ID: 337596
Sample Name:
Payment_Confirmation pdf.exe
Cookbook: default.jbs
Time: 20:06:25
Date: 08/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

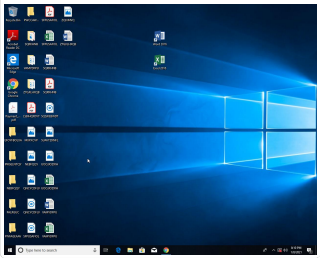
Analysis Report Payment_Confirmation pdf.exe

Overview

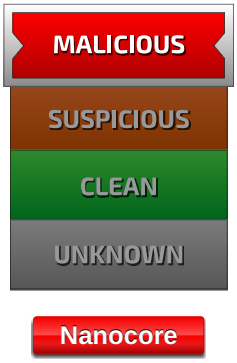
General Information

Sample Name:	Payment_Confirmation pdf.exe
Analysis ID:	337596
MD5:	767f88a961bfbc1..
SHA1:	5577d0635fca390.
SHA256:	4f0035201ba7a3a.
Tags:	exe

Most interesting Screenshot:



Detection

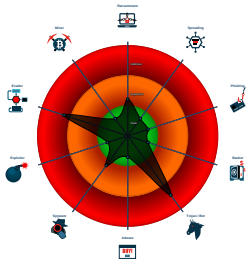


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Detected Nanocore Rat
- Malicious sample detected (through …
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file…
- Yara detected Nanocore RAT
- Allocates memory in foreign process…
- Executable has a suspicious name (…
- Hides that the sample has been dow…
- Initial sample is a PE file and has a …
- Injects a PE file into a foreign proce…
- Machine Learning detection for samp…
- Uses schtasks.exe or at.exe to add

Classification



Startup

- **System is w10x64**
- Payment_Confirmation pdf.exe (PID: 2800 cmdline: 'C:\Users\user\Desktop\Payment_Confirmation pdf.exe' MD5: 767F88A961BFBC1B8F8419A32FBADE0B)
  - vbc.exe (PID: 5332 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe MD5: B3A917344F5610BEEC562556F11300FA)
  - vbc.exe (PID: 5952 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe MD5: B3A917344F5610BEEC562556F11300FA)
  - vbc.exe (PID: 1516 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe MD5: B3A917344F5610BEEC562556F11300FA)
  - vbc.exe (PID: 5352 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe MD5: B3A917344F5610BEEC562556F11300FA)
    - schtasks.exe (PID: 4660 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp863B.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 1304 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 2172 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmp8988.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 5992 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- vbc.exe (PID: 3996 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe 0 MD5: B3A917344F5610BEEC562556F11300FA)
  - conhost.exe (PID: 5972 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- dhcpmon.exe (PID: 5836 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 MD5: B3A917344F5610BEEC562556F11300FA)
  - conhost.exe (PID: 4604 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- dhcpmon.exe (PID: 1000 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: B3A917344F5610BEEC562556F11300FA)
  - conhost.exe (PID: 5796 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
00000000.00000002.233380857.0000000003A0 1000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x472ed:$x1: NanoCore.ClientPluginHost • 0x79f1d:$x1: NanoCore.ClientPluginHost • 0xac93d:$x1: NanoCore.ClientPluginHost • 0x4732a:$x2: IClientNetworkHost • 0x79f5a:$x2: IClientNetworkHost • 0xac97a:$x2: IClientNetworkHost • 0x4ae5d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x7da8d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0xb04ad:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000000.00000002.233380857.0000000003A0 1000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000000.00000002.233380857.0000000003A0 1000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x47055:$a: NanoCore • 0x47065:$a: NanoCore • 0x47299:$a: NanoCore • 0x472ad:$a: NanoCore • 0x472ed:$a: NanoCore • 0x79c85:$a: NanoCore • 0x79c95:$a: NanoCore • 0x79ec9:$a: NanoCore • 0x79edd:$a: NanoCore • 0x79f1d:$a: NanoCore • 0xac6a5:$a: NanoCore • 0xac6b5:$a: NanoCore • 0xac8e9:$a: NanoCore • 0xac8fd:$a: NanoCore • 0xac93d:$a: NanoCore • 0x470b4:$b: ClientPlugin • 0x472b6:$b: ClientPlugin • 0x472f6:$b: ClientPlugin • 0x79ce4:$b: ClientPlugin • 0x79ee6:$b: ClientPlugin • 0x79f26:$b: ClientPlugin
Process Memory Space: Payment_Confirmation pdf.exe PID: 2800	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x131d1:$x1: NanoCore.ClientPluginHost • 0x31b3f:$x1: NanoCore.ClientPluginHost • 0x50410:$x1: NanoCore.ClientPluginHost • 0x13232:$x2: IClientNetworkHost • 0x31ba0:$x2: IClientNetworkHost • 0x50471:$x2: IClientNetworkHost • 0x18637:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x265a9:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x36fa5:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8 JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x44f17:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8 JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x55876:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x637e8:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Process Memory Space: Payment_Confirmation pdf.exe PID: 2800	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 1 entries				

Sigma Overview

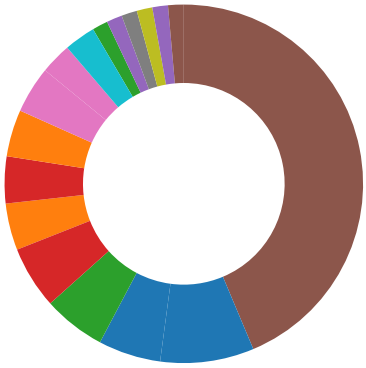
System Summary:

Sigma detected: NanoCore

Sigma detected: Scheduled temp file as task from temp location

Signature Overview

- AV Detection
- Compliance
- Spreading
- Networking
- 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:

Antivirus / Scanner detection for submitted sample

Yara detected Nanocore RAT

Machine Learning detection for sample

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Executable has a suspicious name (potential lure to open the executable)

Initial sample is a PE file and has a suspicious name

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

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:

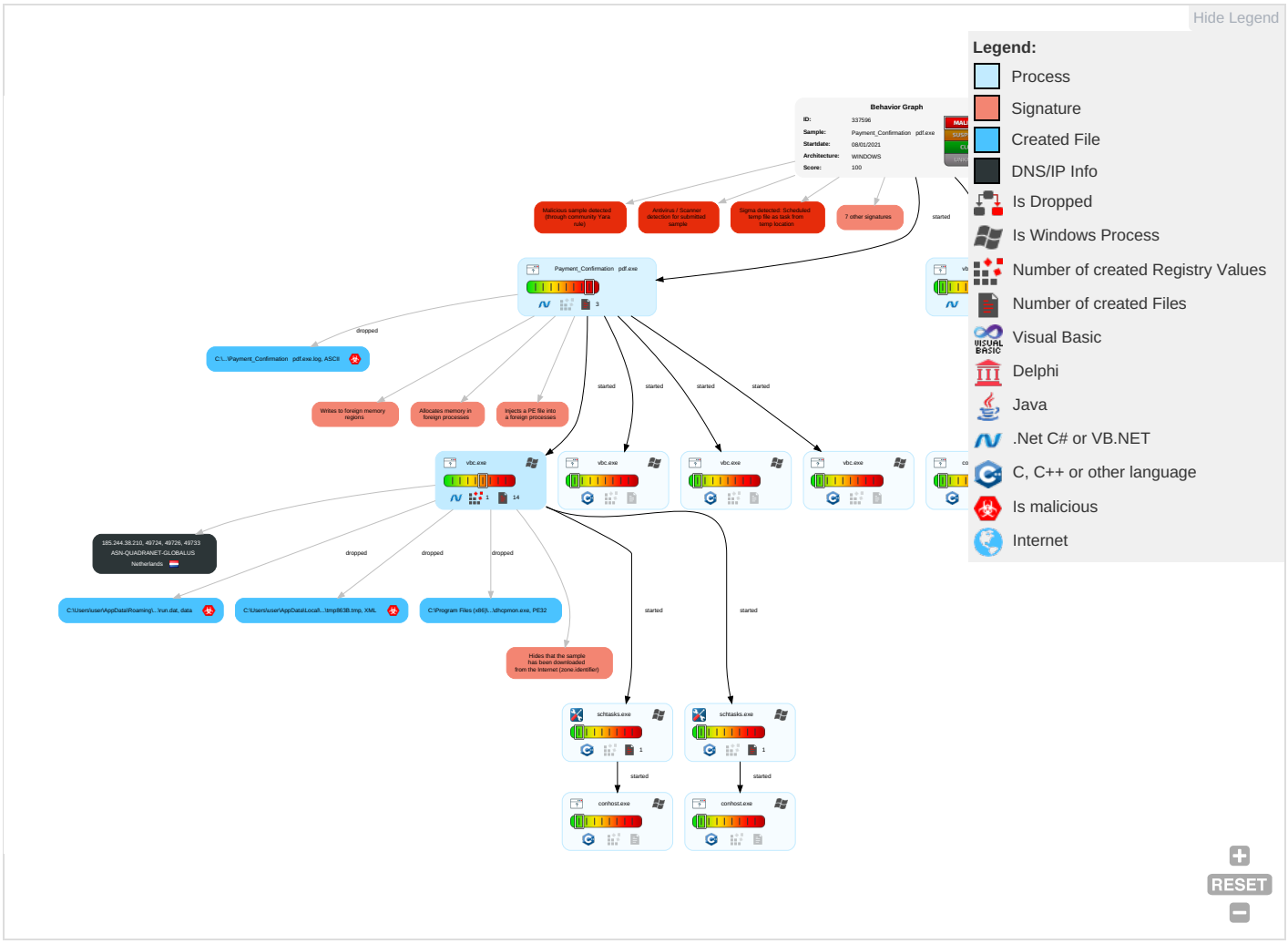
Detected Nanocore Rat

Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effec
Valid Accounts	Windows Management Instrumentation 1	Scheduled Task/Job 1	Process Injection 3 1 1	Masquerading 2	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eave Insec Netw Comr
Default Accounts	Command and Scripting Interpreter 2	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Virtualization/Sandbox Evasion 2	LSASS Memory	Security Software Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Standard Port 1	Explo Redir Calls/
Domain Accounts	Scheduled Task/Job 1	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Virtualization/Sandbox Evasion 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Explo Track Locat
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 3 1 1	NTDS	Process Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM (Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manip Devic Comr
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamn Denia Servi
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 3	DCSync	System Information Discovery 1 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogu Acce
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Down Insec Proto

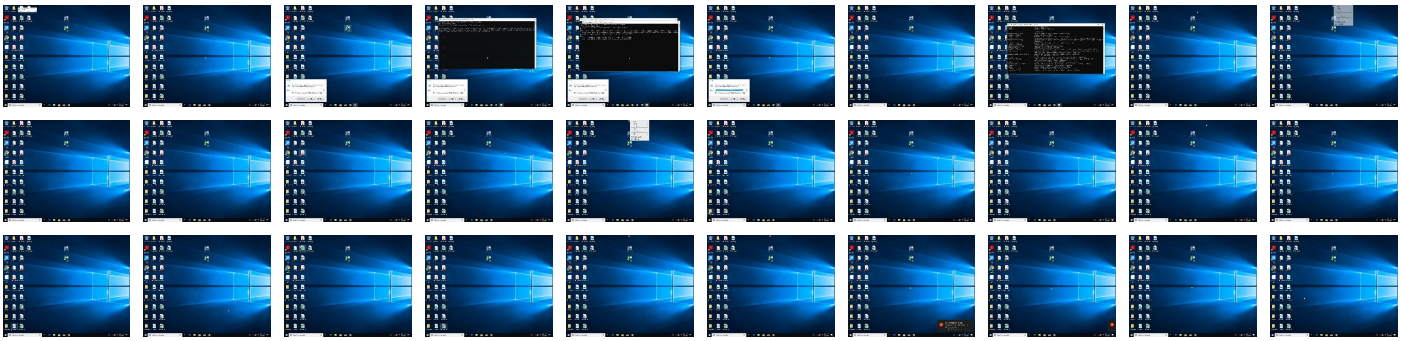
Behavior Graph



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
Payment_Confirmation pdf.exe	100%	Avira	TR/Dropper.MSIL.Gen	
Payment_Confirmation pdf.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	2%	Metadefender		Browse
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.Payment_Confirmation pdf.exe.590000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File
0.0.Payment_Confirmation pdf.exe.590000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://go.microsoft	0%	Virustotal		Browse
http://go.microsoft	0%	Avira URL Cloud	safe	

Domains and IPs

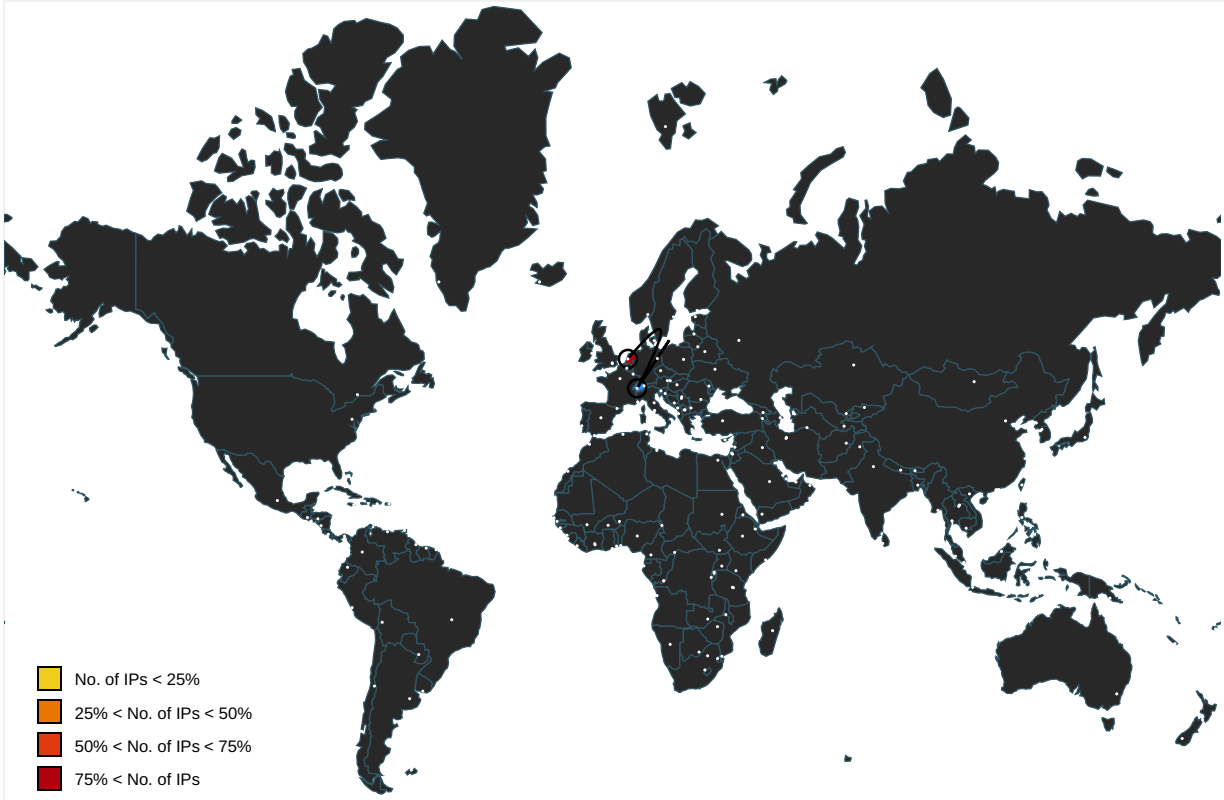
Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://go.microsoft	dhcpmon.exe, 0000000D.00000002.263266383.0000000000BAA000.00000004.00000010.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.244.38.210	unknown	Netherlands		8100	ASN-QUADRANET-GLOBALUS	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	337596
Start date:	08.01.2021
Start time:	20:06:25
Joe Sandbox Product:	CloudBasic

Overall analysis duration:	0h 10m 12s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Payment_Confirmation pdf.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	37
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@21/12@0/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 18% (good quality ratio 16.5%) • Quality average: 68.6% • Quality standard deviation: 28.6%
HCA Information:	Failed
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, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • 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 NtProtectVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
20:07:19	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
20:07:20	Task Scheduler	Run new task: DHCP Monitor path: "C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe" s>$(Arg0)
20:07:20	API Interceptor	1408x Sleep call for process: vbc.exe modified
20:07:21	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ASN-QUADRANET-GLOBALUS	npp.7.9.2.Installer (1).exe	Get hash	malicious	Browse	• 192.169.6.95
	http://https://linkprotect.cudasvc.com/url?a=http%3a%2f%2ffindcloud.id%2fwp-includes%2f8JTmzq3FN6z3OBJBdBCfXrdcZl5H7ZxOaOZzfl2H%2f&c=E,1,2CiyC7FGbs3Pvr1yrAWkewOmRL-xyrP42HL37xX4omRyLZqRrqWOt_1RKb6pLtfzxs7zIBTrrVMEwQ8pOUIr2mFuNwrd9eHNrfkptUp83QPlV-CrGIoXMw,,&typo=1	Get hash	malicious	Browse	• 173.254.250.226
	http://https://mrveggy.com/resgatecarrinho/jcWVa69vj8IDsQRCud8h6RNI9Mz17JqsPPJ0DFnlbXZGyMM2GcZ3/	Get hash	malicious	Browse	• 173.254.250.226
	1I72L29IL3F.doc	Get hash	malicious	Browse	• 173.254.250.226
	http://https://x9sademwnet.gb.net/bnbgfvgrthbg456tr54g6trvecds/?tuk5sx4dsb3=7df34dj4csa	Get hash	malicious	Browse	• 104.129.25.9
	xLH4kwOjXR.exe	Get hash	malicious	Browse	• 104.223.94.66
	utox.exe	Get hash	malicious	Browse	• 104.223.122.15
	QUOTES.exe	Get hash	malicious	Browse	• 69.174.99.26
	file.exe	Get hash	malicious	Browse	• 192.161.187.200
	http://jb092.com/rxlbakzd/goqmmbmi.html?kjmikw5x.3hllr	Get hash	malicious	Browse	• 185.174.103.81
	http://https://www.trackins.org/sale/cat/sale-c199387IoAL&C_fTkoAvATBo-1LAvvTgoAKL6_.T5.html?_emr=12e4edca-8183-44e0-bccb-e3d6e0eeb447&wfcs=cs2&dcrectxid=d48055ba-93d6-4b3f-80c6-70de3252bde6&_eml=2ec38d65-f3da-4587-bd38-7c1f333c6dc8&source=batch&batchid=04&varid=5&csnid=1eab81b4-e54d-4cc2-8735-a5d571cfe688&brcid=13&sm=1&refid=MKTEML_31000&emlid=1131&maiid=1913	Get hash	malicious	Browse	• 173.205.83.250
	Shipment Document BLINV And Packing List Attached.exe	Get hash	malicious	Browse	• 192.161.187.200
	kWbmxCNnPIYLMvvPIVlMbDKbbQCNjT.exe	Get hash	malicious	Browse	• 69.174.99.26
	Purchase Order.exe	Get hash	malicious	Browse	• 104.129.26.162
	SecuriteInfo.com.Variant.Bulz.265335.2250.exe	Get hash	malicious	Browse	• 66.63.162.20
	New order.xls	Get hash	malicious	Browse	• 66.63.162.20
	http://https://app.box.com/s/rdobxcyrhp1cdxwej3pfeyvngfh3lwag	Get hash	malicious	Browse	• 173.254.237.250
	http://https://bit.ly/2VPfIRO	Get hash	malicious	Browse	• 185.174.103.81
	http://https://bit.ly/2VPfIRO	Get hash	malicious	Browse	• 185.174.103.81
	PO122020.exe	Get hash	malicious	Browse	• 104.129.26.162

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	LIST OF ITEMS.pdf.exe	Get hash	malicious	Browse	
	Swift.pdf.gz.exe	Get hash	malicious	Browse	
	EXPORT SHIPMENT CERTIFIED 1.exe	Get hash	malicious	Browse	
	SWIFT_CONFIRMATION.pdf.exe	Get hash	malicious	Browse	
	FIRST ORDER_NOVEMBER.exe	Get hash	malicious	Browse	
	W89xuljgFe.exe	Get hash	malicious	Browse	
	MANDATORY ADVISORY.exe	Get hash	malicious	Browse	
	MTCopy.exe	Get hash	malicious	Browse	
	FIRST ORDER_NOVEMBER.exe	Get hash	malicious	Browse	
	Required SMS quantity.exe	Get hash	malicious	Browse	
	arrival notice-ETA 10th-11,2020.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Generic.mg.56564e2f274ac218.exe	Get hash	malicious	Browse	
	Purchase Order #016543.exe	Get hash	malicious	Browse	
	ORT09937378200002.PDF.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Purchase Order..exe	Get hash	malicious	Browse	
	Transfer form.exe	Get hash	malicious	Browse	
	paymentslip.exe	Get hash	malicious	Browse	
	Dekont.pdf.exe	Get hash	malicious	Browse	
	Bank Receipt.exe	Get hash	malicious	Browse	
	PAYMENT COPY.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	2688096
Entropy (8bit):	6.409257767499659
Encrypted:	false
SSDEEP:	49152:PAa87OQFMC/tWcHUgeRjRKW+0UpzIrFjB5u901ACUTum:PAa87zLtWI6jX+0UFIrZ//1a
MD5:	B3A917344F5610BEEC562556F11300FA
SHA1:	F7B1AC747E7705A21ACDD582B63800016BE21774
SHA-256:	7BA4838E3356B69254730E891ADD84092E3143016A515FF3E990CE19874A2459
SHA-512:	2D1515D75C3E5870F2FB57B321E02CF9611D30F3716A5670F0C32781AEB96576508B3B1C9717B2AC041B7752865842DD8AF7AF712988FF90FE3E6847821FFE60
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 2%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: LIST OF ITEMS.pdf.exe, Detection: malicious, Browse • Filename: Swift.pdf.gz.exe, Detection: malicious, Browse • Filename: EXPORT SHIPMENT CERTIFIED 1.exe, Detection: malicious, Browse • Filename: SWIFT_CONFIRMATION.pdf.exe, Detection: malicious, Browse • Filename: FIRST ORDER_NOVEMBER.exe, Detection: malicious, Browse • Filename: W89xuljgFe.exe, Detection: malicious, Browse • Filename: MANDATORY ADVISORY.exe, Detection: malicious, Browse • Filename: MTCopy.exe, Detection: malicious, Browse • Filename: FIRST ORDER_NOVEMBER.exe, Detection: malicious, Browse • Filename: Required SMS quantity.exe, Detection: malicious, Browse • Filename: arrival notice-ETA 10th-11,2020.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Generic.mg.56564e2f274ac218.exe, Detection: malicious, Browse • Filename: Purchase Order #016543.exe, Detection: malicious, Browse • Filename: ORT09937378200002.PDF.exe, Detection: malicious, Browse • Filename: Purchase Order..exe, Detection: malicious, Browse • Filename: Transfer form.exe, Detection: malicious, Browse • Filename: paymentslip.exe, Detection: malicious, Browse • Filename: Dekont.pdf.exe, Detection: malicious, Browse • Filename: Bank Receipt.exe, Detection: malicious, Browse • Filename: PAYMENT COPY.exe, Detection: malicious, Browse
Preview:	MZ.....@.....(.....!..L.!This program cannot be run in DOS mode....$.....d..O..O..O.....O.....O..v...O..v...O.....O.....O.....O..=:..O..=:..O..=:..O..v...O..O...N.....O.....O.....O.....O..Rich.O.....PE..L...`.Z.....".....".8..... "...@..... )......!)...@..... .....d.".V....#.....#.L.....(.`>....'.46....".T.....`...@.....#.....text...d.".....".....  ..`.data...,....".....".....@....idata.....#.....#.....@..@.tls.....#.....#.....@....rsrc...L.....#.....#.....@..@.reloc..46....'..8....'.....@..B.....

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Payment_Confirmation pdf.exe.log	
Process:	C:\Users\user\Desktop\Payment_Confirmation pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	522
Entropy (8bit):	5.348034597186669
Encrypted:	false
SSDEEP:	12:Q3La/hz92n4M9tDLI4MWuPk21OKbbDLI4MWuPJKiUrRZ9I0ZKhav:MLU84qpE4Ks2wKDE4KhK3VZ9pKhk
MD5:	D4AF6B20AEA9906B4FF574A174E96287
SHA1:	81655019BB100FAADD5B36755F798EE5FB09E672
SHA-256:	DD8AE93DA079839B31327D22A2408E0C3EA4DDE92FD389CD5B96AD57CCE7B2E1
SHA-512:	6D912AC17876D9C21E61ED8C1B435AEA0FBB27FB97626A40903B4DFFC1204BEF3A43B02805DEDD2531822FD6F62CF06F0D758C1B2CA07258E82F95225D71C16E
Malicious:	**true**
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..

C:\Users\user\AppData\Local\Temp\tmp863B.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1316
Entropy (8bit):	5.1354471369850545
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0mcEXxtn:cbk4oL600QydbQxIYODOLedq3ZPj
MD5:	808C6E96C170C90D0DB522E8947EB2BD
SHA1:	44583694C3C23410D637BB96C0DF0921363533AD
SHA-256:	C6B75FB7740D34D55D74B8664FF1EA778638A4916C2B52348EA34DE60EDD3AFC
SHA-512:	928B85E9FDDFD7C93623E954DC53367AAF355F74A14601D77E45612EBDB77F3D6C0FC853E154F91F61E64306361885467C16FC211CF1BBDC023658AD35DBA1E
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\tmp8988.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1310
Entropy (8bit):	5.109425792877704
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0R3xtn:cbk4oL600QydbQxIYODOLedq3S3j
MD5:	5C2F41CFC6F988C859DA7D727AC2B62A
SHA1:	68999C85FC7E37BAB9216E0099836D40D4545C1C
SHA-256:	98B6E66B6C2173B9B91FC97FE51805340EFDE978B695453742EBAB631018398B
SHA-512:	B5DA5DA378D038AFBF8A7738E47921ED39F9B726E2CAA2993D915D9291A3322F94EFE8CCA6E7AD678A670DB19926B22B20E5028460FCC89CEA7F6635E755733
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe
File Type:	data
Category:	dropped
Size (bytes):	1160
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	24:IQnybgCUtvd7xCFhwUuQnybgCUtvd7xCFhwUuQnybgCUtvd7xCFhwUuQnybgCUtd:Ik/lCrwfk/lCrwfk/lCrwfk/lCrwfk/a
MD5:	786E4F1138F3E30FB67C690E55AC5A4F
SHA1:	828C2B627BCB54053173B54C3A4C289EF3476641
SHA-256:	D953043AE0955AA739AF97A60DAC7541048D83FC7601365A861A527E59DBFA38
SHA-512:	5FA075AB5626579DFE5A96E5B6DABF60DC3DDBA8A6E5ADEF0538032E8FB000772C7DCB73D315B208A04125F014ACCB92FAA194108D4C76443B9FB7B97719FF6
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.....&.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.....&.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.....&.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.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Encrypted:	false
SSDEEP:	3:CWtn:Cqn
MD5:	98CFF23FC74E31CD53B1E5F35EDC7355
SHA1:	F3AF7CA1FF18550C89C1808F024B964BFA4466FB
SHA-256:	F1039C77669BBB367B0A5E8638902597904D389A5117680B171337DFF6D8E5E2
SHA-512:	48A6BC86AAC31DD55B328282240F4F4E8D6683870A0C8FBBA454BF0E2405B848567A206A75C58B0904A261A0AC09F2A3E51269666B7CE03A41EB2351B29125DF
Malicious:	**true**
Preview:	..y.T..H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	5.221928094887364
Encrypted:	false
SSDEEP:	3:9bzY6oRDMjmPl:RzWDMCd
MD5:	AE0F5E6CE7122AF264EC533C6B15A27B
SHA1:	1265A495C42EED76CC043D50C60C23297E76CCE1
SHA-256:	73B0B92179C61C26589B47E9732CE418B07EDEE3860EE5A2A5FB06F3B8AA9B26
SHA-512:	DD44C2D24D4E3A0F0B988AD3D04683B5CB128298043134649BBE33B2512CE0C9B1A8E7D893B9F66FBBCDD901E2B0646C4533FB6C0C8C4AFCB95A0EFB95D44F8
Malicious:	false
Preview:	9iH...}Z.4..f..... 8.j....|.&X..e.F.*.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe
File Type:	data
Category:	dropped
Size (bytes):	327432
Entropy (8bit):	**7.99938831605763**
Encrypted:	**true**
SSDEEP:	6144:oX44S90aTiB66x3Pl6nGV4bfD6wXPIZ9iBj0UeprGm2d7Tm:LkjYGsfGUc9iB4UeprKdnm
MD5:	7E8F4A764B981D5B82D1CC49D341E9C6
SHA1:	D9F0685A028FB219E1A6286AEFB7D6FCFC778B85
SHA-256:	0BD3AAC12623520C4E2031C8B96B4A154702F36F97F643158E91E987D317B480
SHA-512:	880E46504FCFB4B15B86B9D8087BA88E6C4950E433616EBB637799F42B081ABF6F07508943ECB1F786B2A89E751F5AE62D750BDCFFDDF535D600CF66EC44E92F7
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..$...e.6:7d.(a.A...=.)*.....{B.[...y%.*..i.Q.<..xt.X..H.. ..H F7g...I.*3.{.n....L.y;i..s-....(5i..........J.5b7}..fK..HV..,...0.... ....n.w6PMI.....v.'".v.....#..X.a...../...cC...i..l{>5n.._+.e.d'...}...[..../...D.t..GVp.zz.....(...o.....b...+`J.{....hS1G.^*I..v&. jm.#u..1..Mg!.E..U.T.....6.2>...6.l.K.w"o..E..."K%{....z.7....<...,....]t.:.....[.Z.u...3X8.QI..j_..&..N..q.e.2...6.R.~..9.Bq..A.v.6.G..#y.....O....Z)G...w..E..k(....+..O.....Vg.2xC..... .O...jc.....z..~.P...q../.-.'.h.._.cj.=..B.x.Q9.pu.\|i4...i...;O...n.?.,. ....v?.5}.OY@.dG\|<.._[.69@.2..m..I..oP=...xrK.?.....b..5....i&...l.c\b}..Q..O+.V.mJ.....pz....>F.....H...6$. ..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\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	53
Entropy (8bit):	4.763403181378978
Encrypted:	false
SSDEEP:	3:oMty8WddSyHG0dAn:oMLW6yRCn
MD5:	D59322238EE2622C9CA6BF1613C78F1E
SHA1:	736603F46BB58920D0F5AB9C967693FDDED9EC8C
SHA-256:	309FD7269277F93FBA977DAF50596F41F1822DDC9EC10BFA1F90FE931D86B07B
SHA-512:	F4E5CF790E254356B1785C83389BEB07B82563626B52FAD00E74FBEAB17B1ACBAEBDC8E41CC42EABD60E8E81684516BC45611094F3D9A4D733C1AF0F065E5EDF
Malicious:	false
Preview:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe

\Device\ConDrv	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with very long lines

\Device\ConDrv	
Category:	dropped
Size (bytes):	6809
Entropy (8bit):	4.315685828355093
Encrypted:	false
SSDEEP:	96:zKHDGKD7zrrRYZZ/HPw4//HP/HH6K1jqQiGyGTFchzCKtihKCsO2b0N/+7vKAKPO:YrRYZXCKgQifr8sC/635P
MD5:	DA37CE62FC9ABAB3226A1797FF449487
SHA1:	18F29B4F3B1D12BA18DF2EF8964DA20107EEFFC9
SHA-256:	80EAB2A83F12150619544DBFFDD130D60B6869EE742F9000F8E3109F406FAD6E
SHA-512:	5A8BF4140440BCB218CFE90A3371AE761212BC4364DC7E7C055980D3FAB4C4E4499B1CADB13666D4D5F03B6AE835AEE4B44F78D4B2A4AA4ABDF20D8161B12F66
Malicious:	false
Preview:	Microsoft (R) Visual Basic Compiler version 14.7.3056.for Visual Basic 2012.Copyright (c) Microsoft Corporation. All rights reserved...This compiler is provided as part of the Microsoft (R) .NET Framework, but only supports language versions up to Visual Basic 2012, which is no longer the latest version. For compilers that support newer versions of the Visual Basic programming language, see http://go.microsoft.com/fwlink/?LinkID=533241.. Visual Basic Compiler Options.. - OUTPUT FILE -./out:<file> Specifies the output file name../target:exe Create a console application (default). (Short form: /t)./target:winexe Create a Windows application../target:library Create a library assembly../target:module Create a module that can be added to an assembly../target:appcontainerexe Create a Windows application that runs in AppContainer../ta

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.126661889459997
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:	Payment_Confirmation pdf.exe
File size:	446464
MD5:	767f88a961bfbc1b8f8419a32fbade0b
SHA1:	5577d0635fca390c305ff560ca80a6ea19ff7c5b
SHA256:	4f0035201ba7a3a536727862b8ac8dbf389038c5af1674ff7a982190fed1e30b
SHA512:	c5ebaabcd0ecdd1d0a29e8964b02b8fad9961d7b2f144f0ad9a9b00e94cff1c4656c3154219a08ff062d97ad8d2b083a584cab7dd6e0417f233249ac3a2926c3
SSDEEP:	12288:hEvO+l2ttKdpbLFl3Xuchx/f0ymCusZ+uhQM:G6tK6Ocf89sRh
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...n.._.....L.....^k... .....@.. ....@.....

File Icon

Icon Hash:	d8c0ecccd4ccc4d4

Static PE Info

General	
Entrypoint:	0x446b5e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5FF7B26E [Fri Jan 8 01:16:30 2021 UTC]
TLS Callbacks:	

General

CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x46b10	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x48000	0x27f38	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x70000	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	

Name	Virtual Address	Virtual Size	Is in Section
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	0x44b64	0x44c00	False	0.983721590909	data	7.99650215148	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x48000	0x27f38	0x28000	False	0.192211914062	data	4.03959679951	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x70000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x48280	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 33554432, next used block 16777216		
RT_ICON	0x58aa8	0x94a8	data		
RT_ICON	0x61f50	0x5488	data		
RT_ICON	0x673d8	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 49407, next used block 4278190080		
RT_ICON	0x6b600	0x25a8	data		
RT_ICON	0x6dba8	0x10a8	data		
RT_ICON	0x6ec50	0x988	data		
RT_ICON	0x6f5d8	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x6fa40	0x76	data		
RT_VERSION	0x6fab8	0x294	data		
RT_MANIFEST	0x6fd4c	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	
Assembly Version	0.0.0.0
InternalName	Payment_Confirmation pdf.exe
FileVersion	0.0.0.0
ProductVersion	0.0.0.0
FileDescription	
OriginalFilename	Payment_Confirmation pdf.exe

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 8, 2021 20:07:21.510366917 CET	49724	7008	192.168.2.7	185.244.38.210
Jan 8, 2021 20:07:21.688452959 CET	7008	49724	185.244.38.210	192.168.2.7
Jan 8, 2021 20:07:21.688581944 CET	49724	7008	192.168.2.7	185.244.38.210
Jan 8, 2021 20:07:21.819392920 CET	49724	7008	192.168.2.7	185.244.38.210
Jan 8, 2021 20:07:22.366861105 CET	49724	7008	192.168.2.7	185.244.38.210
Jan 8, 2021 20:07:23.070003033 CET	49724	7008	192.168.2.7	185.244.38.210
Jan 8, 2021 20:07:23.984666109 CET	7008	49724	185.244.38.210	192.168.2.7
Jan 8, 2021 20:07:23.984740973 CET	49724	7008	192.168.2.7	185.244.38.210

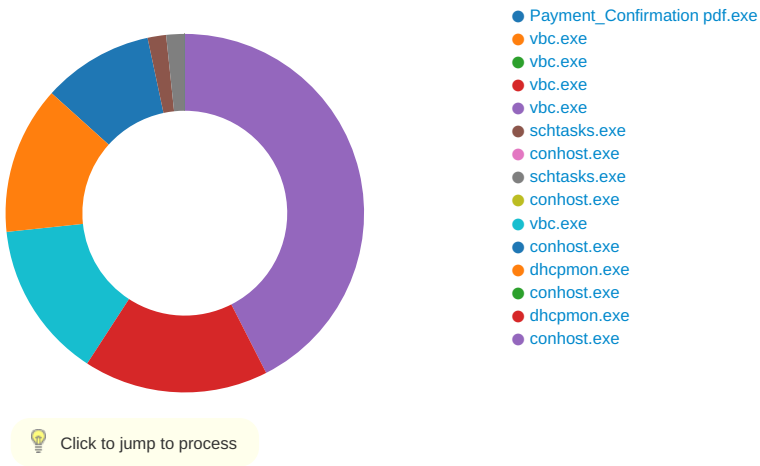
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 8, 2021 20:07:23.993175983 CET	7008	49724	185.244.38.210	192.168.2.7
Jan 8, 2021 20:07:24.070086002 CET	49724	7008	192.168.2.7	185.244.38.210
Jan 8, 2021 20:07:24.121284008 CET	49724	7008	192.168.2.7	185.244.38.210
Jan 8, 2021 20:07:24.239244938 CET	7008	49724	185.244.38.210	192.168.2.7
Jan 8, 2021 20:07:24.239358902 CET	49724	7008	192.168.2.7	185.244.38.210
Jan 8, 2021 20:07:28.420263052 CET	49726	7008	192.168.2.7	185.244.38.210
Jan 8, 2021 20:07:28.597956896 CET	7008	49726	185.244.38.210	192.168.2.7
Jan 8, 2021 20:07:28.598109961 CET	49726	7008	192.168.2.7	185.244.38.210
Jan 8, 2021 20:07:28.599396944 CET	49726	7008	192.168.2.7	185.244.38.210
Jan 8, 2021 20:07:28.787283897 CET	7008	49726	185.244.38.210	192.168.2.7
Jan 8, 2021 20:07:28.787615061 CET	49726	7008	192.168.2.7	185.244.38.210
Jan 8, 2021 20:07:28.966084003 CET	7008	49726	185.244.38.210	192.168.2.7
Jan 8, 2021 20:07:28.982891083 CET	49726	7008	192.168.2.7	185.244.38.210
Jan 8, 2021 20:07:29.205984116 CET	7008	49726	185.244.38.210	192.168.2.7
Jan 8, 2021 20:07:29.206049919 CET	7008	49726	185.244.38.210	192.168.2.7
Jan 8, 2021 20:07:29.206094027 CET	7008	49726	185.244.38.210	192.168.2.7
Jan 8, 2021 20:07:29.206130028 CET	49726	7008	192.168.2.7	185.244.38.210
Jan 8, 2021 20:07:29.206130981 CET	7008	49726	185.244.38.210	192.168.2.7
Jan 8, 2021 20:07:29.206168890 CET	7008	49726	185.244.38.210	192.168.2.7
Jan 8, 2021 20:07:29.206175089 CET	49726	7008	192.168.2.7	185.244.38.210
Jan 8, 2021 20:07:29.206207037 CET	7008	49726	185.244.38.210	192.168.2.7
Jan 8, 2021 20:07:29.206243038 CET	7008	49726	185.244.38.210	192.168.2.7
Jan 8, 2021 20:07:29.206247091 CET	49726	7008	192.168.2.7	185.244.38.210
Jan 8, 2021 20:07:29.206280947 CET	7008	49726	185.244.38.210	192.168.2.7
Jan 8, 2021 20:07:29.206321001 CET	7008	49726	185.244.38.210	192.168.2.7
Jan 8, 2021 20:07:29.206325054 CET	49726	7008	192.168.2.7	185.244.38.210
Jan 8, 2021 20:07:29.206368923 CET	7008	49726	185.244.38.210	192.168.2.7
Jan 8, 2021 20:07:29.206423044 CET	49726	7008	192.168.2.7	185.244.38.210
Jan 8, 2021 20:07:29.384334087 CET	7008	49726	185.244.38.210	192.168.2.7
Jan 8, 2021 20:07:29.384399891 CET	7008	49726	185.244.38.210	192.168.2.7
Jan 8, 2021 20:07:29.384438992 CET	7008	49726	185.244.38.210	192.168.2.7
Jan 8, 2021 20:07:29.384471893 CET	49726	7008	192.168.2.7	185.244.38.210
Jan 8, 2021 20:07:29.384474993 CET	7008	49726	185.244.38.210	192.168.2.7
Jan 8, 2021 20:07:29.384512901 CET	7008	49726	185.244.38.210	192.168.2.7
Jan 8, 2021 20:07:29.384551048 CET	7008	49726	185.244.38.210	192.168.2.7
Jan 8, 2021 20:07:29.384551048 CET	49726	7008	192.168.2.7	185.244.38.210
Jan 8, 2021 20:07:29.384593010 CET	7008	49726	185.244.38.210	192.168.2.7
Jan 8, 2021 20:07:29.384603977 CET	49726	7008	192.168.2.7	185.244.38.210
Jan 8, 2021 20:07:29.384619951 CET	7008	49726	185.244.38.210	192.168.2.7
Jan 8, 2021 20:07:29.384644985 CET	7008	49726	185.244.38.210	192.168.2.7
Jan 8, 2021 20:07:29.384658098 CET	49726	7008	192.168.2.7	185.244.38.210
Jan 8, 2021 20:07:29.384665966 CET	7008	49726	185.244.38.210	192.168.2.7
Jan 8, 2021 20:07:29.384687901 CET	7008	49726	185.244.38.210	192.168.2.7
Jan 8, 2021 20:07:29.384701014 CET	49726	7008	192.168.2.7	185.244.38.210
Jan 8, 2021 20:07:29.384720087 CET	7008	49726	185.244.38.210	192.168.2.7
Jan 8, 2021 20:07:29.384742022 CET	7008	49726	185.244.38.210	192.168.2.7
Jan 8, 2021 20:07:29.384759903 CET	49726	7008	192.168.2.7	185.244.38.210
Jan 8, 2021 20:07:29.384769917 CET	7008	49726	185.244.38.210	192.168.2.7
Jan 8, 2021 20:07:29.384793997 CET	7008	49726	185.244.38.210	192.168.2.7
Jan 8, 2021 20:07:29.384810925 CET	49726	7008	192.168.2.7	185.244.38.210
Jan 8, 2021 20:07:29.384815931 CET	7008	49726	185.244.38.210	192.168.2.7
Jan 8, 2021 20:07:29.384839058 CET	7008	49726	185.244.38.210	192.168.2.7
Jan 8, 2021 20:07:29.384854078 CET	49726	7008	192.168.2.7	185.244.38.210
Jan 8, 2021 20:07:29.384860039 CET	7008	49726	185.244.38.210	192.168.2.7
Jan 8, 2021 20:07:29.384882927 CET	7008	49726	185.244.38.210	192.168.2.7
Jan 8, 2021 20:07:29.384906054 CET	49726	7008	192.168.2.7	185.244.38.210
Jan 8, 2021 20:07:29.384910107 CET	7008	49726	185.244.38.210	192.168.2.7
Jan 8, 2021 20:07:29.384954929 CET	49726	7008	192.168.2.7	185.244.38.210
Jan 8, 2021 20:07:29.562388897 CET	7008	49726	185.244.38.210	192.168.2.7
Jan 8, 2021 20:07:29.562436104 CET	7008	49726	185.244.38.210	192.168.2.7
Jan 8, 2021 20:07:29.562472105 CET	7008	49726	185.244.38.210	192.168.2.7
Jan 8, 2021 20:07:29.562520027 CET	7008	49726	185.244.38.210	192.168.2.7
Jan 8, 2021 20:07:29.562568903 CET	49726	7008	192.168.2.7	185.244.38.210
Jan 8, 2021 20:07:29.562597990 CET	49726	7008	192.168.2.7	185.244.38.210

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 8, 2021 20:07:29.562825918 CET	7008	49726	185.244.38.210	192.168.2.7
Jan 8, 2021 20:07:29.563023090 CET	7008	49726	185.244.38.210	192.168.2.7
Jan 8, 2021 20:07:29.563085079 CET	49726	7008	192.168.2.7	185.244.38.210
Jan 8, 2021 20:07:29.563149929 CET	7008	49726	185.244.38.210	192.168.2.7
Jan 8, 2021 20:07:29.563324928 CET	7008	49726	185.244.38.210	192.168.2.7
Jan 8, 2021 20:07:29.563366890 CET	7008	49726	185.244.38.210	192.168.2.7
Jan 8, 2021 20:07:29.563380957 CET	49726	7008	192.168.2.7	185.244.38.210
Jan 8, 2021 20:07:29.563405991 CET	7008	49726	185.244.38.210	192.168.2.7
Jan 8, 2021 20:07:29.563446045 CET	7008	49726	185.244.38.210	192.168.2.7
Jan 8, 2021 20:07:29.563450098 CET	49726	7008	192.168.2.7	185.244.38.210
Jan 8, 2021 20:07:29.563483000 CET	7008	49726	185.244.38.210	192.168.2.7
Jan 8, 2021 20:07:29.563523054 CET	7008	49726	185.244.38.210	192.168.2.7
Jan 8, 2021 20:07:29.563534021 CET	49726	7008	192.168.2.7	185.244.38.210
Jan 8, 2021 20:07:29.563561916 CET	7008	49726	185.244.38.210	192.168.2.7
Jan 8, 2021 20:07:29.563607931 CET	49726	7008	192.168.2.7	185.244.38.210
Jan 8, 2021 20:07:29.563607931 CET	7008	49726	185.244.38.210	192.168.2.7
Jan 8, 2021 20:07:29.563649893 CET	7008	49726	185.244.38.210	192.168.2.7
Jan 8, 2021 20:07:29.563687086 CET	7008	49726	185.244.38.210	192.168.2.7
Jan 8, 2021 20:07:29.563692093 CET	49726	7008	192.168.2.7	185.244.38.210
Jan 8, 2021 20:07:29.563724995 CET	7008	49726	185.244.38.210	192.168.2.7
Jan 8, 2021 20:07:29.563761950 CET	7008	49726	185.244.38.210	192.168.2.7
Jan 8, 2021 20:07:29.563764095 CET	49726	7008	192.168.2.7	185.244.38.210
Jan 8, 2021 20:07:29.563796997 CET	7008	49726	185.244.38.210	192.168.2.7
Jan 8, 2021 20:07:29.563836098 CET	7008	49726	185.244.38.210	192.168.2.7
Jan 8, 2021 20:07:29.563846111 CET	49726	7008	192.168.2.7	185.244.38.210
Jan 8, 2021 20:07:29.563875914 CET	7008	49726	185.244.38.210	192.168.2.7
Jan 8, 2021 20:07:29.563922882 CET	7008	49726	185.244.38.210	192.168.2.7
Jan 8, 2021 20:07:29.563936949 CET	49726	7008	192.168.2.7	185.244.38.210

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: Payment_Confirmation pdf.exe PID: 2800 Parent PID: 5660

General

Start time:	20:07:12
Start date:	08/01/2021
Path:	C:\Users\user\Desktop\Payment_Confirmation pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Payment_Confirmation pdf.exe'
Imagebase:	0x590000
File size:	446464 bytes
MD5 hash:	767F88A961BFBC1B8F8419A32FBADE0B
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: 00000000.00000002.233380857.0000000003A01000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.233380857.0000000003A01000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.233380857.0000000003A01000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D5ACF06	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	6D5ACF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Payment_Confirmation pdf.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D8BC78D	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\Microsoft\CLR_v4.0_32\UsageLogs\Payment_Confirmation pdf.exe.log	unknown	522	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 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 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0	success or wait	1	6D8BC907	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	6D585705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D585705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D4E03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D58CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D4E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D4E03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D585705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D585705	unknown

Analysis Process: vbc.exe PID: 5332 Parent PID: 2800

General

Start time:	20:07:13
Start date:	08/01/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe
Imagebase:	0xc00000
File size:	2688096 bytes
MD5 hash:	B3A917344F5610BEEC562556F11300FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: vbc.exe PID: 5952 Parent PID: 2800

General

Start time:	20:07:14
Start date:	08/01/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe
Imagebase:	0xc00000
File size:	2688096 bytes
MD5 hash:	B3A917344F5610BEEC562556F11300FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: vbc.exe PID: 1516 Parent PID: 2800

General

Start time:	20:07:15
Start date:	08/01/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe
Imagebase:	0xc00000
File size:	2688096 bytes
MD5 hash:	B3A917344F5610BEEC562556F11300FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: vbc.exe PID: 5352 Parent PID: 2800

General

Start time:	20:07:16
Start date:	08/01/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe
Imagebase:	0xc00000
File size:	2688096 bytes
MD5 hash:	B3A917344F5610BEEC562556F11300FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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	6D5ACF06	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	6D5ACF06	unknown
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C3FBEFF	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	6C3F1E60	CreateFileW
C:\Program Files (x86)\DHCP Monitor	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C3FBEFF	CreateDirectoryW
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6C3FDD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp863B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C3F7038	GetTempFileNameW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C3F1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp8988.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C3F7038	GetTempFileNameW
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	6C3FBEFF	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	6C3FBEFF	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	20	6C3F1E60	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	6C3F1E60	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	6C3F1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp863B.tmp	success or wait	1	6C3F6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp8988.tmp	success or wait	1	6C3F6A95	DeleteFileW

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	8f 9c 79 0e 54 b4 d8 48	..y.T..H	success or wait	1	6C3F1B4F	WriteFile
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0	524288	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 00 00 28 01 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 ef 2e 64 a3 ab 4f 0a f0 ab 4f 0a f0 ab 4f 0a f0 18 00 ea f0 aa 4f 0a f0 18 00 eb f0 a5 4f 0a f0 76 b0 c4 f0 ae 4f 0a f0 76 b0 da f0 aa 4f 0a f0 b5 1d 99 f0 a9 4f 0a f0 1f d3 f8 f0 a8 4f 0a f0 a6 1d eb f0 a9 4f 0a f0 3d 3a e5 f0 af 4f 0a f0 3d 3a fb f0 bb 4f 0a f0 3d 3a f8 f0 bd 4f 0a f0 3d 3a f9 f0 ad 4f 0a f0 76 b0 c1 f0 ba 4f 0a f0 ab 4f 0b f0 da 4e 0a f0 1f d3 fd f0 c0 4f 0a	MZ......................@..... .... (...........!..L.!This program cannot be run in DOS mode.... $.........d..O...O...O.......O ....O..v....O..v....O...... .O.......O.......O..=:...O..=: ...O..=:...O..=:...O..v....O.. .O...N.......O.	success or wait	6	6C3FDD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp863B.tmp	unknown	1316	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 20 2f 3e 0d 0a 20 20 3c 54 72 69 67 67 65 72 73 20 2f 3e 0d 0a 20 20 3c 50 72 69 6e 63 69 70 61 6c 73 3e 0d 0a 20 20 20 20 3c 50 72 69 6e 63 69 70 61 6c 20 69 64 3d 22 41 75 74 68 6f 72 22 3e 0d 0a 20 20 20 20 20 20 3c 4c 6f 67 6f 6e 54 79 70 65 3e 49 6e 74 65 72 61 63 74 69 76 65 54 6f 6b 65 6e 3c 2f 4c 6f 67 6f 6e 54 79 70 65 3e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microso ft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>	success or wait	1	6C3F1B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	unknown	53	43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 45 54 5c 46 72 61 6d 65 77 6f 72 6b 5c 76 34 2e 30 2e 33 30 33 31 39 5c 76 62 63 2e 65 78 65	C:\Windows\Microsoft.NET\Frame work\v4.0.30319\vbc.exe	success or wait	1	6C3F1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp8988.tmp	unknown	1310	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 20 2f 3e 0d 0a 20 20 3c 54 72 69 67 67 65 72 73 20 2f 3e 0d 0a 20 20 3c 50 72 69 6e 63 69 70 61 6c 73 3e 0d 0a 20 20 20 20 3c 50 72 69 6e 63 69 70 61 6c 20 69 64 3d 22 41 75 74 68 6f 72 22 3e 0d 0a 20 20 20 20 20 20 3c 4c 6f 67 6f 6e 54 79 70 65 3e 49 6e 74 65 72 61 63 74 69 76 65 54 6f 6b 65 6e 3c 2f 4c 6f 67 6f 6e 54 79 70 65 3e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microso ft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>	success or wait	1	6C3F1B4F	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	5	6C3F1B4F	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	6C3F1B4F	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 85 16 f4 a5 20 38 a2 6a 80 a4 a3 f3 7c 88 26 58 b6 ca 65 a6 46 b8 2a 80	9iH....}Z..4..f..... 8.j....|. &X..e.F.*.	success or wait	1	6C3F1B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe.config	unknown	4095	success or wait	1	6D585705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe.config	unknown	8173	end of file	1	6D585705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D585705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D585705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D4E03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe.config	unknown	4095	success or wait	1	6D58CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe.config	unknown	8173	end of file	1	6D58CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D58CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D4E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D4E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D4E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D4E03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D585705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D585705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C3F1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C3F1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe.config	unknown	4096	success or wait	1	6C3F1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe.config	unknown	4096	end of file	1	6C3F1B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6D56D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6D56D72F	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe	unknown	4096	success or wait	1	6D56D72F	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe	unknown	512	success or wait	1	6D56D72F	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe.config	unknown	4095	success or wait	1	6D585705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe.config	unknown	8173	end of file	1	6D585705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe.config	unknown	4095	success or wait	1	6D585705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe.config	unknown	8173	end of file	1	6D585705	unknown

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run	DHCP Monitor	unicode	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	success or wait	1	6C3F646A	RegSetValueExW

Analysis Process: schtasks.exe PID: 4660 Parent PID: 5352

General

Start time:	20:07:18
Start date:	08/01/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp863B.tmp'
Imagebase:	0x1d0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp863B.tmp	unknown	2	success or wait	1	1DAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp863B.tmp	unknown	1317	success or wait	1	1DABD9	ReadFile

Analysis Process: conhost.exe PID: 1304 Parent PID: 4660

General

Start time:	20:07:19
Start date:	08/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: 2172 Parent PID: 5352

General

Start time:	20:07:19
Start date:	08/01/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmp8988.tmp'
Imagebase:	0x1d0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp8988.tmp	unknown	2	success or wait	1	1DAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp8988.tmp	unknown	1311	success or wait	1	1DABD9	ReadFile

Analysis Process: conhost.exe PID: 5992 Parent PID: 2172

General

Start time:	20:07:20
Start date:	08/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: vbc.exe PID: 3996 Parent PID: 1104

General

Start time:	20:07:21
Start date:	08/01/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe 0
Imagebase:	0xc00000
File size:	2688096 bytes

MD5 hash:	B3A917344F5610BEEC562556F11300FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	76	4d 69 63 72 6f 73 6f 66 74 20 28 52 29 20 56 69 73 75 61 6c 20 42 61 73 69 63 20 43 6f 6d 70 69 6c 65 72 20 76 65 72 73 69 6f 6e 20 31 34 2e 37 2e 33 30 35 36 0a 66 6f 72 20 56 69 73 75 61 6c 20 42 61 73 69 63 20 32 30 31 32 0a	Microsoft (R) Visual Basic Compiler version 14.7.3056.for Visual Basic 2012.	success or wait	1	C74CE5	WriteFile
\Device\ConDrv	unknown	365	43 6f 70 79 72 69 67 68 74 20 28 63 29 20 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 2e 20 20 41 6c 6c 20 72 69 67 68 74 73 20 72 65 73 65 72 76 65 64 2e 0a 0a 54 68 69 73 20 63 6f 6d 70 69 6c 65 72 20 69 73 20 70 72 6f 76 69 64 65 64 20 61 73 20 70 61 72 74 20 6f 66 20 74 68 65 20 4d 69 63 72 6f 73 6f 66 74 20 28 52 29 20 2e 4e 45 54 20 46 72 61 6d 65 77 6f 72 6b 2c 20 62 75 74 20 6f 6e 6c 79 20 73 75 70 70 6f 72 74 73 20 6c 61 6e 67 75 61 67 65 20 76 65 72 73 69 6f 6e 73 20 75 70 20 74 6f 20 56 69 73 75 61 6c 20 42 61 73 69 63 20 32 30 31 32 2c 20 77 68 69 63 68 20 69 73 20 6e 6f 20 6c 6f 6e 67 65 72 20 74 68 65 20 6c 61 74 65 73 74 20 76 65 72 73 69 6f 6e 2e 20 46 6f 72 20 63 6f 6d 70 69 6c 65 72 73 20 74 68 61 74 20 73 75 70 70 6f	Copyright (c) Microsoft Corporation. All rights reserved...This compiler is provided as part of the Microsoft (R) .NET Framework, but only supports language versions up to Visual Basic 2012, which is no longer the latest version. For compilers that suppo	success or wait	1	C74CE5	WriteFile
\Device\ConDrv	unknown	1	0a	.	success or wait	1	C74CE5	WriteFile
\Device\ConDrv	unknown	3	76 62 63	vbc	success or wait	1	C74CE5	WriteFile
\Device\ConDrv	unknown	3	20 3a 20	:	success or wait	1	C74CE5	WriteFile
\Device\ConDrv	unknown	18	43 6f 6d 6d 61 6e 64 20 6c 69 6e 65 20 65 72 72 6f 72	Command line error	success or wait	1	C74CE5	WriteFile
\Device\ConDrv	unknown	10	20 42 43 32 30 30 31 20 3a 20	BC2001 :	success or wait	1	C74CE5	WriteFile
\Device\ConDrv	unknown	27	66 69 6c 65 20 27 30 27 20 63 6f 75 6c 64 20 6e 6f 74 20 62 65 20 66 6f 75 6e 64	file '0' could not be found	success or wait	1	C74CE5	WriteFile
\Device\ConDrv	unknown	1	0a	.	success or wait	1	C74CE5	WriteFile
\Device\ConDrv	unknown	3	76 62 63	vbc	success or wait	1	C74CE5	WriteFile
\Device\ConDrv	unknown	3	20 3a 20	:	success or wait	1	C74CE5	WriteFile
\Device\ConDrv	unknown	18	43 6f 6d 6d 61 6e 64 20 6c 69 6e 65 20 65 72 72 6f 72	Command line error	success or wait	1	C74CE5	WriteFile
\Device\ConDrv	unknown	10	20 42 43 32 30 30 38 20 3a 20	BC2008 :	success or wait	1	C74CE5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	26	6e 6f 20 69 6e 70 75 74 20 73 6f 75 72 63 65 73 20 73 70 65 63 69 66 69 65 64	no input sources specified	success or wait	1	C74CE5	WriteFile
\Device\ConDrv	unknown	1	0a	.	success or wait	1	C74CE5	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\System.Runtime.dll	unknown	37456	success or wait	1	6D955B9D	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Accessibility.dll	unknown	35912	success or wait	1	6D955B9D	ReadFile

Analysis Process: conhost.exe PID: 5972 Parent PID: 3996

General

Start time:	20:07:21
Start date:	08/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: dhcpmon.exe PID: 5836 Parent PID: 1104

General

Start time:	20:07:21
Start date:	08/01/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0
Imagebase:	0xd40000
File size:	2688096 bytes
MD5 hash:	B3A917344F5610BEEC562556F11300FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 2%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	76	4d 69 63 72 6f 73 6f 66 74 20 28 52 29 20 56 69 73 75 61 6c 20 42 61 73 69 63 20 43 6f 6d 70 69 6c 65 72 20 76 65 72 73 69 6f 6e 20 31 34 2e 37 2e 33 30 35 36 0a 66 6f 72 20 56 69 73 75 61 6c 20 42 61 73 69 63 20 32 30 31 32 0a	Microsoft (R) Visual Basic Compiler version 14.7.3056.for Visual Basic 2012.	success or wait	1	DB4CE5	WriteFile
\Device\ConDrv	unknown	365	43 6f 70 79 72 69 67 68 74 20 28 63 29 20 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 2e 20 20 41 6c 6c 20 72 69 67 68 74 73 20 72 65 73 65 72 76 65 64 2e 0a 0a 54 68 69 73 20 63 6f 6d 70 69 6c 65 72 20 69 73 20 70 72 6f 76 69 64 65 64 20 61 73 20 70 61 72 74 20 6f 66 20 74 68 65 20 4d 69 63 72 6f 73 6f 66 74 20 28 52 29 20 2e 4e 45 54 20 46 72 61 6d 65 77 6f 72 6b 2c 20 62 75 74 20 6f 6e 6c 79 20 73 75 70 70 6f 72 74 73 20 6c 61 6e 67 75 61 67 65 20 76 65 72 73 69 6f 6e 73 20 75 70 20 74 6f 20 56 69 73 75 61 6c 20 42 61 73 69 63 20 32 30 31 32 2c 20 77 68 69 63 68 20 69 73 20 6e 6f 20 6c 6f 6e 67 65 72 20 74 68 65 20 6c 61 74 65 73 74 20 76 65 72 73 69 6f 6e 2e 20 46 6f 72 20 63 6f 6d 70 69 6c 65 72 73 20 74 68 61 74 20 73 75 70 70 6f	Copyright (c) Microsoft Corporation. All rights reserved...This compiler is provided as part of the Microsoft (R) .NET Framework, but only supports language versions up to Visual Basic 2012, which is no longer the latest version. For compilers that suppo	success or wait	1	DB4CE5	WriteFile
\Device\ConDrv	unknown	1	0a	.	success or wait	1	DB4CE5	WriteFile
\Device\ConDrv	unknown	3	76 62 63	vbc	success or wait	1	DB4CE5	WriteFile
\Device\ConDrv	unknown	3	20 3a 20	:	success or wait	1	DB4CE5	WriteFile
\Device\ConDrv	unknown	18	43 6f 6d 6d 61 6e 64 20 6c 69 6e 65 20 65 72 72 6f 72	Command line error	success or wait	1	DB4CE5	WriteFile
\Device\ConDrv	unknown	10	20 42 43 32 30 30 31 20 3a 20	BC2001 :	success or wait	1	DB4CE5	WriteFile
\Device\ConDrv	unknown	27	66 69 6c 65 20 27 30 27 20 63 6f 75 6c 64 20 6e 6f 74 20 62 65 20 66 6f 75 6e 64	file '0' could not be found	success or wait	1	DB4CE5	WriteFile
\Device\ConDrv	unknown	1	0a	.	success or wait	1	DB4CE5	WriteFile
\Device\ConDrv	unknown	3	76 62 63	vbc	success or wait	1	DB4CE5	WriteFile
\Device\ConDrv	unknown	3	20 3a 20	:	success or wait	1	DB4CE5	WriteFile
\Device\ConDrv	unknown	18	43 6f 6d 6d 61 6e 64 20 6c 69 6e 65 20 65 72 72 6f 72	Command line error	success or wait	1	DB4CE5	WriteFile
\Device\ConDrv	unknown	10	20 42 43 32 30 30 38 20 3a 20	BC2008 :	success or wait	1	DB4CE5	WriteFile
\Device\ConDrv	unknown	26	6e 6f 20 69 6e 70 75 74 20 73 6f 75 72 63 65 73 20 73 70 65 63 69 66 69 65 64	no input sources specified	success or wait	1	DB4CE5	WriteFile
\Device\ConDrv	unknown	1	0a	.	success or wait	1	DB4CE5	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\System.Runtime.dll	unknown	37456	success or wait	1	6D955B9D	ReadFile

Analysis Process: conhost.exe PID: 4604 Parent PID: 5836

General

Start time:	20:07:22
Start date:	08/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: dhcpmon.exe PID: 1000 Parent PID: 3292

General

Start time:	20:07:28
Start date:	08/01/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0xd40000
File size:	2688096 bytes
MD5 hash:	B3A917344F5610BEEC562556F11300FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	76	4d 69 63 72 6f 73 6f 66 74 20 28 52 29 20 56 69 73 75 61 6c 20 42 61 73 69 63 20 43 6f 6d 70 69 6c 65 72 20 76 65 72 73 69 6f 6e 20 31 34 2e 37 2e 33 30 35 36 0a 66 6f 72 20 56 69 73 75 61 6c 20 42 61 73 69 63 20 32 30 31 32 0a	Microsoft (R) Visual Basic Compiler version 14.7.3056.for Visual Basic 2012.	success or wait	1	DB4CE5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	365	43 6f 70 79 72 69 67 68 74 20 28 63 29 20 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 2e 20 20 41 6c 6c 20 72 69 67 68 74 73 20 72 65 73 65 72 76 65 64 2e 0a 0a 54 68 69 73 20 63 6f 6d 70 69 6c 65 72 20 69 73 20 70 72 6f 76 69 64 65 64 20 61 73 20 70 61 72 74 20 6f 66 20 74 68 65 20 4d 69 63 72 6f 73 6f 66 74 20 28 52 29 20 2e 4e 45 54 20 46 72 61 6d 65 77 6f 72 6b 2c 20 62 75 74 20 6f 6e 6c 79 20 73 75 70 70 6f 72 74 73 20 6c 61 6e 67 75 61 67 65 20 76 65 72 73 69 6f 6e 73 20 75 70 20 74 6f 20 56 69 73 75 61 6c 20 42 61 73 69 63 20 32 30 31 32 2c 20 77 68 69 63 68 20 69 73 20 6e 6f 20 6c 6f 6e 67 65 72 20 74 68 65 20 6c 61 74 65 73 74 20 76 65 72 73 69 6f 6e 2e 20 46 6f 72 20 63 6f 6d 70 69 6c 65 72 73 20 74 68 61 74 20 73 75 70 70 6f	Copyright (c) Microsoft Corporation. All rights reserved...This compiler is provided as part of the Microsoft (R) .NET Framework, but only supports language versions up to Visual Basic 2012, which is no longer the latest version. For compilers that suppo	success or wait	1	DB4CE5	WriteFile
\Device\ConDrv	unknown	1	0a	.	success or wait	1	DB4CE5	WriteFile
\Device\ConDrv	unknown	18	20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20		success or wait	1	DB4CE5	WriteFile
\Device\ConDrv	unknown	29	56 69 73 75 61 6c 20 42 61 73 69 63 20 43 6f 6d 70 69 6c 65 72 20 4f 70 74 69 6f 6e 73	Visual Basic Compiler Options	success or wait	1	DB4CE5	WriteFile
\Device\ConDrv	unknown	1	0a	.	success or wait	1	DB4CE5	WriteFile
\Device\ConDrv	unknown	1	0a	.	success or wait	1	DB4CE5	WriteFile
\Device\ConDrv	unknown	34	20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20		success or wait	8	DB4CE5	WriteFile
\Device\ConDrv	unknown	15	2d 20 4f 55 54 50 55 54 20 46 49 4c 45 20 2d	- OUTPUT FILE -	success or wait	8	DB4CE5	WriteFile
\Device\ConDrv	unknown	1	0a	.	success or wait	8	DB4CE5	WriteFile
\Device\ConDrv	unknown	11	2f 6f 75 74 3a 3c 66 69 6c 65 3e	/out:<file>	success or wait	46	DB4CE5	WriteFile
\Device\ConDrv	unknown	23	20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20		success or wait	46	DB4CE5	WriteFile
\Device\ConDrv	unknown	31	53 70 65 63 69 66 69 65 73 20 74 68 65 20 6f 75 74 70 75 74 20 66 69 6c 65 20 6e 61 6d 65 2e	Specifies the output file name.	success or wait	54	DB4CE5	WriteFile
\Device\ConDrv	unknown	1	0a	.	success or wait	53	DB4CE5	WriteFile
\Device\ConDrv	unknown	11	2f 74 61 72 67 65 74 3a 65 78 65	/target:exe	success or wait	18	DB4CE5	WriteFile
\Device\ConDrv	unknown	23	20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20		success or wait	18	DB4CE5	WriteFile
\Device\ConDrv	unknown	56	43 72 65 61 74 65 20 61 20 63 6f 6e 73 6f 6c 65 20 61 70 70 6c 69 63 61 74 69 6f 6e 20 28 64 65 66 61 75 6c 74 29 2e 20 28 53 68 6f 72 74 20 66 6f 72 6d 3a 20 2f 74 29	Create a console application (default). (Short form: /t)	success or wait	18	DB4CE5	WriteFile
\Device\ConDrv	unknown	1	0a	.	success or wait	18	DB4CE5	WriteFile
\Device\ConDrv	unknown	1	0a	.	success or wait	8	DB4CE5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	34	20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20		success or wait	8	DB4CE5	WriteFile

Analysis Process: conhost.exe PID: 5796 Parent PID: 1000

General

Start time:	20:07:29
Start date:	08/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis