ID: 339042
Sample Name: order-181289654312464648.exe
Cookbook: default.jbs
Time: 10:15:43
Date: 13/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

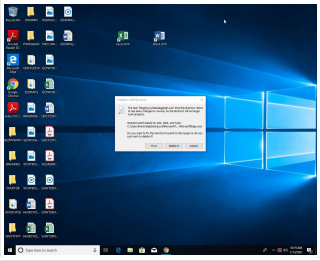
Analysis Report order-181289654312464648.exe

Overview

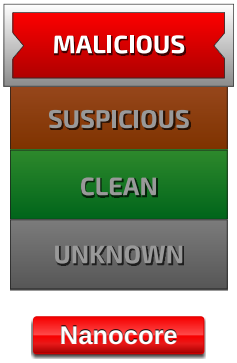
General Information

Sample Name:	order-181289654312464648.exe
Analysis ID:	339042
MD5:	28da42c2cd57e5..
SHA1:	81c980f2cda9b42..
SHA256:	2d564ae361eb49..
Tags:	exe NanoCore RAT

Most interesting Screenshot:



Detection

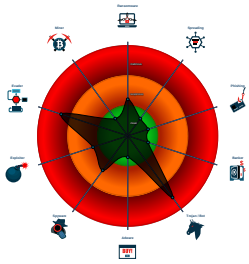


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Icon mismatch, binary includes an ic…
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Sigma detected: NanoCore
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- Allocates memory in foreign process…
- Binary contains a suspicious time st…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Initial sample is a PE file and has a…

Classification



Startup

- **System is w10x64**
- order-181289654312464648.exe (PID: 5964 cmdline: 'C:\Users\user\Desktop\order-181289654312464648.exe' MD5: 28DA42C2CD57E51CB8EA7DF263802924)
  - fdcgjhjyuyihdastagghejh.exe (PID: 6692 cmdline: 'C:\Users\user\AppData\Roaming\fdcgjhjyuyihdastagghejh.exe' MD5: 28DA42C2CD57E51CB8EA7DF263802924)
    - AddInProcess32.exe (PID: 4316 cmdline: C:\Users\user\AppData\Local\Temp\AddInProcess32.exe MD5: F2A47587431C466535F3C3D3427724BE)
    - fdexedxfuuyytwq.exe (PID: 5168 cmdline: 'C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
      - fdexedxfuuyytwq.exe (PID: 5188 cmdline: 'C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
    - fdexedxfuuyytwq.exe (PID: 5688 cmdline: 'C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
      - fdexedxfuuyytwq.exe (PID: 3564 cmdline: 'C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
    - fdexedxfuuyytwq.exe (PID: 1048 cmdline: 'C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
      - fdexedxfuuyytwq.exe (PID: 5044 cmdline: 'C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
    - fdexedxfuuyytwq.exe (PID: 6328 cmdline: 'C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
      - fdexedxfuuyytwq.exe (PID: 6816 cmdline: 'C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
    - fdexedxfuuyytwq.exe (PID: 6880 cmdline: 'C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
      - fdexedxfuuyytwq.exe (PID: 6708 cmdline: 'C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
    - fdexedxfuuyytwq.exe (PID: 6800 cmdline: 'C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
      - fdexedxfuuyytwq.exe (PID: 5504 cmdline: 'C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
    - fdexedxfuuyytwq.exe (PID: 6124 cmdline: 'C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
      - fdexedxfuuyytwq.exe (PID: 6892 cmdline: 'C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
    - fdexedxfuuyytwq.exe (PID: 2792 cmdline: 'C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
      - fdexedxfuuyytwq.exe (PID: 6936 cmdline: 'C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
    - fdexedxfuuyytwq.exe (PID: 7120 cmdline: 'C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
- **cleanup**

Malware Configuration

Threatname: NanoCore


```
{
  "C2: ": [
    "185.157.162.81"
  ],
  "Version: ": "NanoCore Client, Version=1.2.2.0"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000F.00000002.624408872.0000000005C0 0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
0000000F.00000002.624408872.0000000005C0 0000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost
0000000F.00000002.624408872.0000000005C0 0000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000000F.00000002.624910732.0000000006BD 0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x8ba5:$x1: NanoCore.ClientPluginHost • 0x8bd2:$x2: IClientNetworkHost
0000000F.00000002.624910732.0000000006BD 0000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x8ba5:$x2: NanoCore.ClientPluginHost • 0x9b74:$s2: FileCommand • 0xe576:$s4: PipeCreated • 0x8bbf:$s5: IClientLoggingHost
Click to see the 66 entries				

Unpacked PEs

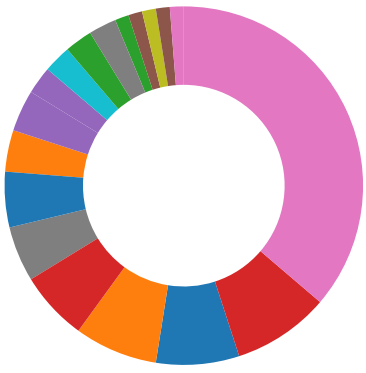
Source	Rule	Description	Author	Strings
15.2.AddInProcess32.exe.6bc0000.8.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x2dbb:$x1: NanoCore.ClientPluginHost • 0x2de5:$x2: IClientNetworkHost
15.2.AddInProcess32.exe.6bc0000.8.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x2dbb:$x2: NanoCore.ClientPluginHost • 0x4c6b:$s4: PipeCreated
15.2.AddInProcess32.exe.6ca0000.18.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1d3db:$x1: NanoCore.ClientPluginHost • 0x1d3f5:$x2: IClientNetworkHost
15.2.AddInProcess32.exe.6ca0000.18.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x1d3db:$x2: NanoCore.ClientPluginHost • 0x20718:$s4: PipeCreated • 0x1d3c8:$s5: IClientLoggingHost
15.2.AddInProcess32.exe.6c60000.15.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x39eb:$x1: NanoCore.ClientPluginHost • 0x3a24:$x2: IClientNetworkHost
Click to see the 51 entries				

Sigma Overview

System Summary:

Sigma detected: NanoCore

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- 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
- Lowering of HIPS / PFW / Operating System Security Settings
- 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
- Yara detected Nanocore RAT
- Machine Learning detection for dropped file
- Machine Learning detection for sample

Networking:

- C2 URLs / IPs found in malware configuration

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 potential unpacker
- Binary contains a suspicious time stamp

Hooking and other Techniques for Hiding and Protection:

- Icon mismatch, binary includes an icon from a different legit application in order to fool users
- Hides that the sample has been downloaded from the Internet (zone.identifier)

HIPS / PFW / Operating System Protection Evasion:

- Allocates memory in foreign processes
- Injects a PE file into a foreign processes
- Writes to foreign memory regions

Stealing of Sensitive Information:

- Yara detected Nanocore RAT

Remote Access Functionality:

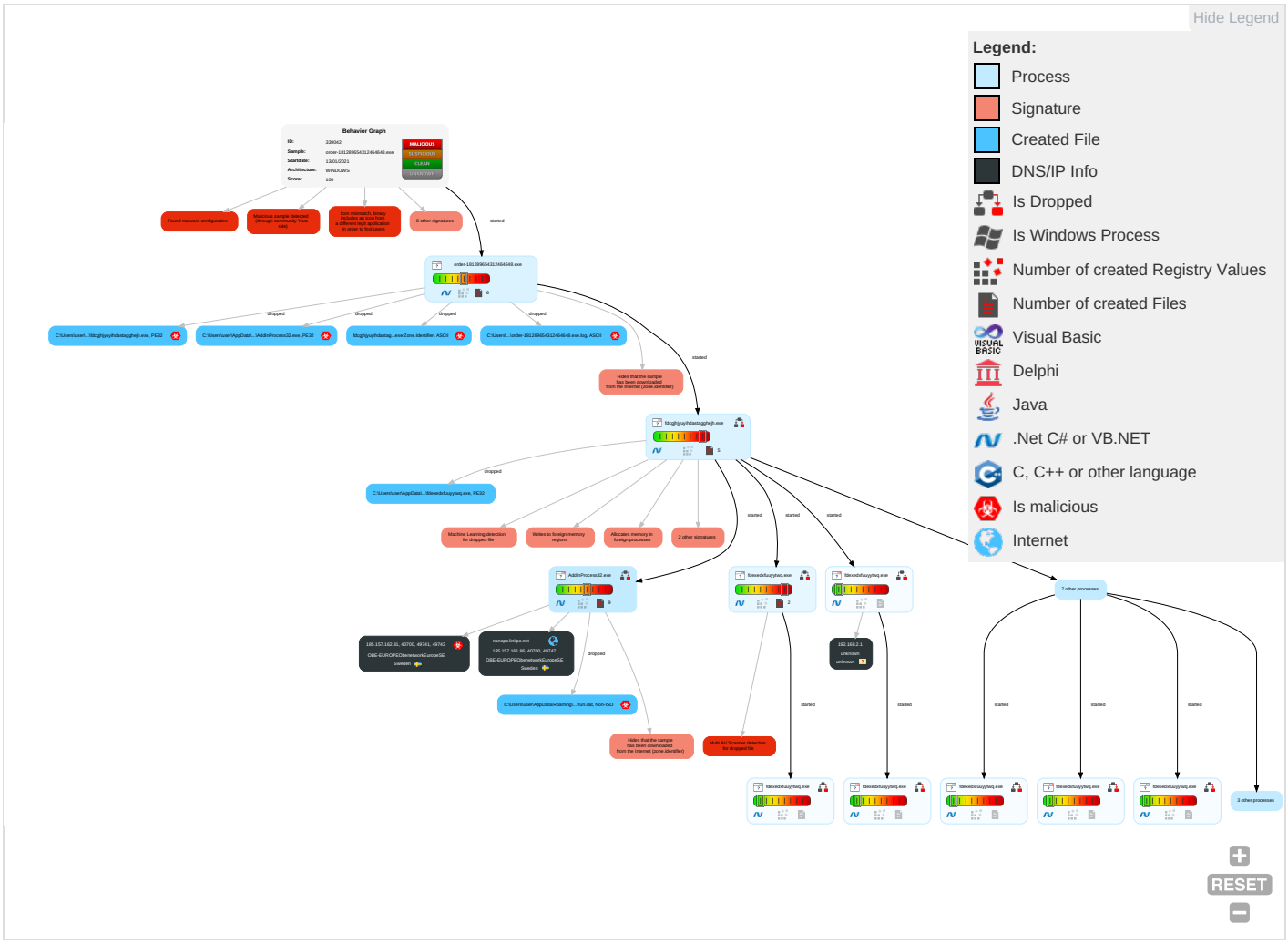
- Detected Nanocore Rat
- Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	C ar

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	C a
Valid Accounts 1	Windows Management Instrumentation 1	Startup Items 1	Startup Items 1	Disable or Modify Tools 1	Input Capture 2 1	System Time Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	E C
Default Accounts	Scheduled Task/Job	Valid Accounts 1	Valid Accounts 1	Deobfuscate/Decode Files or Information 1	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Input Capture 2 1	Exfiltration Over Bluetooth	N P
Domain Accounts	At (Linux)	Registry Run Keys / Startup Folder 2	Access Token Manipulation 1	Obfuscated Files or Information 2	Security Account Manager	System Information Discovery 1 3	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	R S
Local Accounts	At (Windows)	Logon Script (Mac)	Process Injection 3 1 2	Software Packing 1 1	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	N A L P
Cloud Accounts	Cron	Network Logon Script	Registry Run Keys / Startup Folder 2	Timestomp 1	LSA Secrets	Security Software Discovery 1 2 1	SSH	Keylogging	Data Transfer Size Limits	A L P
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	M C
External Remote Services	Scheduled Task	Startup Items	Startup Items	Valid Accounts 1	DCSync	Process Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	C U
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Access Token Manipulation 1	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	A L
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Virtualization/Sandbox Evasion 3	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	W
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Process Injection 3 1 2	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	Fi P
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Hidden Files and Directories 1	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	M

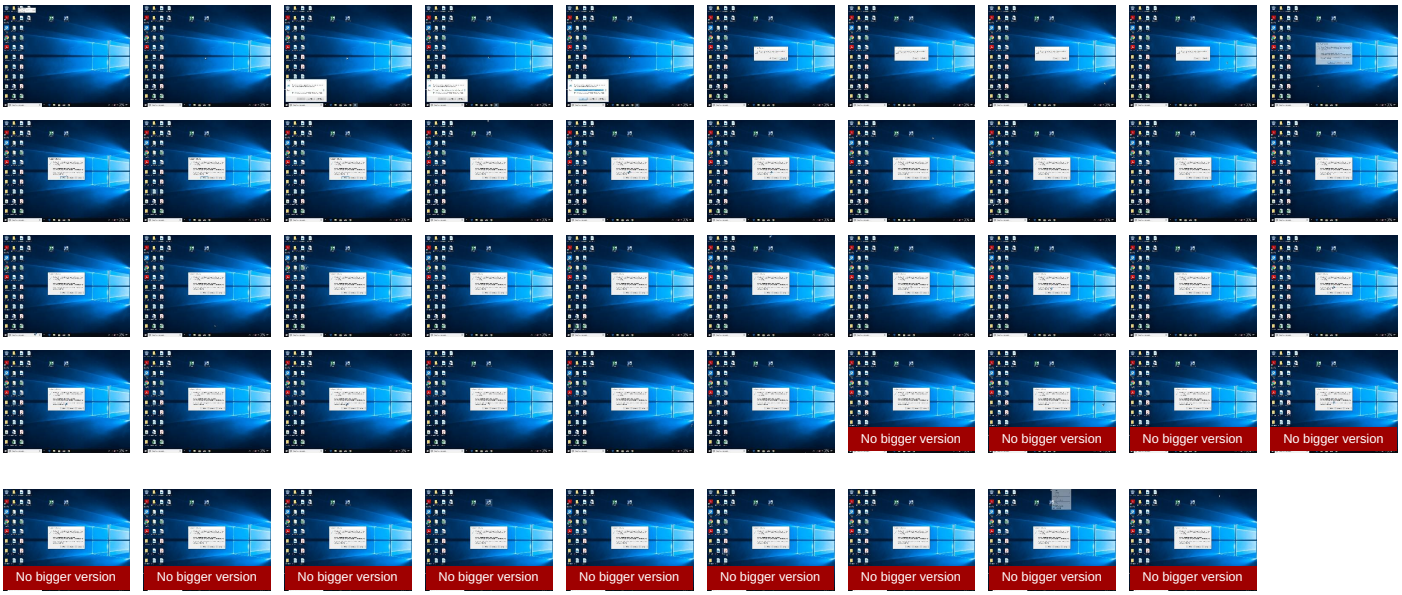
Behavior Graph



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
order-181289654312464648.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\fdcgjhjyuyihdastagghejh.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\AddInProcess32.exe	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\AddInProcess32.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\AddInProcess32.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.exe	7%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.exe	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.exe	7%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
15.2.AddInProcess32.exe.5c00000.6.unpack	100%	Avira	TR/NanoCore.fadte		Download File
15.2.AddInProcess32.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://iptc.tc4xmp3	0%	Avira URL Cloud	safe	
http://ns.ado/Ident	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
nanopc.linkpc.net	185.157.161.86	true	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://iptc.tc4xmp3	fdcgjhjyuyihdastagghejh.exe, 0000000D.00000002.616518111.0000000001789000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown
http://ns.ado/Ident	fdcgjhjyuyihdastagghejh.exe, 0000000D.00000002.616518111.0000000001789000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.157.162.81	unknown	Sweden		197595	OBE-EUROPEObenetworkEuropeSE	true
185.157.161.86	unknown	Sweden		197595	OBE-EUROPEObenetworkEuropeSE	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	339042
Start date:	13.01.2021
Start time:	10:15:43
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 33s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	order-181289654312464648.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:	40
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@41/29@1/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 2.2% (good quality ratio 1.8%) • Quality average: 67.9% • Quality standard deviation: 33%
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 • 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): MpCmdRun.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • Excluded IPs from analysis (whitelisted): 40.88.32.150, 52.255.188.83, 23.210.248.85, 51.104.139.180, 92.122.213.194, 92.122.213.247, 2.20.143.16, 2.20.142.210, 2.20.142.209, 51.103.5.159, 20.54.26.129, 51.11.168.160, 20.190.129.2, 40.126.1.128, 40.126.1.166, 20.190.129.133, 20.190.129.128, 40.126.1.145, 40.126.1.130, 20.190.129.160, 52.155.217.156 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, www.tm.lg.prod.aadmsa.akadns.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, wns.notify.windows.com.akadns.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, par02p.wns.notify.windows.com.akadns.net, emea1.notify.windows.com.akadns.net, login.live.com, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, www.tm.a.prd.aadg.akadns.net, login.msa.msidentity.com, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net • Report creation exceeded maximum time and may have missing disassembly code information. • Report size exceeded maximum capacity and may have missing behavior information. • 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. • Report size getting too big, too many NtReadVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
10:16:39	API Interceptor	180x Sleep call for process: order-181289654312464648.exe modified
10:16:43	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\fdcgjhjyuyihdastaggh ejh.lnk
10:17:29	API Interceptor	194x Sleep call for process: fdcgjhjyuyihdastagghejh.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.157.162.81	89GsVCJAXv.exe	Get hash	malicious	Browse	
	spetsifikatsiya.xls	Get hash	malicious	Browse	
	dpR3o92MH1.exe	Get hash	malicious	Browse	
	0qNSJXB8nG.exe	Get hash	malicious	Browse	
	7w7LwD8bqe.exe	Get hash	malicious	Browse	
	ZZB5zuv1X0.exe	Get hash	malicious	Browse	
	spetsifikatsiya.xls	Get hash	malicious	Browse	
	ptoovvKZ80.exe	Get hash	malicious	Browse	
	spetsifikatsiya.xls	Get hash	malicious	Browse	
	EnJsj6nuD4.exe	Get hash	malicious	Browse	
	zlkcd7HSQp.exe	Get hash	malicious	Browse	
	machine.xls	Get hash	malicious	Browse	
	qdnLoWn1E8.exe	Get hash	malicious	Browse	
	ogYg79jWpR.exe	Get hash	malicious	Browse	
	ORDER PMX-PT-2001 STOCK+NOVO.exe	Get hash	malicious	Browse	
	DHL_10177_R293_DOCUMENT.exe	Get hash	malicious	Browse	
	Order_List_PO# 081928.pdf.exe	Get hash	malicious	Browse	
	CF09550WJ901.pdf.exe	Get hash	malicious	Browse	
	Order List PO# 081927.pdf.exe	Get hash	malicious	Browse	
	Doc#66202009475352765301499.pdf.exe	Get hash	malicious	Browse	
185.157.161.86	Order_1101201918_AUTECH.exe	Get hash	malicious	Browse	
	50404868-c352-422f-a608-7fd64b335eec.exe	Get hash	malicious	Browse	
	74725794.pdf.exe	Get hash	malicious	Browse	
	Order_List_PO# 0819289.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
nanopc.linkpc.net	ORDER PMX-PT-2001 STOCK+NOVO.exe	Get hash	malicious	Browse	• 185.157.162.81
	DHL_10177_R293_DOCUMENT.exe	Get hash	malicious	Browse	• 105.112.101.201

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
OBE-EUROPEObenetworkEuropeSE	Doc#6620200947535257653.exe	Get hash	malicious	Browse	• 185.157.160.233
	Scan_order.exe	Get hash	malicious	Browse	• 185.157.161.61
	inrfzFzDHR.exe	Get hash	malicious	Browse	• 45.148.16.42
	SecuriteInfo.com.generic.ml.exe	Get hash	malicious	Browse	• 185.157.161.61
	New PO.doc	Get hash	malicious	Browse	• 185.157.161.61
	89GsVCJAXv.exe	Get hash	malicious	Browse	• 185.157.162.81
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 185.157.162.81
	DHL_file 187652345643476245.exe	Get hash	malicious	Browse	• 185.157.160.233
	dpR3o92MH1.exe	Get hash	malicious	Browse	• 185.157.162.81
	0qNSJXB8nG.exe	Get hash	malicious	Browse	• 185.157.162.81
	Order_1101201918_AUTECH.exe	Get hash	malicious	Browse	• 185.157.161.86
	7w7LwD8bqe.exe	Get hash	malicious	Browse	• 185.157.162.81
	ZZB5zuv1X0.exe	Get hash	malicious	Browse	• 185.157.162.81
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 185.157.162.81
	ptoovvKZ80.exe	Get hash	malicious	Browse	• 185.157.162.81
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 185.157.162.81
	EnJsj6nuD4.exe	Get hash	malicious	Browse	• 185.157.162.81
	AdviceSlip.xls	Get hash	malicious	Browse	• 217.64.149.169
	DHL_file 187652345643476245.exe	Get hash	malicious	Browse	• 185.157.160.233
	DHL_file 187652345643476245.exe	Get hash	malicious	Browse	• 185.157.160.233
OBE-EUROPEObenetworkEuropeSE	Doc#6620200947535257653.exe	Get hash	malicious	Browse	• 185.157.160.233
	Scan_order.exe	Get hash	malicious	Browse	• 185.157.161.61
	inrfzFzDHR.exe	Get hash	malicious	Browse	• 45.148.16.42

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.generic.ml.exe	Get hash	malicious	Browse	• 185.157.161.61
	New PO.doc	Get hash	malicious	Browse	• 185.157.161.61
	89GsVCJAXv.exe	Get hash	malicious	Browse	• 185.157.162.81
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 185.157.162.81
	DHL_file 187652345643476245.exe	Get hash	malicious	Browse	• 185.157.160.233
	dpR3o92MH1.exe	Get hash	malicious	Browse	• 185.157.162.81
	0qNSJXB8nG.exe	Get hash	malicious	Browse	• 185.157.162.81
	Order_1101201918_AUTECH.exe	Get hash	malicious	Browse	• 185.157.161.86
	7w7LwD8bqe.exe	Get hash	malicious	Browse	• 185.157.162.81
	ZZB5zuv1X0.exe	Get hash	malicious	Browse	• 185.157.162.81
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 185.157.162.81
	ptoovvKZ80.exe	Get hash	malicious	Browse	• 185.157.162.81
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 185.157.162.81
	EnJsj6nuD4.exe	Get hash	malicious	Browse	• 185.157.162.81
	AdviceSlip.xls	Get hash	malicious	Browse	• 217.64.149.169
	DHL_file 187652345643476245.exe	Get hash	malicious	Browse	• 185.157.160.233
	DHL_file 187652345643476245.exe	Get hash	malicious	Browse	• 185.157.160.233

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\AddInProcess32.exe	PO_60577.exe	Get hash	malicious	Browse	
	IMG_73344332#U00e2#U20ac#U00aegpj.exe	Get hash	malicious	Browse	
	Ziraat Bankasi Swift Mesaji.exe	Get hash	malicious	Browse	
	Doc#6620200947535257653.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Generic.mg.15368412abd71685.exe	Get hash	malicious	Browse	
	RT-05723.exe	Get hash	malicious	Browse	
	Dekont.pdf.exe	Get hash	malicious	Browse	
	cFAWQ1mv83.exe	Get hash	malicious	Browse	
	I7313Y5Rr2.exe	Get hash	malicious	Browse	
	SWIFT-COPY Payment advice3243343.exe	Get hash	malicious	Browse	
	bWVvaTptgL.exe	Get hash	malicious	Browse	
	umOXxQ9PFS.exe	Get hash	malicious	Browse	
	BL,IN&PL.exe	Get hash	malicious	Browse	
	ORDER #0554.exe	Get hash	malicious	Browse	
	Dekont.pdf.exe	Get hash	malicious	Browse	
	IMG_84755643#U00e2#U20ac#U00aegpj.exe	Get hash	malicious	Browse	
	8WLxD8uxRN.exe	Get hash	malicious	Browse	
	Quotation.exe	Get hash	malicious	Browse	
	e-dekont.html.exe	Get hash	malicious	Browse	
	Dekont.pdf.exe	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.exe	SecuriteInfo.com.Generic.mg.5a4b41327cabca49.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.FileRepMalware.exe	Get hash	malicious	Browse	
	TD-10057.exe	Get hash	malicious	Browse	
	FedExAWB 772584418730.doc	Get hash	malicious	Browse	
	Doc#6620200947535257653.exe	Get hash	malicious	Browse	
	TD-10057.doc	Get hash	malicious	Browse	
	ndSscoDob9.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Generic.mg.15368412abd71685.exe	Get hash	malicious	Browse	
	QL-0217.doc	Get hash	malicious	Browse	
	DXXJmIDl3C.exe	Get hash	malicious	Browse	
	0YdVJ6vqhO.exe	Get hash	malicious	Browse	
	RT-05723.exe	Get hash	malicious	Browse	
	RT-05723.doc	Get hash	malicious	Browse	
	DHL_file 187652345643476245.exe	Get hash	malicious	Browse	
	Order_1101201918_AUTECH.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\fdexedxfuuyytwq.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1362
Entropy (8bit):	5.343186145897752
Encrypted:	false
SSDEEP:	24:ML9E4Ks2eE4O1lEE4UVwPKDE4KhK3VZ9pKhuE4IWUAE4KI6no84j:MxHKXeHKlEHU0YHKhQnouHIW7HKjovj
MD5:	1249251E90A1C28AB8F7235F30056DEB
SHA1:	166BA6B64E9B0D9BA7B856334F7D7EC027030BA1
SHA-256:	B5D65BF3581136CD5368BC47FA3972E06F526EED407BC6571D11D9CD4B5C4D83
SHA-512:	FD880C5B12B22241F67139ABD09B99ACE7A4DD24635FC6B340A3E7C463E2AEF3FA68EF647352132934BC1F8CA134F46064049449ACB67954BEDDEA9AA967088
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..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..3,"PresentationCore, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll",0..3,"PresentationFramework, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll",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,"WindowsBase, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Wi

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\order-181289654312464648.exe.log	
Process:	C:\Users\user\Desktop\order-181289654312464648.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1451
Entropy (8bit):	5.345862727722058
Encrypted:	false
SSDEEP:	24:ML9E4Ks2eE4O1lEE4UVwPKDE4KhK3VZ9pKhuE4IWUAE4KI6no84G1qE4j:MxHKXeHKlEHU0YHKhQnouHIW7HKjovGm
MD5:	06F54CDBFEF62849AF5AE052722BD7B6
SHA1:	FB0250AAC2057D0B5BCE4CE130891E428F28DA05
SHA-256:	4C039B93A728B546F49C47ED8B448D40A3553CDAABB147067AEE3958133CB446
SHA-512:	34EF5F6D5EAB0E5B11AC81F0D72FC56304291EDEEF6D19DF7145FDECAB5D342767DBBC0B4384B8DECB5741E6B85A4B431DF14FBEB5DDF2DEE103064D2895EABB
Malicious:	**true**
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..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..3,"PresentationCore, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll",0..3,"PresentationFramework, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll",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,"WindowsBase, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Wi

C:\Users\user\AppData\Local\Temp\AddInProcess32.exe	
Process:	C:\Users\user\Desktop\order-181289654312464648.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	42080
Entropy (8bit):	6.2125074198825105
Encrypted:	false
SSDEEP:	384:gc3JOvwWj8Gpw0A67dOpRIMKJ9Yl6dnPU3SERztmbqCJstdMardz/JikPZ+QsPZw:g4JU8g17dl6Iq88MoBd7mFViqM5sL2
MD5:	F2A47587431C466535F3C3D3427724BE
SHA1:	90DF719241CE04828F0DD4D31D683F84790515FF
SHA-256:	23F4A2CCDCE499C524CF43793FDA8E773D809514B5471C02FA5E68F0CDA7A10B
SHA-512:	E9D0819478DDDA47763C7F5F617CD258D0FACBBBFFE0C7A965EDE9D0D884A6D7BB445820A3FD498B243BBD8BECBA146687B61421745E32B86272232C6F9E90D8
Malicious:	**true**
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%

C:\Users\user\AppData\Local\Temp\AddInProcess32.exe	
Joe Sandbox View:	• Filename: PO_60577.exe, Detection: malicious, Browse • Filename: IMG_73344332#U00e2#U20ac#U00aegpj.exe, Detection: malicious, Browse • Filename: Ziraat Bankasi Swift Mesaji.exe, Detection: malicious, Browse • Filename: Doc#6620200947535257653.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Generic.mg.15368412abd71685.exe, Detection: malicious, Browse • Filename: RT-05723.exe, Detection: malicious, Browse • Filename: Dekont.pdf.exe, Detection: malicious, Browse • Filename: cFAWQ1mv83.exe, Detection: malicious, Browse • Filename: I7313Y5Rr2.exe, Detection: malicious, Browse • Filename: SWIFT-COPY Payment advice3243343.exe, Detection: malicious, Browse • Filename: bWVvaTptgL.exe, Detection: malicious, Browse • Filename: umOXxQ9PFS.exe, Detection: malicious, Browse • Filename: BL,IN&PL.exe, Detection: malicious, Browse • Filename: ORDER #0554.exe, Detection: malicious, Browse • Filename: Dekont.pdf.exe, Detection: malicious, Browse • Filename: IMG_84755643#U00e2#U20ac#U00aegpj.exe, Detection: malicious, Browse • Filename: 8WLxD8uxRN.exe, Detection: malicious, Browse • Filename: Quotation.exe, Detection: malicious, Browse • Filename: e-dekont.html.exe, Detection: malicious, Browse • Filename: Dekont.pdf.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Z.Z.....0..X.....w... .....@.. ..... .`.....Hw..O..... .....f..`>.....v..... ....H.....text....W... ...X..... ..`.rsrc... .....Z.....@..@.relo c.....d.....@..B.....\|w.....H.....#...Q.....u.....0..K.....-..*..i....*...r...p.o....,...r...p.o....-..*....o.....o.....$...*.....o....(....(.....:...(....o.....r...p.o.....4.....o..... .....o.....s .....o!...s".....s#.....r]..prg..po$.....r...p.o$.....r...pr...po$.....s.....(%.....tB...r...p(&...&..r...p.('...s(.....o)...&..o*....(+...o,.....&...(- ....*.....3..@.....R...s.....s....(....*:.(/.....}P...*J.{P....o0..

C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.exe	
Process:	C:\Users\user\AppData\Roaming\fdcgjhjyuyihdastagghejh.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	78336
Entropy (8bit):	4.369296705546591
Encrypted:	false
SSDEEP:	768:jlU4+MS3Fu0thSOV4GM0SuHk9Oh/1TRIWUk7NlfaNV9KQLxXXSv:l6o03IGMLuHk+Ck5lfaNP7xSv
MD5:	0E362E7005823D0BEC3719B902ED6D62
SHA1:	590D860B909804349E0CDC2F1662B37BD62F7463
SHA-256:	2D0DC6216F613AC7551A7E70A798C22AEE8EB9819428B1357E2B8C73BEF905AD
SHA-512:	518991B68496B3F8545E418CF9B345E0791E09CC20D177B8AA47E0ABA447AA55383C64F5BDACA39F2B061A5D08C16F2AD484AF8A9F238CA23AB081618FBA3AD3
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 7%, Browse • Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 7%
Joe Sandbox View:	• Filename: SecuriteInfo.com.Generic.mg.5a4b41327cabca49.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.FileRepMalware.exe, Detection: malicious, Browse • Filename: TD-10057.exe, Detection: malicious, Browse • Filename: FedExAWB 772584418730.doc, Detection: malicious, Browse • Filename: Doc#6620200947535257653.exe, Detection: malicious, Browse • Filename: TD-10057.doc, Detection: malicious, Browse • Filename: ndSscoDob9.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Generic.mg.15368412abd71685.exe, Detection: malicious, Browse • Filename: QL-0217.doc, Detection: malicious, Browse • Filename: DXXJmIDl3C.exe, Detection: malicious, Browse • Filename: 0YdVJ6vqhO.exe, Detection: malicious, Browse • Filename: RT-05723.exe, Detection: malicious, Browse • Filename: RT-05723.doc, Detection: malicious, Browse • Filename: DHL_file 187652345643476245.exe, Detection: malicious, Browse • Filename: Order_1101201918_AUTECH.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...Y .....P..&.....D.. .....@.. ....`.....D..W....`.....hD..... ....H.....text....$... ...&..... ..`.rsrc.....`.....(.....@..@.rel oc.....0.....@..B.....D.....H.....l....%.....).....0..6.....(8...t....&.(8...t...&.....(8...t.....8;....8%.....(8...t....&.(8...t..... .:.....(8...t....:.....(8...t....:....(8...t.....\:@....(8...t....&.)...&8.....(8...t....&(8...t....&.....:.....8x.....:L...88....(8...t....&(8...t....&(8...t....&(8...t.....:....8!.... (8...t....&.....(8...t....&.....(8...t....:8.....(8...t....&.

C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.txt	
Process:	C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	72
Entropy (8bit):	4.885154258886507
Encrypted:	false
SSDEEP:	3:uVNWXp5cViEaKC5dVPF9OA1YnXVy:uVNWXp+NaZ5rPF9O2Ync
MD5:	EACC6D9F7D6EFE25CB48137E7064F313
SHA1:	1E767634BE3B749B6549F3101A09E2715859558B
SHA-256:	DBDFB40802DF3D9FA9923C7186586AEAB2985126EFB203E78A7CE2B53546F6D8

C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.txt	
SHA-512:	0C3187B94CEFAAFD731D504E17D602D14A2819A68B239444BDA6135476F7EDCEC6B0A017E2762C59ADDAFDC405B884373A608CE3A9A9DB8087C62B6F330159B
Malicious:	false
Preview:	6692..C:\Users\user\AppData\Roaming\fdcgjhjyuyihdastagghejh.exe..7120..

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Users\user\AppData\Local\Temp\AddInProcess32.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	6:X4LDAnybgCFcpJSQwP4d7ZrqJgTFwoaw+9XU4:X4LEnybgCFCtvd7ZrCgpwoaw+Z9
MD5:	32D0AAE13696FF7F8AF33B2D22451028
SHA1:	EF80C4E0DB2AE8EF288027C9D3518E6950B583A4
SHA-256:	5347661365E7AD2C1ACC27AB0D150FFA097D9246BB3626FCA06989E976E8DD29
SHA-512:	1D77FC13512C0DBC4EFD7A66ACB502481E4EFA0FB73D0C7D0942448A72B9B05BA1EA78DDF0BE966363C2E3122E0B631DB7630D044D08C1E1D32B9FB025C356A5
Malicious:	false
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0. :e[7w{1.!.4.....&.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\AppData\Local\Temp\AddInProcess32.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:TOt:TOt
MD5:	9DCCFC1428F275A4E2429AFEA104655B
SHA1:	4C4AAC284536CFB553FEBE32DF9D4C8DAEB47741
SHA-256:	F8026D5E1B4CA4035C68C75F13026580B0A5B39CC6663D238FC92FD2D139D359
SHA-512:	E320E38E187436748EE236F6F11EEAF7C61DC9C14A96A271E97A3EF8B6F22DD9C79F783FF5F48CBBF5FE7A64E15F38B52AC817C088FABCE9FE4757236C78D887
Malicious:	**true**
Preview:	J=...H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Users\user\AppData\Local\Temp\AddInProcess32.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	5.153055907333276
Encrypted:	false
SSDEEP:	3:9bzY6oRDT6P2bfVn1:RzWDT621
MD5:	4E5E92E2369688041CC82EF9650EDED2
SHA1:	15E44F2F3194EE232B44E9684163B6F66472C862
SHA-256:	F8098A6290118F2944B9E7C842BD014377D45844379F863B00D54515A8A64B48
SHA-512:	1B368018907A3BC30421FDA2C935B39DC9073B9B1248881E70AD48EDB6CAA256070C1A90B97B0F64BBE61E316DBB8D5B2EC8DBABCD0B0B2999AB50B933671BCB
Malicious:	false
Preview:	9iH...}Z.4..f.~a.....~.~.....3.U.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Process:	C:\Users\user\AppData\Local\Temp\AddInProcess32.exe
File Type:	data
Category:	dropped
Size (bytes):	327432
Entropy (8bit):	**7.99938831605763**
Encrypted:	**true**
SSDEEP:	6144:oX44S90aTiB66x3Pl6nGV4bfD6wXPIZ9iBj0UeprGm2d7Tm:LkjYGsfGUc9iB4UeprKdnm
MD5:	7E8F4A764B981D5B82D1CC49D341E9C6

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
SHA1:	D9F0685A028FB219E1A6286AEFB7D6FCFC778B85
SHA-256:	0BD3AAC12623520C4E2031C8B96B4A154702F36F97F643158E91E987D317B480
SHA-512:	880E46504FCFB4B15B86B9D8087BA88E6C4950E433616EBB637799F42B081ABF6F07508943ECB1F786B2A89E751F5AE62D750BDCFFDDF535D600CF66EC44E92
Malicious:	false
Preview:	pT..!..W..G.J..a.).@.i..wpK.so@...5.=.^..Q.oy.=e@9.B...F..09u"3.. 0t..RDn_4d.....E...i.....~...|..fX_...Xf.p^.....>a..$...e.6:7d.(a.A...=.)*.....{B.[...y%.*..i.Q.<..xt.X..H.. ..H F7g...I.*3.{.n....L.y;i..s-....(5i..........J.5b7}..fK..HV.,...0.... ....n.w6PMl.....v.'".v.....#..X.a...../...cC...i..l{>5n.._+.e.d'...}...[..../...D.t..GVp.zz.....(...o.....b...+`J.{....hS1G.^*I..v&. jm.#u..1..Mg!.E..U.T.....6.2>...6.l.K.w"o..E..."K%{....z.7....<...,...]t.:.....[.Z.u...3X8.QI..j_.&..N..q.e.2...6.R.~..9.Bq..A.v.6.G..#y.....O....Z)G...w..E..k(....+..O.....Vg.2xC..... .O...jc.....z..~.P...q../.-.'.h._.cj.=..B.x.Q9.pu.\|i4...i...;O...n.?.,. ....v?.5}.OY@.dG\|<.._[.69@.2..m..I..oP=...xrK.?.....b..5....i&...l.c\b}..Q..O+.V.mJ.....pz....>F.....H...6$. ..d...|m...N..1.R..B.i.....$....$.....CY}..$....r.....H...8...li.....7 P.....?h....R.iF..6...q(.@LI.s..+K.....?m..H....*. l..&<}....`|.B....3.....I..o...u1..8i=.z.W..7

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\fdcgjhjyuyihdastagghejh.lnk	
Process:	C:\Users\user\Desktop\order-181289654312464648.exe
File Type:	MS Windows shortcut, Item id list present, Has Relative path, Has Working directory, ctime=Sun Dec 31 23:06:32 1600, mtime=Sun Dec 31 23:06:32 1600, atime=Sun Dec 31 23:06:32 1600, length=0, window=hide
Category:	dropped
Size (bytes):	1008
Entropy (8bit):	3.2517421808078684
Encrypted:	false
SSDEEP:	12:8wl06sXou41w/tz0/CSLMeI2DsAMPHAMYmO3qMJCHAM2gTCNfBT/v4t2Y+xIBjK:8Rf4eWLZ//7DPthJVpd7aB
MD5:	FB516F578D9499D6DB698AE541F8FCCB
SHA1:	E26C9B2F619BCD1216E1C17689392BAF50E202C9
SHA-256:	7EA8400005E701A3C980DE2BAB4EE042A927863E50689A81F79BAEE90CCF72EA
SHA-512:	EC1BF91EC5559196056757324l7D32E94B9C53AA063A6823042DD59010317C15EE0599C2BD3E5E4CC622226625E29E29B69E56C2BD7588124A0081D446B3761B
Malicious:	false
Preview:	L.....F.....P.O. .:i....+00.../C:\.....P.1.....Users.<.....U.s.e.r.s.....P.1.....user.<..... .....h.a.r.d.z.....V.1.....AppData.@.....A.p.p.D.a.t.a.....V.1.....Roaming.@.....R.o.a.m.i.n.g.....2..... ....fdcgjhjyuyihdastagghejh.exe.h.....f.d.c.g.j.h.j.y.u.y.i.h.d.a.s.t.a.g.g.h.e.j.h...e.x.e...*...*.....\.....\.....\.....\.....\.f.d.c.g.j.h.j.y.u.y.i.h.d.a.s.t.a.g.g.h.e .j.h...e.x.e.:.C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.R.o.a.m.i.n.g.\.f.d.c.g.j.h.j.y.u.y.i.h.d.a.s.t.a.g.g.h.e.j.h...e.x.e.....y.....>.e.L.:..er.=y.....1SPS.XF.L8C... .&.m.q.....\...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2.....

C:\Users\user\AppData\Roaming\fdcgjhjyuyihdastagghejh.exe	
Process:	C:\Users\user\Desktop\order-181289654312464648.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	5815808
Entropy (8bit):	7.8329710414512155
Encrypted:	false
SSDEEP:	98304:3QRUDjYYo/PJhTLqj7tLS+5xZEU2ytc40Gk15GhYwfxK+gEwj7u/B:3QRUIzTLq75x+U/tc9GrhPAFOJ
MD5:	28DA42C2CD57E51CB8EA7DF263802924
SHA1:	81C980F2CDA9B42B0B8BF50C7128CC88AFD942FD
SHA-256:	2D564AE361EB499CA493273E9FCFB88546105C88293C7633A7E1580A435CEE9F
SHA-512:	594EF84101106F21760953B8DD2660CAA21FC6F08790B588875781B1233586A000CFAE1D3A3001A1221762A08F18705E401C5AF60F25D7E37032335346D9F828
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...c..9.....U.....V.. .....@.. .....Y..... ..`.....T.V.W.... V.J.....X..... ..... ..H.....text....U.. ....U..... ..`.rsrc...J.... V.....V.....@..@.rel oc.....X.....X.....@..B.....V.....H.....\.U..&.....P....B...R..... ....%.....(..... ".....%.....(.....*...0.....(....t.... ...H (:...t....&.N&..... .j.(:...t.....-.+..(....t....&.....-.....+J.....-:.....(....t..... .....(:...t.....(:...t...&.....-.....(....t.... |-.....(:...t....(....t.....(:...t....:p....(....t..... ..\:....+w.....(....t....(....t..... ..c(:

C:\Users\user\AppData\Roaming\fdcgjhjyuyihdastagghejh.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\order-181289654312464648.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.8329710414512155
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	order-181289654312464648.exe
File size:	5815808
MD5:	28da42c2cd57e51cb8ea7df263802924
SHA1:	81c980f2cda9b42b0b8bf50c7128cc88afd942fd
SHA256:	2d564ae361eb499ca493273e9fcfb88546105c88293c7633a7e1580a435cee9f
SHA512:	594ef84101106f21760953b8dd2660caa21fc6f08790b588875781b1233586a000cfae1d3a3001a1221762a08f1875e401c5af60f25d7e37032335346d9f828
SSDEEP:	98304:3QRUDjYYo/PJhTLqj7tLS+5xZEU2ytc40Gk15GhYwfxK+gEwj7u/B:3QRUIzTLq75x+U/tc9GrhPAFOJ
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...c..9.....U.....V.. .....@.. .....Y.....`.....

File Icon

Icon Hash:	c6a9989ae8ccb6cc

Static PE Info

General

Entrypoint:	0x961cae
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, HIGH_ENTROPY_VA
Time Stamp:	0x39BE9B63 [Tue Sep 12 21:08:51 2000 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

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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x561c54	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x562000	0x2ba4a	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x58e000	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	0x55fcb4	0x55fe00	unknown	unknown	unknown	unknown	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x562000	0x2ba4a	0x2bc00	False	0.236199776786	data	5.5567301511	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x58e000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x5622b0	0x39bc	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		

Name	RVA	Size	Type	Language	Country
RT_ICON	0x565c6c	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x576494	0x94a8	data		
RT_ICON	0x57f93c	0x5488	data		
RT_ICON	0x584dc4	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 254, next used block 520093696		
RT_ICON	0x588fec	0x25a8	data		
RT_ICON	0x58b594	0x10a8	data		
RT_ICON	0x58c63c	0x988	data		
RT_ICON	0x58cfc4	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x58d42c	0x84	data		
RT_VERSION	0x58d4b0	0x3b0	data		
RT_MANIFEST	0x58d860	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

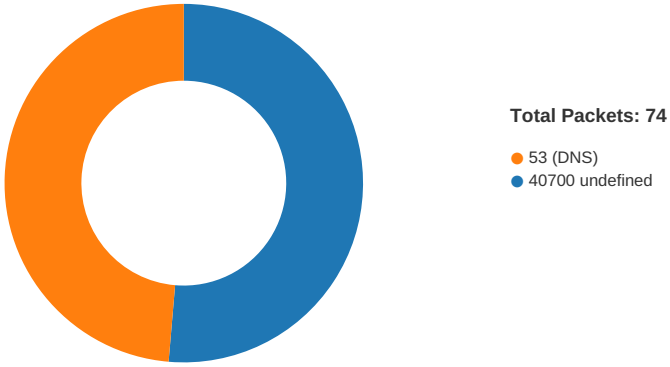
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2010 ?;BH8HG?:@DJDEDB753GC
Assembly Version	1.0.0.0
InternalName	hugefrssaw.exe
FileVersion	7.10.13.17
CompanyName	?;BH8HG?:@DJDEDB753GC
Comments	3:7=7B8D46?BJC<65<C>8?
ProductName	GJJ=2H538>53D9C4CD
ProductVersion	7.10.13.17
FileDescription	GJJ=2H538>53D9C4CD
OriginalFilename	hugefrssaw.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 10:18:05.183847904 CET	49741	40700	192.168.2.3	185.157.162.81
Jan 13, 2021 10:18:05.265274048 CET	40700	49741	185.157.162.81	192.168.2.3
Jan 13, 2021 10:18:05.772847891 CET	49741	40700	192.168.2.3	185.157.162.81

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 10:18:05.858684063 CET	40700	49741	185.157.162.81	192.168.2.3
Jan 13, 2021 10:18:06.366697073 CET	49741	40700	192.168.2.3	185.157.162.81
Jan 13, 2021 10:18:06.448652029 CET	40700	49741	185.157.162.81	192.168.2.3
Jan 13, 2021 10:18:10.541047096 CET	49743	40700	192.168.2.3	185.157.162.81
Jan 13, 2021 10:18:10.624140024 CET	40700	49743	185.157.162.81	192.168.2.3
Jan 13, 2021 10:18:11.132726908 CET	49743	40700	192.168.2.3	185.157.162.81
Jan 13, 2021 10:18:11.221738100 CET	40700	49743	185.157.162.81	192.168.2.3
Jan 13, 2021 10:18:11.726533890 CET	49743	40700	192.168.2.3	185.157.162.81
Jan 13, 2021 10:18:11.816729069 CET	40700	49743	185.157.162.81	192.168.2.3
Jan 13, 2021 10:18:16.591576099 CET	49744	40700	192.168.2.3	185.157.162.81
Jan 13, 2021 10:18:16.685046911 CET	40700	49744	185.157.162.81	192.168.2.3
Jan 13, 2021 10:18:17.195848942 CET	49744	40700	192.168.2.3	185.157.162.81
Jan 13, 2021 10:18:17.294382095 CET	40700	49744	185.157.162.81	192.168.2.3
Jan 13, 2021 10:18:17.805157900 CET	49744	40700	192.168.2.3	185.157.162.81
Jan 13, 2021 10:18:17.886883020 CET	40700	49744	185.157.162.81	192.168.2.3
Jan 13, 2021 10:18:22.147533894 CET	49747	40700	192.168.2.3	185.157.161.86
Jan 13, 2021 10:18:22.430186033 CET	40700	49747	185.157.161.86	192.168.2.3
Jan 13, 2021 10:18:22.430293083 CET	49747	40700	192.168.2.3	185.157.161.86
Jan 13, 2021 10:18:22.464010000 CET	49747	40700	192.168.2.3	185.157.161.86
Jan 13, 2021 10:18:22.758575916 CET	40700	49747	185.157.161.86	192.168.2.3
Jan 13, 2021 10:18:22.758668900 CET	49747	40700	192.168.2.3	185.157.161.86
Jan 13, 2021 10:18:23.191312075 CET	40700	49747	185.157.161.86	192.168.2.3
Jan 13, 2021 10:18:23.191379070 CET	49747	40700	192.168.2.3	185.157.161.86
Jan 13, 2021 10:18:23.605516911 CET	40700	49747	185.157.161.86	192.168.2.3
Jan 13, 2021 10:18:23.633533955 CET	49747	40700	192.168.2.3	185.157.161.86
Jan 13, 2021 10:18:23.958090067 CET	40700	49747	185.157.161.86	192.168.2.3
Jan 13, 2021 10:18:24.070549965 CET	40700	49747	185.157.161.86	192.168.2.3
Jan 13, 2021 10:18:24.083247900 CET	40700	49747	185.157.161.86	192.168.2.3
Jan 13, 2021 10:18:24.083295107 CET	40700	49747	185.157.161.86	192.168.2.3
Jan 13, 2021 10:18:24.083316088 CET	40700	49747	185.157.161.86	192.168.2.3
Jan 13, 2021 10:18:24.083338976 CET	40700	49747	185.157.161.86	192.168.2.3
Jan 13, 2021 10:18:24.083389044 CET	49747	40700	192.168.2.3	185.157.161.86
Jan 13, 2021 10:18:24.083417892 CET	49747	40700	192.168.2.3	185.157.161.86
Jan 13, 2021 10:18:24.083436966 CET	40700	49747	185.157.161.86	192.168.2.3
Jan 13, 2021 10:18:24.083726883 CET	49747	40700	192.168.2.3	185.157.161.86
Jan 13, 2021 10:18:24.085408926 CET	40700	49747	185.157.161.86	192.168.2.3
Jan 13, 2021 10:18:24.087407112 CET	40700	49747	185.157.161.86	192.168.2.3
Jan 13, 2021 10:18:24.087611914 CET	49747	40700	192.168.2.3	185.157.161.86
Jan 13, 2021 10:18:24.089659929 CET	40700	49747	185.157.161.86	192.168.2.3
Jan 13, 2021 10:18:24.090418100 CET	40700	49747	185.157.161.86	192.168.2.3
Jan 13, 2021 10:18:24.090538025 CET	49747	40700	192.168.2.3	185.157.161.86
Jan 13, 2021 10:18:24.357623100 CET	40700	49747	185.157.161.86	192.168.2.3
Jan 13, 2021 10:18:24.357680082 CET	40700	49747	185.157.161.86	192.168.2.3
Jan 13, 2021 10:18:24.357753992 CET	49747	40700	192.168.2.3	185.157.161.86
Jan 13, 2021 10:18:24.359256983 CET	40700	49747	185.157.161.86	192.168.2.3
Jan 13, 2021 10:18:24.361134052 CET	40700	49747	185.157.161.86	192.168.2.3
Jan 13, 2021 10:18:24.361207962 CET	49747	40700	192.168.2.3	185.157.161.86
Jan 13, 2021 10:18:24.362083912 CET	40700	49747	185.157.161.86	192.168.2.3
Jan 13, 2021 10:18:24.362200022 CET	40700	49747	185.157.161.86	192.168.2.3
Jan 13, 2021 10:18:24.362242937 CET	40700	49747	185.157.161.86	192.168.2.3
Jan 13, 2021 10:18:24.362272978 CET	49747	40700	192.168.2.3	185.157.161.86
Jan 13, 2021 10:18:24.363096952 CET	40700	49747	185.157.161.86	192.168.2.3
Jan 13, 2021 10:18:24.363154888 CET	49747	40700	192.168.2.3	185.157.161.86
Jan 13, 2021 10:18:24.365103960 CET	40700	49747	185.157.161.86	192.168.2.3
Jan 13, 2021 10:18:24.366099119 CET	40700	49747	185.157.161.86	192.168.2.3
Jan 13, 2021 10:18:24.366158009 CET	49747	40700	192.168.2.3	185.157.161.86
Jan 13, 2021 10:18:24.368100882 CET	40700	49747	185.157.161.86	192.168.2.3
Jan 13, 2021 10:18:24.369003057 CET	40700	49747	185.157.161.86	192.168.2.3
Jan 13, 2021 10:18:24.369066000 CET	49747	40700	192.168.2.3	185.157.161.86
Jan 13, 2021 10:18:24.390433073 CET	40700	49747	185.157.161.86	192.168.2.3
Jan 13, 2021 10:18:24.391096115 CET	40700	49747	185.157.161.86	192.168.2.3
Jan 13, 2021 10:18:24.391381979 CET	49747	40700	192.168.2.3	185.157.161.86
Jan 13, 2021 10:18:24.392076969 CET	40700	49747	185.157.161.86	192.168.2.3
Jan 13, 2021 10:18:24.395148993 CET	40700	49747	185.157.161.86	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 10:18:24.395257950 CET	49747	40700	192.168.2.3	185.157.161.86
Jan 13, 2021 10:18:24.396030903 CET	40700	49747	185.157.161.86	192.168.2.3
Jan 13, 2021 10:18:24.398098946 CET	40700	49747	185.157.161.86	192.168.2.3
Jan 13, 2021 10:18:24.398341894 CET	49747	40700	192.168.2.3	185.157.161.86
Jan 13, 2021 10:18:24.399117947 CET	40700	49747	185.157.161.86	192.168.2.3
Jan 13, 2021 10:18:24.400033951 CET	40700	49747	185.157.161.86	192.168.2.3
Jan 13, 2021 10:18:24.400301933 CET	49747	40700	192.168.2.3	185.157.161.86
Jan 13, 2021 10:18:24.629337072 CET	40700	49747	185.157.161.86	192.168.2.3
Jan 13, 2021 10:18:24.630142927 CET	40700	49747	185.157.161.86	192.168.2.3
Jan 13, 2021 10:18:24.630208969 CET	49747	40700	192.168.2.3	185.157.161.86
Jan 13, 2021 10:18:24.631036997 CET	40700	49747	185.157.161.86	192.168.2.3
Jan 13, 2021 10:18:24.633137941 CET	40700	49747	185.157.161.86	192.168.2.3
Jan 13, 2021 10:18:24.633208990 CET	49747	40700	192.168.2.3	185.157.161.86
Jan 13, 2021 10:18:24.634157896 CET	40700	49747	185.157.161.86	192.168.2.3
Jan 13, 2021 10:18:24.636156082 CET	40700	49747	185.157.161.86	192.168.2.3
Jan 13, 2021 10:18:24.636291027 CET	49747	40700	192.168.2.3	185.157.161.86
Jan 13, 2021 10:18:24.637115002 CET	40700	49747	185.157.161.86	192.168.2.3
Jan 13, 2021 10:18:24.646197081 CET	40700	49747	185.157.161.86	192.168.2.3
Jan 13, 2021 10:18:24.646245956 CET	40700	49747	185.157.161.86	192.168.2.3
Jan 13, 2021 10:18:24.646256924 CET	49747	40700	192.168.2.3	185.157.161.86
Jan 13, 2021 10:18:24.646291018 CET	40700	49747	185.157.161.86	192.168.2.3
Jan 13, 2021 10:18:24.646372080 CET	49747	40700	192.168.2.3	185.157.161.86
Jan 13, 2021 10:18:24.651071072 CET	40700	49747	185.157.161.86	192.168.2.3
Jan 13, 2021 10:18:24.651117086 CET	40700	49747	185.157.161.86	192.168.2.3
Jan 13, 2021 10:18:24.651154041 CET	40700	49747	185.157.161.86	192.168.2.3
Jan 13, 2021 10:18:24.651186943 CET	49747	40700	192.168.2.3	185.157.161.86
Jan 13, 2021 10:18:24.651247978 CET	40700	49747	185.157.161.86	192.168.2.3
Jan 13, 2021 10:18:24.651350975 CET	49747	40700	192.168.2.3	185.157.161.86
Jan 13, 2021 10:18:24.651381016 CET	40700	49747	185.157.161.86	192.168.2.3
Jan 13, 2021 10:18:24.677258968 CET	40700	49747	185.157.161.86	192.168.2.3
Jan 13, 2021 10:18:24.677321911 CET	40700	49747	185.157.161.86	192.168.2.3
Jan 13, 2021 10:18:24.677360058 CET	40700	49747	185.157.161.86	192.168.2.3
Jan 13, 2021 10:18:24.677427053 CET	49747	40700	192.168.2.3	185.157.161.86

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 10:16:25.588076115 CET	58361	53	192.168.2.3	8.8.8.8
Jan 13, 2021 10:16:25.636162996 CET	53	58361	8.8.8.8	192.168.2.3
Jan 13, 2021 10:16:26.546324968 CET	63492	53	192.168.2.3	8.8.8.8
Jan 13, 2021 10:16:26.597145081 CET	53	63492	8.8.8.8	192.168.2.3
Jan 13, 2021 10:16:27.383486986 CET	60831	53	192.168.2.3	8.8.8.8
Jan 13, 2021 10:16:27.447304964 CET	53	60831	8.8.8.8	192.168.2.3
Jan 13, 2021 10:16:28.179534912 CET	60100	53	192.168.2.3	8.8.8.8
Jan 13, 2021 10:16:28.230333090 CET	53	60100	8.8.8.8	192.168.2.3
Jan 13, 2021 10:16:29.101223946 CET	53195	53	192.168.2.3	8.8.8.8
Jan 13, 2021 10:16:29.149468899 CET	53	53195	8.8.8.8	192.168.2.3
Jan 13, 2021 10:16:30.176811934 CET	50141	53	192.168.2.3	8.8.8.8
Jan 13, 2021 10:16:30.227729082 CET	53	50141	8.8.8.8	192.168.2.3
Jan 13, 2021 10:16:31.113049030 CET	53023	53	192.168.2.3	8.8.8.8
Jan 13, 2021 10:16:31.160996914 CET	53	53023	8.8.8.8	192.168.2.3
Jan 13, 2021 10:16:32.278944016 CET	49563	53	192.168.2.3	8.8.8.8
Jan 13, 2021 10:16:32.326936960 CET	53	49563	8.8.8.8	192.168.2.3
Jan 13, 2021 10:16:33.979722977 CET	51352	53	192.168.2.3	8.8.8.8
Jan 13, 2021 10:16:34.027630091 CET	53	51352	8.8.8.8	192.168.2.3
Jan 13, 2021 10:16:34.787209034 CET	59349	53	192.168.2.3	8.8.8.8
Jan 13, 2021 10:16:34.835278988 CET	53	59349	8.8.8.8	192.168.2.3
Jan 13, 2021 10:16:35.579917908 CET	57084	53	192.168.2.3	8.8.8.8
Jan 13, 2021 10:16:35.628056049 CET	53	57084	8.8.8.8	192.168.2.3
Jan 13, 2021 10:16:36.404805899 CET	58823	53	192.168.2.3	8.8.8.8
Jan 13, 2021 10:16:36.452902079 CET	53	58823	8.8.8.8	192.168.2.3
Jan 13, 2021 10:16:37.318686962 CET	57568	53	192.168.2.3	8.8.8.8
Jan 13, 2021 10:16:37.366640091 CET	53	57568	8.8.8.8	192.168.2.3
Jan 13, 2021 10:16:38.166954041 CET	50540	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 10:16:38.218033075 CET	53	50540	8.8.8.8	192.168.2.3
Jan 13, 2021 10:17:00.392678022 CET	54366	53	192.168.2.3	8.8.8.8
Jan 13, 2021 10:17:00.451812983 CET	53	54366	8.8.8.8	192.168.2.3
Jan 13, 2021 10:17:07.054548979 CET	53034	53	192.168.2.3	8.8.8.8
Jan 13, 2021 10:17:07.102667093 CET	53	53034	8.8.8.8	192.168.2.3
Jan 13, 2021 10:17:10.299029112 CET	57762	53	192.168.2.3	8.8.8.8
Jan 13, 2021 10:17:10.356970072 CET	53	57762	8.8.8.8	192.168.2.3
Jan 13, 2021 10:17:14.910196066 CET	55435	53	192.168.2.3	8.8.8.8
Jan 13, 2021 10:17:14.968230963 CET	53	55435	8.8.8.8	192.168.2.3
Jan 13, 2021 10:17:16.544255972 CET	50713	53	192.168.2.3	8.8.8.8
Jan 13, 2021 10:17:16.603800058 CET	53	50713	8.8.8.8	192.168.2.3
Jan 13, 2021 10:17:19.857759953 CET	56132	53	192.168.2.3	8.8.8.8
Jan 13, 2021 10:17:19.918687105 CET	53	56132	8.8.8.8	192.168.2.3
Jan 13, 2021 10:17:28.169715881 CET	58987	53	192.168.2.3	8.8.8.8
Jan 13, 2021 10:17:28.234174013 CET	53	58987	8.8.8.8	192.168.2.3
Jan 13, 2021 10:18:04.993757010 CET	56579	53	192.168.2.3	8.8.8.8
Jan 13, 2021 10:18:05.041783094 CET	53	56579	8.8.8.8	192.168.2.3
Jan 13, 2021 10:18:05.433362007 CET	60633	53	192.168.2.3	8.8.8.8
Jan 13, 2021 10:18:05.497874022 CET	53	60633	8.8.8.8	192.168.2.3
Jan 13, 2021 10:18:21.244446993 CET	61292	53	192.168.2.3	8.8.8.8
Jan 13, 2021 10:18:21.308711052 CET	53	61292	8.8.8.8	192.168.2.3
Jan 13, 2021 10:18:21.970290899 CET	63619	53	192.168.2.3	8.8.8.8
Jan 13, 2021 10:18:22.055340052 CET	64938	53	192.168.2.3	8.8.8.8
Jan 13, 2021 10:18:22.103426933 CET	53	64938	8.8.8.8	192.168.2.3
Jan 13, 2021 10:18:22.143655062 CET	53	63619	8.8.8.8	192.168.2.3
Jan 13, 2021 10:19:14.275618076 CET	61946	53	192.168.2.3	8.8.8.8
Jan 13, 2021 10:19:14.360590935 CET	53	61946	8.8.8.8	192.168.2.3
Jan 13, 2021 10:19:14.806078911 CET	64910	53	192.168.2.3	8.8.8.8
Jan 13, 2021 10:19:14.862519026 CET	53	64910	8.8.8.8	192.168.2.3
Jan 13, 2021 10:19:15.392956018 CET	52123	53	192.168.2.3	8.8.8.8
Jan 13, 2021 10:19:15.462754965 CET	53	52123	8.8.8.8	192.168.2.3
Jan 13, 2021 10:19:15.920629025 CET	56130	53	192.168.2.3	8.8.8.8
Jan 13, 2021 10:19:15.980170965 CET	53	56130	8.8.8.8	192.168.2.3
Jan 13, 2021 10:19:16.363198042 CET	56338	53	192.168.2.3	8.8.8.8
Jan 13, 2021 10:19:16.419696093 CET	53	56338	8.8.8.8	192.168.2.3
Jan 13, 2021 10:19:16.858954906 CET	59420	53	192.168.2.3	8.8.8.8
Jan 13, 2021 10:19:16.915719986 CET	53	59420	8.8.8.8	192.168.2.3
Jan 13, 2021 10:19:17.363606930 CET	58784	53	192.168.2.3	8.8.8.8
Jan 13, 2021 10:19:17.411675930 CET	53	58784	8.8.8.8	192.168.2.3
Jan 13, 2021 10:19:17.964610100 CET	63978	53	192.168.2.3	8.8.8.8
Jan 13, 2021 10:19:18.020894051 CET	53	63978	8.8.8.8	192.168.2.3
Jan 13, 2021 10:19:18.641583920 CET	62938	53	192.168.2.3	8.8.8.8
Jan 13, 2021 10:19:18.700896978 CET	53	62938	8.8.8.8	192.168.2.3
Jan 13, 2021 10:19:19.112045050 CET	55708	53	192.168.2.3	8.8.8.8
Jan 13, 2021 10:19:19.168608904 CET	53	55708	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 13, 2021 10:18:21.970290899 CET	192.168.2.3	8.8.8.8	0x3f77	Standard query (0)	nanopc.linkpc.net	A (IP address)	IN (0x0001)

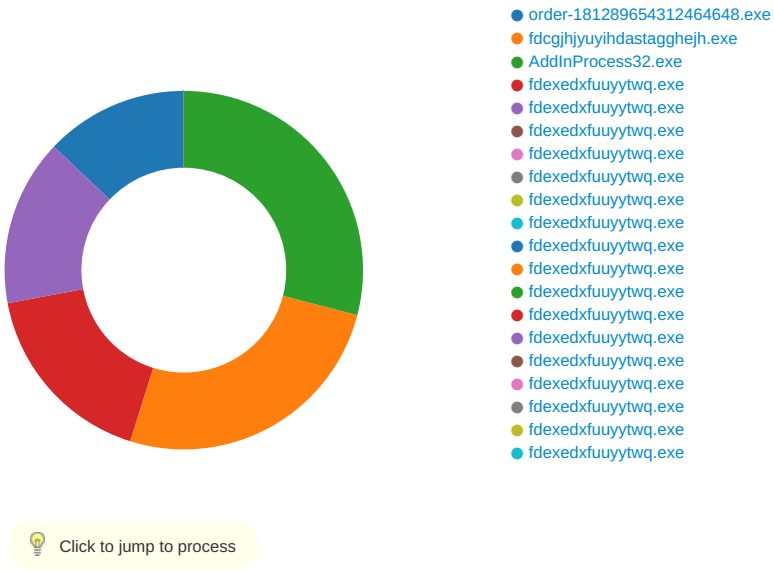
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2021 10:18:21.308711052 CET	8.8.8.8	192.168.2.3	0xddbc	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 10:18:22.143655062 CET	8.8.8.8	192.168.2.3	0x3f77	No error (0)	nanopc.linkpc.net		185.157.161.86	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: order-181289654312464648.exe PID: 5964 Parent PID: 5652

General

Start time:	10:16:32
Start date:	13/01/2021
Path:	C:\Users\user\Desktop\order-181289654312464648.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\order-181289654312464648.exe'
Imagebase:	0x50000
File size:	5815808 bytes
MD5 hash:	28DA42C2CD57E51CB8EA7DF263802924
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: 00000000.00000002.315049409.0000000003B84000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.315049409.0000000003B84000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.315049409.0000000003B84000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.314866304.0000000003A5E000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.314866304.0000000003A5E000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.314866304.0000000003A5E000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.315098998.0000000003C10000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.315098998.0000000003C10000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.315098998.0000000003C10000.00000004.00000001.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\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\order-181289654312464648.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E40C78D	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\order-181289654312464648.exe.log	unknown	1451	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 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 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 50 72 65 73 65 6e 74 61 74 69 6f 6e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..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..3,"PresentationCore, Version=	success or wait	1	6E40C907	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	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0D5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0DCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\dd5a228cf16a218ff0d3f02cdcbab8c9\WindowsBase.ni.dll.aux	unknown	1348	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xaml\8c85184f1e0cfe359eea86373661a3f8\System.Xaml.ni.dll.aux	unknown	572	success or wait	1	6E0303DE	ReadFile

Analysis Process: fdcgjhjyuyihdastagghejh.exe PID: 6692 Parent PID: 5964

General

Start time:	10:17:19
Start date:	13/01/2021
Path:	C:\Users\user\AppData\Roaming\fdcgjhjyuyihdastagghejh.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\fdcgjhjyuyihdastagghejh.exe'
Imagebase:	0x8c0000
File size:	5815808 bytes
MD5 hash:	28DA42C2CD57E51CB8EA7DF263802924
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: 0000000D.00000002.623442854.00000000044AD000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.623442854.00000000044AD000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000002.623442854.00000000044AD000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.624104734.000000000465F000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.624104734.000000000465F000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000002.624104734.000000000465F000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000003.390444818.000000000470C000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000003.390444818.000000000470C000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000003.390444818.000000000470C000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.623152761.0000000004411000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.623152761.0000000004411000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000002.623152761.0000000004411000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.624021744.00000000045D3000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.624021744.00000000045D3000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000002.624021744.00000000045D3000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
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	6E0FCF06	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	6E0FCF06	unknown
C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.txt	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CF41E60	CreateFileW
C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CF41E60	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.txt	unknown	69	36 36 39 32 0d 0a 43 3a 5c 55 73 65 72 73 5c 68 61 72 64 7a 5c 41 70 70 44 61 74 61 5c 52 6f 61 6d 69 6e 67 5c 66 64 63 67 6a 68 6a 79 75 79 69 68 64 61 73 74 61 67 67 68 65 6a 68 2e 65 78 65 0d 0a 30 0d 0a	6692..C:\Users\user\AppData\Roaming\fdcgjhjyuyihdastagghejh.exe..0..	success or wait	1	6CF41B4F	WriteFile
C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.exe	unknown	78336	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 59 20 14 c7 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 26 01 00 00 0a 00 00 00 00 00 00 de 44 01 00 00 20 00 00 00 00 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 a0 01 00 00 02 00 00 00 00 00 00 02 00 60 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...Y................P..&...........D.........@.. ....`..............................	success or wait	1	6CF41B4F	WriteFile
C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.txt	unknown	69	36 36 39 32 0d 0a 43 3a 5c 55 73 65 72 73 5c 68 61 72 64 7a 5c 41 70 70 44 61 74 61 5c 52 6f 61 6d 69 6e 67 5c 66 64 63 67 6a 68 6a 79 75 79 69 68 64 61 73 74 61 67 67 68 65 6a 68 2e 65 78 65 0d 0a 30 0d 0a	6692..C:\Users\user\AppData\Roaming\fdcgjhjyuyihdastagghejh.exe..0..	success or wait	9	6CF41B4F	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	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0D5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0DCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\dd5a228cf16a218ff0d3f02cdcbab8c9\WindowsBase.ni.dll.aux	unknown	1348	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xaml\8c85184f1e0cfe359eea86373661a3f8\System.Xaml.ni.dll.aux	unknown	572	success or wait	1	6E0303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0D5705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.txt	unknown	4096	success or wait	1	6CF41B4F	ReadFile
C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.txt	unknown	4096	success or wait	1	6CF41B4F	ReadFile
C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.txt	unknown	4096	success or wait	1	6CF41B4F	ReadFile
C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.txt	unknown	4096	success or wait	10	6CF41B4F	ReadFile
C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.txt	unknown	4096	success or wait	8	6CF41B4F	ReadFile

Analysis Process: AddInProcess32.exe PID: 4316 Parent PID: 6692

General

Start time:	10:17:59
Start date:	13/01/2021
Path:	C:\Users\user\AppData\Local\Temp\AddInProcess32.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\AddInProcess32.exe
Imagebase:	0x6a0000
File size:	42080 bytes
MD5 hash:	F2A47587431C466535F3C3D3427724BE
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: 0000000F.00000002.624408872.0000000005C00000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000F.00000002.624408872.0000000005C00000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000002.624408872.0000000005C00000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000002.624910732.0000000006BD0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000F.00000002.624910732.0000000006BD0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000002.625265297.0000000006CE0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000F.00000002.625265297.0000000006CE0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000002.625016694.0000000006C30000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000F.00000002.625016694.0000000006C30000.00000004.00000001.sdmp, Author: Florian Roth • Rule: NanoCore, Description: unknown, Source: 0000000F.00000002.612358336.0000000002BA4000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000002.624983363.0000000006C10000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000F.00000002.624983363.0000000006C10000.00000004.00000001.sdmp, Author: Florian Roth • Rule: NanoCore, Description: unknown, Source: 0000000F.00000002.620423784.0000000003E84000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000002.625032550.0000000006C40000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000F.00000002.625032550.0000000006C40000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000002.619247841.0000000003B51000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000002.625156989.0000000006CA0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000F.00000002.625156989.0000000006CA0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000002.625048622.0000000006C50000.00000004.00000001.sdmp, Author:

	Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000F.00000002.625048622.0000000006C50000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000002.605043000.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000002.605043000.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000002.605043000.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000002.625126493.0000000006C90000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000F.00000002.625126493.0000000006C90000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000002.624889874.0000000006BC0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000F.00000002.624889874.0000000006BC0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: NanoCore, Description: unknown, Source: 0000000F.00000002.619550033.0000000003C3E000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000002.625086476.0000000006C70000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000F.00000002.625086476.0000000006C70000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000002.624999401.0000000006C20000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000F.00000002.624999401.0000000006C20000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000002.623946602.00000000051A0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000F.00000002.623946602.00000000051A0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000002.625068564.0000000006C60000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000F.00000002.625068564.0000000006C60000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000002.620771478.0000000003F6F000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000002.620771478.0000000003F6F000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 0%, Virustotal, Browse • Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

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	6E0FCF06	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	6E0FCF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6CF4BEFF	CreateDirectoryW
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	6CF41E60	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	6CF4BEFF	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	6CF4BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CF41E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CF41E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CF41E60	CreateFileW

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	4a 3d c7 91 ef b7 d8 48	J=.....H	success or wait	1	6CF41B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	unknown	232	47 6a 93 68 5c a3 33 c7 ba 41 97 d8 c4 35 b2 78 95 96 26 15 ab 98 69 2b 98 cd 89 63 28 31 a3 50 c6 e5 50 83 63 4c 54 a1 9f c5 82 41 c5 62 c9 e2 1b 95 b8 f0 f0 e7 34 68 a6 12 b5 74 bc 2b f0 07 5a 5c b0 bf 20 9f 69 cc d5 c2 a4 ed f2 80 40 dc 33 8c a4 7b 0c cc 1c 67 72 76 2b 56 81 e7 f3 bf b9 42 19 0e 82 0d c5 eb 15 5d f3 50 8b f6 16 57 df 34 43 7d 75 4c 1e b2 93 0b a6 73 7e 82 c7 46 04 b7 fb 7d 99 ad 83 81 ed 81 00 45 f9 c7 db f0 db f0 45 f9 14 f3 b4 36 45 8f 94 b5 81 a3 7b d9 9f 05 18 7b ed a9 79 53 82 bd bf 37 fa c4 22 16 68 4b d7 21 03 78 86 32 be 99 69 df a3 8f 7a 4a d5 da bb fa 20 fc b4 c0 c0 66 d0 dd a7 3f c0 5f 0b e4 fb a3 30 ca 3a 65 5b 37 77 7b 31 81 21 de 34 a9 bb 99 d3 ca 26 b9	Gj.h\.3..A...5.x..&...i+...c(1 .P..P.cLT....A.b.....4h...t .+..Z\.. .i.....@.3..{...grv +V.....B.....].P...W.4C}uL.. ...s~..F...}.....E.....E... .6E.....{....{..yS...7..".hK.! .x.2..i...zJ.... ....f...?._.. ..0.:e[7w{1.!.4.....&.	success or wait	1	6CF41B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	unknown	327432	70 54 c7 ab ad 21 b0 08 57 f6 fa 47 14 4a ba aa 61 dd a0 29 17 40 c6 8b 69 8b df 77 70 4b 98 73 6f 40 e2 06 e5 35 e7 b7 3d e9 b8 90 5e ab 1d 51 82 6f 79 f9 3d 65 40 39 c3 42 8d f7 95 46 bc cb 30 39 75 22 33 8b f5 20 30 74 c0 19 52 44 6e 5f 34 64 fb b8 17 02 df 45 c0 90 06 69 f4 08 9f ae bb 8a 7e 0c 89 85 7c 87 eb 66 58 5f 0e c2 ed 58 66 88 70 5e e2 f5 ff 94 03 e5 3e 61 db 8b 91 24 8d 8a 8f 65 05 36 3a 37 64 b6 28 61 05 41 e4 fe e0 3d be 29 2a 0d 96 a8 90 8e 7b 42 1c 5b ab 87 cb 79 25 b3 2a e4 b8 b1 9f 69 a7 51 84 3c f3 94 a2 90 78 74 c4 a9 58 13 11 48 09 d7 20 ad cc a4 48 46 37 67 0f e0 c5 49 96 2a 33 03 7b 0c 6e 92 bf 90 be 4c d1 9b 79 3b 69 87 bc 73 2d 1e b6 f9 b8 28 35 69 c2 8b 92 d6 10 ac a7 02 93 ee 89 08 17 4a 09 35 62 37 7d fe 86 66 4b af ab 48 56	pT...!..W..G.J..a..).@..i..wpK .so@...5..=...^..Q.oy.=e@9 .B...F..09u"3.. 0t..RDn_4d.....E.. .i.....~...|..fX_....Xf.p^.... ..>a...$...e.6:7d.(a.A...=.)*. ....{B.[...y%.*....i.Q.<....xt ..X..H.. ...HF7g...I.*3.{.n... .L..y;i..s-....(5i..... .J.5b7}..fK..HV	success or wait	1	6CF41B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	unknown	40	39 69 48 cc 1a df 85 7d 5a d7 8d 34 00 a8 66 0d 7e 61 d3 f8 a3 01 06 96 0c a9 7e ba 7e 86 90 d9 e5 05 8d ca 33 e7 55 0b	9iH....}Z..4..f.~a.....~.~. .....3.U.	success or wait	1	6CF41B4F	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	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0D5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0DCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF41B4F	ReadFile
C:\Users\user\AppData\Local\Temp\AddInProcess32.exe	unknown	4096	success or wait	1	6E0BD72F	unknown
C:\Users\user\AppData\Local\Temp\AddInProcess32.exe	unknown	512	success or wait	1	6E0BD72F	unknown

Analysis Process: fdexedxfuuyytwq.exe PID: 5168 Parent PID: 6692

General

Start time:	10:18:09
Start date:	13/01/2021

Path:	C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.exe'
Imagebase:	0x860000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 7%, Virustotal, Browse • Detection: 3%, Metadefender, Browse • Detection: 7%, ReversingLabs
Reputation:	moderate

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\fdexedxfuuyytwq.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E40C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.txt	unknown	72	36 36 39 32 0d 0a 43 3a 5c 55 73 65 72 73 5c 68 61 72 64 7a 5c 41 70 70 44 61 74 61 5c 52 6f 61 6d 69 6e 67 5c 66 64 63 67 6a 68 6a 79 75 79 69 68 64 61 73 74 61 67 67 68 65 6a 68 2e 65 78 65 0d 0a 35 31 36 38 0d 0a	6692..C:\Users\user\AppData\Roaming\fdcgjhjyuyihdastaggehejh.exe..5168..	success or wait	1	6CF41B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\fdexedxfuuyytwq.exe.log	unknown	1362	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 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 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 50 72 65 73 65 6e 74 61 74 69 6f 6e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d	1,"fusion","GAC",0..1,"WinRT","NotApp",1..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..3,"PresentationCore, Version=	success or wait	1	6E40C907	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	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0D5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0DCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5a e0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationC ore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\d d5a228cf16a218ff0d3f02cdcbab8c9\WindowsBase.ni.dll.aux	unknown	1348	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xaml\8 c85184f1e0cfe359eea86373661a3f8\System.Xaml.ni.dll.aux	unknown	572	success or wait	1	6E0303DE	ReadFile
C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.txt	unknown	4096	success or wait	1	6CF41B4F	ReadFile
C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.txt	unknown	4096	success or wait	1	6CF41B4F	ReadFile
C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.txt	unknown	4096	success or wait	1	6CF41B4F	ReadFile

Analysis Process: fdexedxfuuyytwq.exe PID: 5188 Parent PID: 5168

General

Start time:	10:18:12
Start date:	13/01/2021
Path:	C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.exe'
Imagebase:	0xda0000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.txt	unknown	72	36 36 39 32 0d 0a 43 3a 5c 55 73 65 72 73 5c 68 61 72 64 7a 5c 41 70 70 44 61 74 61 5c 52 6f 61 6d 69 6e 67 5c 66 64 63 67 6a 68 6a 79 75 79 69 68 64 61 73 74 61 67 67 68 65 6a 68 2e 65 78 65 0d 0a 35 31 38 38 0d 0a	6692..C:\Users\user\AppData\Ro aming\fdcgjhjyuyihdastagg hejh.exe..5188..	success or wait	1	6CF41B4F	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	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0D5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0DCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5a e0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	6E0303DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\dd5a228cf16a218ff0d3f02cdcbab8c9\WindowsBase.ni.dll.aux	unknown	1348	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xaml\8c85184f1e0cfe359eea86373661a3f8\System.Xaml.ni.dll.aux	unknown	572	success or wait	1	6E0303DE	ReadFile
C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.txt	unknown	4096	success or wait	1	6CF41B4F	ReadFile
C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.txt	unknown	4096	success or wait	1	6CF41B4F	ReadFile
C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.txt	unknown	4096	success or wait	1	6CF41B4F	ReadFile

Analysis Process: fdexedxfuuyytwq.exe PID: 5688 Parent PID: 6692

General

Start time:	10:18:15
Start date:	13/01/2021
Path:	C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.exe'
Imagebase:	0x510000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

Analysis Process: fdexedxfuuyytwq.exe PID: 3564 Parent PID: 5688

General

Start time:	10:18:18
Start date:	13/01/2021
Path:	C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.exe'
Imagebase:	0x740000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

Analysis Process: fdexedxfuuyytwq.exe PID: 1048 Parent PID: 6692

General

Start time:	10:18:21
Start date:	13/01/2021
Path:	C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.exe'
Imagebase:	0x220000

File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

Analysis Process: fdexedxfuuyytwq.exe PID: 5044 Parent PID: 1048

General

Start time:	10:18:23
Start date:	13/01/2021
Path:	C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.exe'
Imagebase:	0xd80000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

Analysis Process: fdexedxfuuyytwq.exe PID: 6328 Parent PID: 6692

General

Start time:	10:18:27
Start date:	13/01/2021
Path:	C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.exe'
Imagebase:	0xff0000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

Analysis Process: fdexedxfuuyytwq.exe PID: 6816 Parent PID: 6328

General

Start time:	10:18:29
Start date:	13/01/2021
Path:	C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.exe'
Imagebase:	0x170000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

Analysis Process: fdexedxfuuyytwq.exe PID: 6880 Parent PID: 6692

General

Start time:	10:18:32
Start date:	13/01/2021
Path:	C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.exe'
Imagebase:	0x650000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

Analysis Process: fdexedxfuuyytwq.exe PID: 6708 Parent PID: 6880

General

Start time:	10:18:36
Start date:	13/01/2021
Path:	C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.exe'
Imagebase:	0xf70000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

Analysis Process: fdexedxfuuyytwq.exe PID: 6800 Parent PID: 6692

General

Start time:	10:18:40
Start date:	13/01/2021
Path:	C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.exe'
Imagebase:	0xd60000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

Analysis Process: fdexedxfuuyytwq.exe PID: 5504 Parent PID: 6800

General

Start time:	10:18:42

Start date:	13/01/2021
Path:	C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.exe'
Imagebase:	0x10000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

Analysis Process: fdexedxfuuyytwq.exe PID: 6124 Parent PID: 6692

General

Start time:	10:18:46
Start date:	13/01/2021
Path:	C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.exe'
Imagebase:	0xe20000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

Analysis Process: fdexedxfuuyytwq.exe PID: 6892 Parent PID: 6124

General

Start time:	10:18:48
Start date:	13/01/2021
Path:	C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.exe'
Imagebase:	0xe70000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

Analysis Process: fdexedxfuuyytwq.exe PID: 2792 Parent PID: 6692

General

Start time:	10:18:54
Start date:	13/01/2021
Path:	C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.exe'
Imagebase:	0xcf0000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: fdexedxfuuyytwq.exe PID: 6936 Parent PID: 2792

General

Start time:	10:18:57
Start date:	13/01/2021
Path:	C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.exe'
Imagebase:	0x830000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: fdexedxfuuyytwq.exe PID: 7120 Parent PID: 6692

General

Start time:	10:19:01
Start date:	13/01/2021
Path:	C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\fdexedxfuuyytwq.exe'
Imagebase:	0x5c0000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Disassembly

Code Analysis