ID: 508404
Sample Name: Yeni sipari#U015f _WJO-001, pdf.exe
Cookbook: default.jbs
Time: 08:21:59
Date: 25/10/2021
Version: 33.0.0 White Diamond

Table of Contents

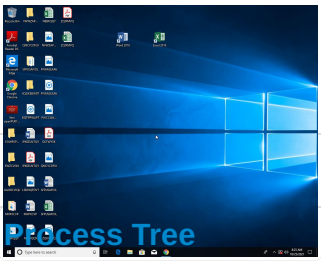
Windows Analysis Report Yeni sipari#U015f _WJO-001, …

Overview

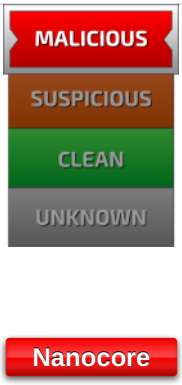
General Information

Sample Name:	Yeni sipari#U015f _WJO-001, pdf.exe
Analysis ID:	508404
MD5:	7e0600a5300a5c..
SHA1:	c52fb2df7f32b3b…
SHA256:	5f86426410b741a.
Tags:	exe geo NanoCore RAT TUR
Infos:	

Most interesting Screenshot:



Detection

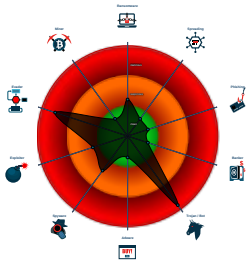


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Sigma detected: NanoCore
- Yara detected AntiVM3
- Detected Nanocore Rat
- Yara detected Nanocore RAT
- Writes to foreign memory regions
- Tries to detect sandboxes and other…
- Machine Learning detection for samp…
- Allocates memory in foreign process…
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…

Classification



- **System is w10x64**
- Yeni sipari#U015f _WJO-001, pdf.exe (PID: 1380 cmdline: 'C:\Users\user\Desktop\Yeni sipari#U015f _WJO-001, pdf.exe' MD5: 7E0600A5300A5CD87FCE0CF4398B578F)
  - MSBuild.exe (PID: 4540 cmdline: {path} MD5: 88BBB7610152B48C2B3879473B17857E)
  - MSBuild.exe (PID: 6692 cmdline: {path} MD5: 88BBB7610152B48C2B3879473B17857E)
- dhcpmon.exe (PID: 6112 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: 88BBB7610152B48C2B3879473B17857E)
  - conhost.exe (PID: 2848 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "c44e3244-c9be-4fcb-8e75-051ae087",
  "Group": "MAX LOGS",
  "Domain1": "cashlink.ddns.net",
  "Domain2": "",
  "Port": 4774,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "ClearZoneIdentifier": "Disable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Disable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.943511160.000000000564 0000.00000004.00020000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
00000005.00000002.943511160.000000000564 0000.00000004.00020000.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost
00000005.00000002.943511160.000000000564 0000.00000004.00020000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000000.00000002.684104761.000000000410 1000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x70535:$x1: NanoCore.ClientPluginHost • 0x70572:$x2: IClientNetworkHost • 0x740a5:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000000.00000002.684104761.000000000410 1000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Click to see the 18 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.MSBuild.exe.3ece424.4.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0x28269:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost • 0x28296:$x2: IClientNetworkHost
5.2.MSBuild.exe.3ece424.4.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x28269:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0x29344:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost • 0x28283:$s5: IClientLoggingHost
5.2.MSBuild.exe.3ece424.4.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
5.2.MSBuild.exe.2e916e0.1.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
5.2.MSBuild.exe.2e916e0.1.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost

Click to see the 33 entries

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Yara detected Nanocore RAT

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

Uses dynamic DNS services

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

.NET source code contains potential unpacker

Malware Analysis System Evasion:

Yara detected AntiVM3

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

HIPS / PFW / Operating System Protection Evasion:

Writes to foreign memory regions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

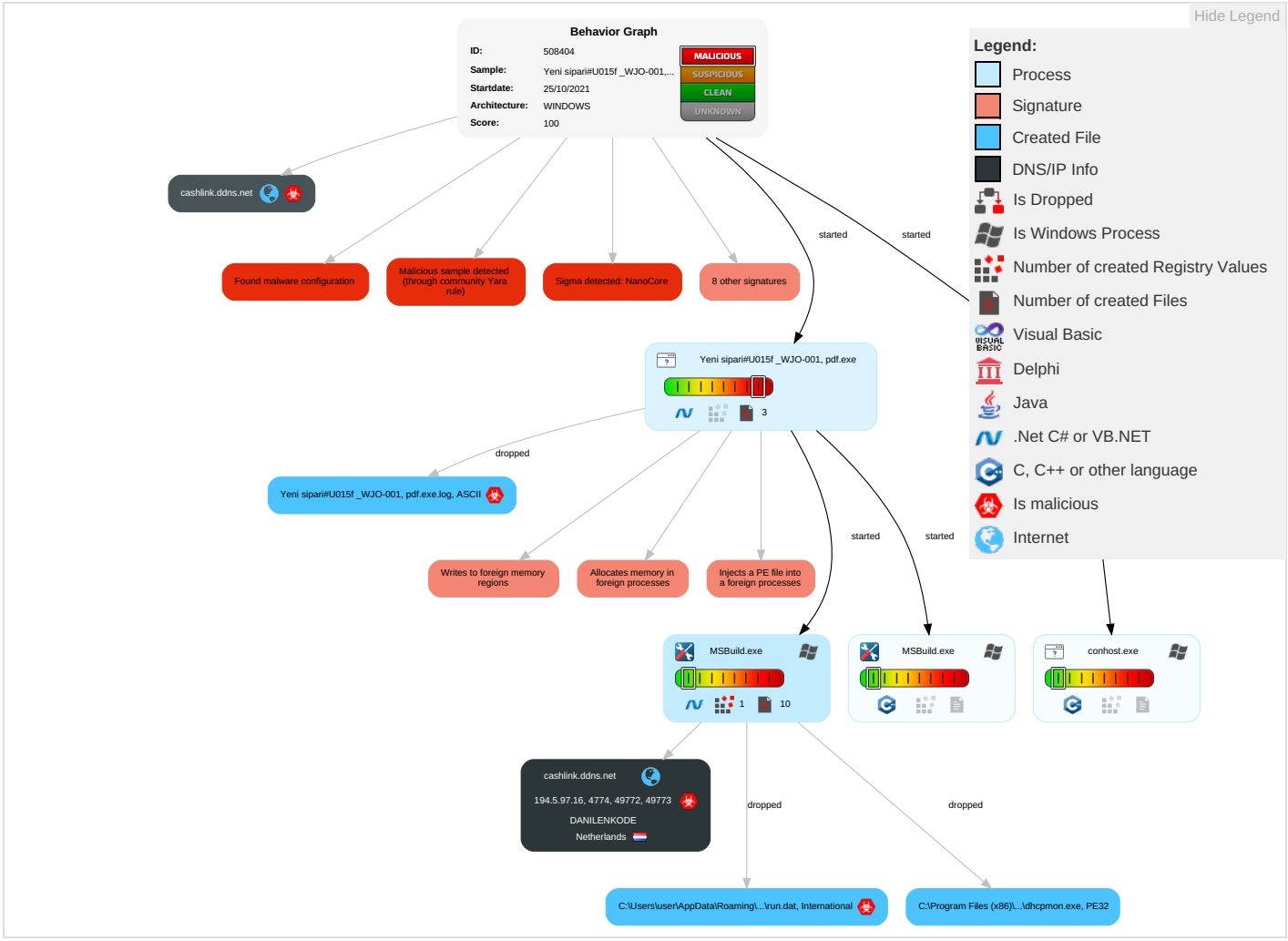
Detected Nanocore Rat

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	Ne Eff
Valid Accounts	Windows Management Instrumentation	Path Interception	Access Token Manipulation 1	Masquerading 2	Input Capture 2 1	Security Software Discovery 1 1	Remote Services	Input Capture 2 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Ea Ins Ne Co
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Process Injection 3 1 2	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Ex Re Ca
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2 1	Security Account Manager	Virtualization/Sandbox Evasion 2 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Ex Tra Lo
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Access Token Manipulation 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1	SI Sw
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 3 1 2	LSA Secrets	System Information Discovery 1 3	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 2 1	Ma De Co
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Ja De Se
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Ro Ac
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Do Ins Pr

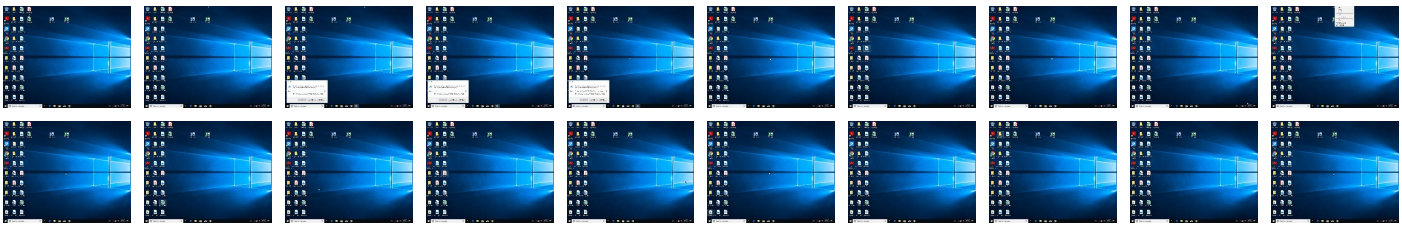
Behavior Graph



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
Yeni sipari#U015f _WJO-001, pdf.exe	100%	Joe Sandbox ML		

Dropped Files

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

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.MSBuild.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
5.2.MSBuild.exe.5640000.6.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Domains

Source	Detection	Scanner	Label	Link
cashlink.ddns.net	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
	0%	Avira URL Cloud	safe	
http://go.microsoft.	0%	URL Reputation	safe	
http://tempuri.org/sipDataSet.xsd	2%	Virustotal		Browse
http://tempuri.org/sipDataSet.xsd	0%	Avira URL Cloud	safe	
http://tempuri.org/XXXXXXXXXXXXXXXXXXXXXX.xsd	0%	Avira URL Cloud	safe	
http://go.microsoft.LinkId=42127	0%	Avira URL Cloud	safe	
cashlink.ddns.net	0%	Avira URL Cloud	safe	
http://tempuri.org/XXXXXXXXXXXXXXXXXXXXXX.xsd9WinForms_RecursiveFormCreate5WinForms_SeeInnerExcepti	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cashlink.ddns.net	194.5.97.16	true	true	• 1%, Virustotal, Browse	unknown

Contacted URLs

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

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.5.97.16	cashlink.ddns.net	Netherlands		208476	DANILENKODE	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	508404
Start date:	25.10.2021
Start time:	08:21:59
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Yeni sipari#U015f _WJO-001, pdf.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	19
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout

Detection:	MAL
Classification:	mal100.troj.evad.winEXE@7/5@19/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.6% (good quality ratio 0%) • Quality average: 0% • Quality standard deviation: 0%
HCA Information:	• Successful, ratio: 95% • 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

Simulations

Behavior and APIs

Time	Type	Description
08:23:00	API Interceptor	1x Sleep call for process: Yeni sipari#U015f _WJO-001, pdf.exe modified
08:23:06	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
194.5.97.16	DHL_1012617429350,pdf.exe	Get hash	malicious	Browse	
	DHL_1012617429350,pdf.exe	Get hash	malicious	Browse	
	1012617429350,pdf.exe	Get hash	malicious	Browse	
	AWB# 2617429350,pdf.exe	Get hash	malicious	Browse	
	Yeni Sipari#U015f # 765-3523663, pdf.exe	Get hash	malicious	Browse	
	Nuevo pedido _WJO-001,pdf.exe	Get hash	malicious	Browse	
	765-3523663 ,pdf.exe	Get hash	malicious	Browse	
	New Order #86-55113,pdf.exe	Get hash	malicious	Browse	
	Nuevo pedido # 765-3523663 ,pdf.exe	Get hash	malicious	Browse	
	Nuevo pedido # 86-55113,pdf.exe	Get hash	malicious	Browse	
	Nuevo pedido # 86-55113 .pdf.exe	Get hash	malicious	Browse	
	Nuevo pedido # 86-55113,pdf.exe	Get hash	malicious	Browse	
	Urgent RFQ_AP65425652_032421,pdf.exe	Get hash	malicious	Browse	
	OC CVE6535 TVOP-MIO 16(C) 2021,pdf.exe	Get hash	malicious	Browse	
	Pos withdrawal reduced to 0.5%.exe	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DANILENKODE	7STXNgZD3g.exe	Get hash	malicious	Browse	• 194.5.98.107
	ORIGINAL DOCUMENTS BL, C.I. & PACKING LIST.exe	Get hash	malicious	Browse	• 194.5.98.158
	Comprobante de pago.xls	Get hash	malicious	Browse	• 194.5.98.74
	Comprobante de pago.doc	Get hash	malicious	Browse	• 194.5.98.40
	AWB # 1012617429350,pdf.exe	Get hash	malicious	Browse	• 194.5.97.23
	SK202-8 #YN12-60387.exe	Get hash	malicious	Browse	• 194.5.97.207
	nIXnNtZvtI.exe	Get hash	malicious	Browse	• 194.5.98.205
	SecuriteInfo.com.VB.Trojan.Valyria.3530.8728.xls	Get hash	malicious	Browse	• 194.5.98.249
	DHL_1012617429350,pdf.exe	Get hash	malicious	Browse	• 194.5.97.23

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Pago_Monex_usd.xls	Get hash	malicious	Browse	• 194.5.98.46
	Niki-Gmbh Germany Inquiry.exe	Get hash	malicious	Browse	• 194.5.97.97
	new.exe	Get hash	malicious	Browse	• 194.5.98.212
	XdZ4ad8GpU.exe	Get hash	malicious	Browse	• 194.5.98.48
	we-ship-SNE-9874657.xlsx	Get hash	malicious	Browse	• 194.5.98.48
	Bankdetails86507.exe	Get hash	malicious	Browse	• 194.5.98.126
	Order Quotation Request_pdf.exe	Get hash	malicious	Browse	• 194.5.97.128
	IMG0000030_Pago_SWIFT.exe	Get hash	malicious	Browse	• 194.5.98.202
	2qDKwiGx46.exe	Get hash	malicious	Browse	• 194.5.98.134
	Specifications.docx.exe	Get hash	malicious	Browse	• 194.5.97.212
	Specifications.xls.exe	Get hash	malicious	Browse	• 194.5.97.212

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	FeDEx AWB TRACKING DETAILS.exe	Get hash	malicious	Browse	
	09142021_PDF.vbs	Get hash	malicious	Browse	
	P0 (2021)-2790 new order.exe	Get hash	malicious	Browse	
	TNT AWB TRACKING DETAILS.exe	Get hash	malicious	Browse	
	BankSlip.exe	Get hash	malicious	Browse	
	PAYMENT ERROR.exe	Get hash	malicious	Browse	
	DHL AWB TRACKING DETAILS.exe	Get hash	malicious	Browse	
	DHL AWB TRACKING DETAILS.exe	Get hash	malicious	Browse	
	PcgYFOwcNQ.exe	Get hash	malicious	Browse	
	Invoice Fanpage Karma.bat.exe	Get hash	malicious	Browse	
	zslaUKmBfr.exe	Get hash	malicious	Browse	
	scanbankdoc210999796432225.bat.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Zusy.394472.4088.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.W32.AIDetect.malware1.17748.exe	Get hash	malicious	Browse	
	fnnEkbo4cW.exe	Get hash	malicious	Browse	
	kAGA3XtSEaOxfvA.exe	Get hash	malicious	Browse	
	PO 18-3081.exe	Get hash	malicious	Browse	
	Order417.exe	Get hash	malicious	Browse	
	PCT00029827656278 27BC.exe	Get hash	malicious	Browse	
	NO19800800.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	69632
Entropy (8bit):	5.20894581699571
Encrypted:	false
SSDEEP:	768:NElGiBcBuiyFjUwF0wdP9/rJMDnRFRJfStGpwV3e3qtAcy:ilGBu7jjP9/tMDn9Jt+VO3GO
MD5:	88BBB7610152B48C2B3879473B17857E
SHA1:	0F6CF8DD66AA58CE31DA4E8AC0631600EF055636
SHA-256:	2C7ACC16D19D076D67E9F1F37984935899B79536C9AC6EEC8850C44D20F87616
SHA-512:	5BACDF6C190A76C2C6A9A3519936E08E898AC8A2B1384D60429DF850BE778860435BF9E5EB316517D2345A5AAE201F369863F7A242134253978BCB5B2179CA58
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Joe Sandbox View:	• Filename: FeDEx AWB TRACKING DETAILS.exe, Detection: malicious, Browse • Filename: 09142021_PDF.vbs, Detection: malicious, Browse • Filename: P0 (2021)-2790 new order.exe, Detection: malicious, Browse • Filename: TNT AWB TRACKING DETAILS.exe, Detection: malicious, Browse • Filename: BankSlip.exe, Detection: malicious, Browse • Filename: PAYMENT ERROR.exe, Detection: malicious, Browse • Filename: DHL AWB TRACKING DETAILS.exe, Detection: malicious, Browse • Filename: DHL AWB TRACKING DETAILS.exe, Detection: malicious, Browse • Filename: PcgYFOwcNQ.exe, Detection: malicious, Browse • Filename: Invoice Fanpage Karma.bat.exe, Detection: malicious, Browse • Filename: zslaUKmBfr.exe, Detection: malicious, Browse • Filename: scanbankdoc210999796432225.bat.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Variant.Zusy.394472.4088.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.W32.AIDetect.malware1.17748.exe, Detection: malicious, Browse • Filename: fnnEkbo4cW.exe, Detection: malicious, Browse • Filename: kAGA3XtSEaOxfvA.exe, Detection: malicious, Browse • Filename: PO 18-3081.exe, Detection: malicious, Browse • Filename: Order417.exe, Detection: malicious, Browse • Filename: PCT0002982765627827BC.exe, Detection: malicious, Browse • Filename: NO19800800.exe, Detection: malicious, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....{Z.....@..... .....@.. .....@.....99.. ..@.....S.....`/..... ..... ..... ..H.....text..... ..... ..`.rsrc...`/.....0.....@..@.reloc..... . .....@..B..... .....

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\Yeni sipari#U015f _WJO-001, pdf.exe.log	
Process:	C:\Users\user\Desktop\Yeni sipari#U015f _WJO-001, pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	664
Entropy (8bit):	5.288448637977022
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10Ug+9Yz9t0U29hJ5g1B0U2ukyrFk70U2xANlW3ANv:MLF20NaL3z2p29hJ5g522rW2xAi3A9
MD5:	B1DB55991C3DA14E35249AEA1BC357CA
SHA1:	0DD2D91198FDEF296441B12F1A906669B279700C
SHA-256:	34D3E48321D5010AD2BD1F3F0B728077E4F5A7F70D66FA36B57E5209580B6BDC
SHA-512:	BE38A31888C9C2F8047FA9C99672CB985179D325107514B7500DDA9523AE3E1D20B45EACC4E6C8A5D096360D0FBB98A120E63F38FFE324DF8A0559F6890CC80
Malicious:	**true**
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Runtime.Remo#\35774dc3cd31b4550ab06c3354cf4ba5\System.Runtime.Remoting.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	441
Entropy (8bit):	5.388715099859351
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U2+gYhD5itZbgbe4MqJsGMe4M6:MLF20NaL32+g2OH4xvn4j
MD5:	88F0104DB9A3F9BC4F0FC3805F571B0D
SHA1:	CDD4F34385792F0CCE0A844F4ABB447C25AB4E73
SHA-256:	F6C11D3D078ED73F2640DA510E68DEEAA5F14F79CAE2E23A254B4E37C7D0230F
SHA-512:	04B977F63CAB8DE20EA7EFA9D4299C2E625D92FA6D54CA03EECD9F322E978326B353824F23BEC0E712083BDE0DBC5CC4EE90922137106B096050CA46A166DFE
Malicious:	false
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Xml\527c933194f3a99a816d83c619a3e1d3\System.Xml.ni.dll",0..2,"Microsoft.Build.Engine, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.Build.Framework, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
File Type:	International EBCDIC text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
SSDEEP:	3:Z8:Z8
MD5:	43EDE2DCA45F13D48C642FFE1081E662
SHA1:	E60E211D5742F3AC1C891A586CAB2138B23CEEFF
SHA-256:	B247C2053D99F6AB51812F74E0859DA326EE30524D14CC37A6FD34A7DDEA12BE
SHA-512:	56E66BFD8589C030E2777306C917728706E27415BF2B17FF12FFC6011786668BE2ECA1F2CD328D594A5516BFD917AD5650CAD86FDFA044582C5993BEB80EF871
Malicious:	**true**
Preview:	Vi.....H

\Device\ConDrv	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	306
Entropy (8bit):	4.969261552825097
Encrypted:	false
SSDEEP:	6:zx3M1tlAX8bSWR30qysGMQbSVRRZBXVRbJ0fFdCsq2UTiMdH8stCal+n:zK1XnV30ZsGMIG9BFRbQdCT2UftCM+
MD5:	F227448515085A647910907084E6728E
SHA1:	5FA1A8E28B084DA25A1BBC51A2D75810CEF57E2C
SHA-256:	662BA47D628FE8EBE95DD47B4482110A10B49AED09387BC0E028BB66E68E20BD
SHA-512:	6F6E5DFFF7B17C304FB19B0BA5466AF84EF98A5C2EFA573AF72CFD3ED6964E9FD7F8E4B79FCFFBEF87CE545418C69D4984F4DD60BBF457D0A3640950F8FC5AF0
Malicious:	false
Preview:	Microsoft (R) Build Engine Version 2.0.50727.8922..[Microsoft .NET Framework, Version 2.0.50727.8922]..Copyright (C) Microsoft Corporation 2005. All rights reserved.....MSBUILD : error MSB1003: Specify a project or solution file. The current working directory does not contain a project or solution file...

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.26643085265657
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:	Yeni sipari#U015f _WJO-001, pdf.exe
File size:	884224
MD5:	7e0600a5300a5cd87fce0cf4398b578f
SHA1:	c52fb2df7f32b3bfadaa923a67e59204bb306429
SHA256:	5f86426410b741a6c2c5c3693069520197f2789e490a36c75ace1a4b2792cab6
SHA512:	d339f29c09bf5d79b597af2299123c70b3a1be02a325d7254413ce23c4230065d95fa68b21138730d6c0d4ae94717ea7ac9664f58c2bfc8bd7605bb3b43f916a
SSDEEP:	24576:Fba+q9hGIdbYGMszLPgVmIsAleFHH+HHHHHWHVHCUXGHnHHhHraHoeXO:FbNSV/HOmIpeFHH+HHHHHWHVHCUXGHnt
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....sa.....P..h.....n.... .....@.. .....@.....

File Icon

Icon Hash:	00d0524c687048a0

Static PE Info

General

Entrypoint:	0x4a876e
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:	0x6173E0F7 [Sat Oct 23 10:16:23 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
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

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xa6774	0xa6800	False	0.71680274024	data	7.48504821183	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xaa000	0x31040	0x31200	False	0.423564726463	data	5.88116448591	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xdc000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
10/25/21-08:23:06.720778	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	53097	8.8.8.8	192.168.2.4
10/25/21-08:23:13.047508	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	49257	8.8.8.8	192.168.2.4
10/25/21-08:23:19.338896	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	49910	8.8.8.8	192.168.2.4
10/25/21-08:23:31.723363	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	53700	8.8.8.8	192.168.2.4
10/25/21-08:23:38.861357	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	51726	8.8.8.8	192.168.2.4
10/25/21-08:24:22.408140	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	51255	8.8.8.8	192.168.2.4
10/25/21-08:24:37.557508	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	60579	8.8.8.8	192.168.2.4
10/25/21-08:24:43.309583	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	49228	8.8.8.8	192.168.2.4
10/25/21-08:24:54.742082	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	55916	8.8.8.8	192.168.2.4
10/25/21-08:25:06.910564	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	60542	8.8.8.8	192.168.2.4

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 25, 2021 08:23:06.696093082 CEST	192.168.2.4	8.8.8.8	0x4a0	Standard query (0)	cashlink.ddns.net	A (IP address)	IN (0x0001)
Oct 25, 2021 08:23:13.027206898 CEST	192.168.2.4	8.8.8.8	0x5f07	Standard query (0)	cashlink.ddns.net	A (IP address)	IN (0x0001)
Oct 25, 2021 08:23:19.315490961 CEST	192.168.2.4	8.8.8.8	0x174c	Standard query (0)	cashlink.ddns.net	A (IP address)	IN (0x0001)
Oct 25, 2021 08:23:25.126760006 CEST	192.168.2.4	8.8.8.8	0x9075	Standard query (0)	cashlink.ddns.net	A (IP address)	IN (0x0001)
Oct 25, 2021 08:23:31.702912092 CEST	192.168.2.4	8.8.8.8	0xe166	Standard query (0)	cashlink.ddns.net	A (IP address)	IN (0x0001)
Oct 25, 2021 08:23:38.841285944 CEST	192.168.2.4	8.8.8.8	0xe8b6	Standard query (0)	cashlink.ddns.net	A (IP address)	IN (0x0001)
Oct 25, 2021 08:23:47.204689980 CEST	192.168.2.4	8.8.8.8	0x1fc2	Standard query (0)	cashlink.ddns.net	A (IP address)	IN (0x0001)
Oct 25, 2021 08:23:53.762490034 CEST	192.168.2.4	8.8.8.8	0xfec7	Standard query (0)	cashlink.ddns.net	A (IP address)	IN (0x0001)
Oct 25, 2021 08:24:03.365789890 CEST	192.168.2.4	8.8.8.8	0x9a74	Standard query (0)	cashlink.ddns.net	A (IP address)	IN (0x0001)
Oct 25, 2021 08:24:10.144007921 CEST	192.168.2.4	8.8.8.8	0x6ef3	Standard query (0)	cashlink.ddns.net	A (IP address)	IN (0x0001)
Oct 25, 2021 08:24:16.123938084 CEST	192.168.2.4	8.8.8.8	0x5010	Standard query (0)	cashlink.ddns.net	A (IP address)	IN (0x0001)
Oct 25, 2021 08:24:22.384063959 CEST	192.168.2.4	8.8.8.8	0x9341	Standard query (0)	cashlink.ddns.net	A (IP address)	IN (0x0001)
Oct 25, 2021 08:24:30.390775919 CEST	192.168.2.4	8.8.8.8	0x23aa	Standard query (0)	cashlink.ddns.net	A (IP address)	IN (0x0001)
Oct 25, 2021 08:24:37.539165974 CEST	192.168.2.4	8.8.8.8	0x1de	Standard query (0)	cashlink.ddns.net	A (IP address)	IN (0x0001)
Oct 25, 2021 08:24:43.288317919 CEST	192.168.2.4	8.8.8.8	0xa70b	Standard query (0)	cashlink.ddns.net	A (IP address)	IN (0x0001)
Oct 25, 2021 08:24:49.017062902 CEST	192.168.2.4	8.8.8.8	0xeb8c	Standard query (0)	cashlink.ddns.net	A (IP address)	IN (0x0001)
Oct 25, 2021 08:24:54.721607924 CEST	192.168.2.4	8.8.8.8	0xcf0c	Standard query (0)	cashlink.ddns.net	A (IP address)	IN (0x0001)
Oct 25, 2021 08:25:00.597276926 CEST	192.168.2.4	8.8.8.8	0xbcd5	Standard query (0)	cashlink.ddns.net	A (IP address)	IN (0x0001)
Oct 25, 2021 08:25:06.890649080 CEST	192.168.2.4	8.8.8.8	0xc4fb	Standard query (0)	cashlink.ddns.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 25, 2021 08:23:06.720777988 CEST	8.8.8.8	192.168.2.4	0x4a0	No error (0)	cashlink.ddns.net		194.5.97.16	A (IP address)	IN (0x0001)
Oct 25, 2021 08:23:13.047508001 CEST	8.8.8.8	192.168.2.4	0x5f07	No error (0)	cashlink.ddns.net		194.5.97.16	A (IP address)	IN (0x0001)
Oct 25, 2021 08:23:19.338896036 CEST	8.8.8.8	192.168.2.4	0x174c	No error (0)	cashlink.ddns.net		194.5.97.16	A (IP address)	IN (0x0001)
Oct 25, 2021 08:23:25.145519018 CEST	8.8.8.8	192.168.2.4	0x9075	No error (0)	cashlink.ddns.net		194.5.97.16	A (IP address)	IN (0x0001)
Oct 25, 2021 08:23:31.723362923 CEST	8.8.8.8	192.168.2.4	0xe166	No error (0)	cashlink.ddns.net		194.5.97.16	A (IP address)	IN (0x0001)
Oct 25, 2021 08:23:38.861356974 CEST	8.8.8.8	192.168.2.4	0xe8b6	No error (0)	cashlink.ddns.net		194.5.97.16	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 25, 2021 08:23:47.221677065 CEST	8.8.8.8	192.168.2.4	0x1fc2	No error (0)	cashlink.ddns.net		194.5.97.16	A (IP address)	IN (0x0001)
Oct 25, 2021 08:23:53.781286001 CEST	8.8.8.8	192.168.2.4	0xfec7	No error (0)	cashlink.ddns.net		194.5.97.16	A (IP address)	IN (0x0001)
Oct 25, 2021 08:24:03.384665966 CEST	8.8.8.8	192.168.2.4	0x9a74	No error (0)	cashlink.ddns.net		194.5.97.16	A (IP address)	IN (0x0001)
Oct 25, 2021 08:24:10.160450935 CEST	8.8.8.8	192.168.2.4	0x6ef3	No error (0)	cashlink.ddns.net		194.5.97.16	A (IP address)	IN (0x0001)
Oct 25, 2021 08:24:16.142330885 CEST	8.8.8.8	192.168.2.4	0x5010	No error (0)	cashlink.ddns.net		194.5.97.16	A (IP address)	IN (0x0001)
Oct 25, 2021 08:24:22.408139944 CEST	8.8.8.8	192.168.2.4	0x9341	No error (0)	cashlink.ddns.net		194.5.97.16	A (IP address)	IN (0x0001)
Oct 25, 2021 08:24:30.410547972 CEST	8.8.8.8	192.168.2.4	0x23aa	No error (0)	cashlink.ddns.net		194.5.97.16	A (IP address)	IN (0x0001)
Oct 25, 2021 08:24:37.557507992 CEST	8.8.8.8	192.168.2.4	0x1de	No error (0)	cashlink.ddns.net		194.5.97.16	A (IP address)	IN (0x0001)
Oct 25, 2021 08:24:43.309582949 CEST	8.8.8.8	192.168.2.4	0xa70b	No error (0)	cashlink.ddns.net		194.5.97.16	A (IP address)	IN (0x0001)
Oct 25, 2021 08:24:49.035656929 CEST	8.8.8.8	192.168.2.4	0xeb8c	No error (0)	cashlink.ddns.net		194.5.97.16	A (IP address)	IN (0x0001)
Oct 25, 2021 08:24:54.742082119 CEST	8.8.8.8	192.168.2.4	0xcf0c	No error (0)	cashlink.ddns.net		194.5.97.16	A (IP address)	IN (0x0001)
Oct 25, 2021 08:25:00.615669012 CEST	8.8.8.8	192.168.2.4	0xbcd5	No error (0)	cashlink.ddns.net		194.5.97.16	A (IP address)	IN (0x0001)
Oct 25, 2021 08:25:06.910563946 CEST	8.8.8.8	192.168.2.4	0xc4fb	No error (0)	cashlink.ddns.net		194.5.97.16	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Yeni sipari#U015f _WJO-001, pdf.exe PID: 1380 Parent PID: 6020

General

Start time:	08:22:59
Start date:	25/10/2021
Path:	C:\Users\user\Desktop\Yeni sipari#U015f _WJO-001, pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Yeni sipari#U015f _WJO-001, pdf.exe'
Imagebase:	0x830000

File size:	884224 bytes
MD5 hash:	7E0600A5300A5CD87FCE0CF4398B578F
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: 00000000.00000002.684104761.0000000004101000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.684104761.0000000004101000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.684104761.0000000004101000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.683440077.0000000003FF1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.683440077.0000000003FF1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.683440077.0000000003FF1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: MSBuild.exe PID: 4540 Parent PID: 1380

General

Start time:	08:23:02
Start date:	25/10/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x420000
File size:	69632 bytes
MD5 hash:	88BBB7610152B48C2B3879473B17857E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: MSBuild.exe PID: 6692 Parent PID: 1380

General

Start time:	08:23:02
Start date:	25/10/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x870000
File size:	69632 bytes
MD5 hash:	88BBB7610152B48C2B3879473B17857E
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: 00000005.00000002.943511160.0000000005640000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.943511160.0000000005640000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.943511160.0000000005640000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.942525404.0000000003EC7000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.942525404.0000000003EC7000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.940978754.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.940978754.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.940978754.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.943376551.00000000053A0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.943376551.00000000053A0000.00000004.00020000.sdmp, Author: Florian Roth
Reputation:	moderate

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: dhcpmon.exe PID: 6112 Parent PID: 3424

General

Start time:	08:23:15
Start date:	25/10/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0x10000
File size:	69632 bytes
MD5 hash:	88BBB7610152B48C2B3879473B17857E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: conhost.exe PID: 2848 Parent PID: 6112

General

Start time:	08:23:17
Start date:	25/10/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis