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 6, 2021 14:58:20.931477070 CEST	8.8.8.8	192.168.2.4	0x41c0	No error (0)	wealth2021 .ddns.net		185.140.53.138	A (IP address)	IN (0x0001)
Apr 6, 2021 14:58:26.144759893 CEST	8.8.8.8	192.168.2.4	0xc9af	No error (0)	wealth2021 .ddns.net		185.140.53.138	A (IP address)	IN (0x0001)
Apr 6, 2021 14:58:31.377226114 CEST	8.8.8.8	192.168.2.4	0xb36b	No error (0)	wealth2021 .ddns.net		185.140.53.138	A (IP address)	IN (0x0001)
Apr 6, 2021 14:58:52.107770920 CEST	8.8.8.8	192.168.2.4	0x5b64	No error (0)	wealth2021 .ddns.net		185.140.53.138	A (IP address)	IN (0x0001)
Apr 6, 2021 14:58:57.350332975 CEST	8.8.8.8	192.168.2.4	0xfb07	No error (0)	wealth2021 .ddns.net		185.140.53.138	A (IP address)	IN (0x0001)
Apr 6, 2021 14:59:02.604027987 CEST	8.8.8.8	192.168.2.4	0xa550	No error (0)	wealth2021 .ddns.net		185.140.53.138	A (IP address)	IN (0x0001)
Apr 6, 2021 14:59:23.444430113 CEST	8.8.8.8	192.168.2.4	0x2ee3	No error (0)	wealth2021 .ddns.net		185.140.53.138	A (IP address)	IN (0x0001)
Apr 6, 2021 14:59:28.665932894 CEST	8.8.8.8	192.168.2.4	0x2cfb	No error (0)	wealth2021 .ddns.net		185.140.53.138	A (IP address)	IN (0x0001)
Apr 6, 2021 14:59:33.897640944 CEST	8.8.8.8	192.168.2.4	0x9973	No error (0)	wealth2021 .ddns.net		185.140.53.138	A (IP address)	IN (0x0001)
Apr 6, 2021 14:59:54.680380106 CEST	8.8.8.8	192.168.2.4	0x29f2	No error (0)	wealth2021 .ddns.net		185.140.53.138	A (IP address)	IN (0x0001)
Apr 6, 2021 14:59:59.913978100 CEST	8.8.8.8	192.168.2.4	0xb40c	No error (0)	wealth2021 .ddns.net		185.140.53.138	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

- NEW_ORDER.pdf.exe
- schtasks.exe
- conhost.exe
- RegSvcs.exe



Click to jump to process

System Behavior

Analysis Process: NEW_ORDER.pdf.exe PID: 7156 Parent PID: 5904

General

Start time:	14:57:53
Start date:	06/04/2021
Path:	C:\Users\user\Desktop\NEW_ORDER.pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\NEW_ORDER.pdf.exe'
Imagebase:	0x620000
File size:	812032 bytes
MD5 hash:	17BDD9B47882DFBA3B0D800F94D7DBC1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.657514928.0000000003B9A000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.657514928.0000000003B9A000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.657514928.0000000003B9A000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
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	6D1CCF06	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	6D1CCF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\lmZfKRr.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C011E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp53CF.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C017038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\NEW_ORDER.pdf.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D4DC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp53CF.tmp	success or wait	1	6C016A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\lmZfKRr.exe	unknown	812032	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 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 fc 83 6b 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 5a 0c 00 00 08 00 00 00 00 00 00 5e 76 0c 00 00 20 00 00 00 80 0c 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 c0 0c 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.....k`.......... ....0..Z..........^v... ....@.. ....@................	success or wait	1	6C011B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp53CF.tmp	unknown	1640	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 6a 6f 6e 65 73 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 6e 49 6e	<?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>.. </RegistrationIn	success or wait	1	6C011B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\NEW_ORDER.pdf.exe.log	unknown	1216	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	6D4DC907	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	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D1A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1ACA54	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	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Users\user\Desktop\NEW_ORDER.pdf.exe	unknown	812032	success or wait	1	6C011B4F	ReadFile

Analysis Process: schtasks.exe PID: 5124 Parent PID: 7156

General

Start time:	14:58:01
Start date:	06/04/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\lmZfKRr' /XML 'C:\Users\ user\AppData\Local\Temp\tmp53CF.tmp'
Imagebase:	0x1330000
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\tmp53CF.tmp	unknown	2	success or wait	1	133AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp53CF.tmp	unknown	1641	success or wait	1	133ABD9	ReadFile

Analysis Process: conhost.exe PID: 5720 Parent PID: 5124

General

Start time:	14:58:01
Start date:	06/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RegSvcs.exe PID: 5832 Parent PID: 7156

General

Start time:	14:58:01
Start date:	06/04/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x460000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.908113491.0000000005140000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.908113491.0000000005140000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.908113491.0000000005140000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.903831602.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.903831602.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.903831602.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.908094344.0000000005130000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.908094344.0000000005130000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.905010283.0000000002981000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.905761481.00000000039C9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.905761481.00000000039C9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	high

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	6D1CCF06	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	6D1CCF06	unknown
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C01BEFF	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C011E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C01BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C01BEFF	CreateDirectoryW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	unknown	8	af e1 aa 9d fb f8 d8 48	.....H	success or wait	1	6C011B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D1A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6D1ACA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6D1ACA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe	unknown	4096	success or wait	1	6D18D72F	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe	unknown	512	success or wait	1	6D18D72F	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6D1A5705	unknown

Disassembly

Code Analysis